1 of 18 DOCUMENTS

Whether Social Media "Harvesting" or "Scraping" is a Crime

2010 Emerging Issues 5364

Whether Social Media "Harvesting" or "Scraping" is a Crime

By Kirsten Koepsel, Carey Lening and Ron Weikers

October 19, 2010

SUMMARY: Most of us are well aware that savvy computer people can use social media sites like Facebook to obtain information that members don't want them to have, or to use it in ways the members would not want it. But what can be done if that happens? Are there any federal criminal statutes that would apply? Kirsten Koepsel, Carey Lening, and Ron Weikers explain the possible crimes committed in such "scraping" or "harvesting" of data off the Web.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Facebook users were recently warned to lock down their privacy settings and "rid their minds of the idea that all the friends that they have collected are really friends," because "internet predators are trying to use Facebook for their own purposes." n1 Less than two weeks later, a security consultant named Ron Bowes posted on BitTorrent n2 a downloadable torrent file n3 containing the names and profile URLs of 171 million Facebook accounts. n4 The consultant harvested data from public profiles n5 of users who had not changed their privacy settings. n6 According to the security consultants' blog posting, the harvesting was undertaken to test a new security tool then under development. n7

Hackers regularly use similar means to harvest data from social media, but they often do so for nefarious purposes, such as perpetrating various types of identity theft. Accessing publicly available information is certainly not a crime, because this is, after all, the very purpose of the Internet. However, to do so on such a massive scale certainly violates our collective notion of fair play, and may even violate current cybercrime laws. This article examines whether "scraping" of public data on such a massive scale violates the Computer Fraud and Abuse Act, the Stored Communications Act, the Wire Act, and other existing fraud and identity-theft statutes.

ANALYSIS UNDER CURRENT CYBERCRIME LAWS.

Under the Computer Fraud and Abuse Act of 1986 ("CFAA"), n8 the first question that arises is whether the consultant intentionally accessed a computer without authorization or exceeded authorized access, and thereby obtained information from a protected computer. n9 The Facebook.com network was intentionally accessed, according to the consultant's blog post, n10 but was his access unauthorized or in excess of his authorization? Facebook's "About" page describes the site's stated purpose as: "Giving people the power to share and make the world more open and connected." n11 Users of Facebook communicate their activities, thoughts and photos through their own pages, through friends'

pages, and through private e-mails. n12

Furthermore, the same harvesting could be done by any Internet user by going to the Facebook directory and clicking on every publicly available name and then recording the URL associated with the name. Such access not only is granted freely to users of the site, but is openly available to any user of the Internet. Some news stories also noted that the same information provided in the BitTorrent download is also available through search engines such as Google and Bing. n13

Although the harvested material is accessible to any user of the Internet, Facebook states that by "using or accessing Facebook, you agree ... [y]ou will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission." n14 Courts have held that scraping and harvesting violate the CFAA; therefore, the consultant violated the terms of use of Facebook. n15 Under the Facebook terms of use, the user also agrees not to "use Facebook to do anything unlawful, misleading, malicious, or discriminatory." n16 The consultant could be prosecuted under CFAA for his harvesting activities.

Under the CFAA, another question is whether the consultant "intentionally accesse[d] a protected computer without authorization, and as a result of such conduct, recklessly cause[d] damage." n17 The consultant intentionally accessed a protected computer, but it is not clear whether the harvesting caused damage to the computer or network. Damage under the CFAA is defined as "any impairment to the integrity or availability of data, a program, a system, or information." n18 From the consultant's account of his actions, it does not appear that any impairment or availability of data, the system, or Facebook information occurred. A prosecution under CFAA would likely not succeed, based on an apparent absence of damage to Facebook.

In the recent case of *United States v. Drew*, the court examined the "issue of whether ... violations of an Internet website's terms of service constitute a crime under the Computer Fraud and Abuse Act." n19 In *Drew*, the defendant allegedly registered a fake profile on Myspace.com, which violated the MySpace terms of service. In ruling on the defendant's motion to dismiss the indictment, the court held that a prosecution for a violation of a website's terms of service, without more, "would result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals." n20 The court also held that it was "unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization." n21 Based on *Drew*, it is likely that a prosecution under CFAA would not succeed.

The second question that arises is whether the harvesting and subsequent public posting of Facebook profile information constitutes a violation of the Stored Communications Act of 1986 ("SCA") n22 by "intentionally access[ing] without authorization a facility through which an electronic communication service is provided." n23 The definition of electronic communication service ("ECS") - "any service which provides to users thereof the ability to send or receive wire or electronic communications" - is applies to Facebook by virtue of the fact that once a Facebook member has "friended" another member, both can send private messages (electronic communications) or post the message on other members' pages. n24 A California district court addressed this very question in *Crispin v. Christian Audigier, Inc.* n25 The court recognized that Facebook provided private messaging or e-mail services and, as such, was an ECS. n26

Did the harvesting "intentionally exceed an authorization to access that facility," or "obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage"? n27 The consultant's blog post explains that he collected "two pieces of data: 1. The names of 170 million users. 2. The URL of those users. I did **NOT** collect email addresses, friends, private data, public data, or anything else." n28 According to his blog posting, the harvester does not appear to have obtained, altered, or prevented "authorized access to a communication ... in electronic storage." Accordingly, prosecution under the SCA would most likely not succeed.

Although prosecution under the CFAA and SCA would likely fail, there are other cybercrime laws that could be

considered, such as on wiretapping or identity theft. Under the Wiretap Act, n29 for example, did the consultant intentionally intercept, endeavor to intercept, or procure "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication"? n30 According to the consultant's blog post, he did not do so. His harvesting was only of the Facebook member names and URLs.

Perhaps the consultant's activities rose to the level of identity theft under various state and federal laws. n31 The Federal Trade Commission defines identity theft as any act where someone "uses personally identifying information [of another], like name, Social Security number, or credit card number, without permission, to commit fraud or other crimes." n32 The downloadable file contains only the name and related URL but no other personally identifying information. The consultant publicly posted names (without permission), but did not use the names for any other purpose; i.e., he apparently did not commit fraud or other crimes. Did the consultant perhaps aid and abet the commission of identity-theft crimes? Not likely, as anyone can access the harvested information on Facebook or through any number of search engines.

Although they sparked public outrage, the consultant's actions appear to have been legal under current laws.

GIVING POWER BACK TO THE USERS.

Congress has not ignored social networking and crime victimization. On July 28, 2010, the United States House of Representatives Committee on the Judiciary held a hearing titled "Online Privacy, Social Networking, and Crime Victimization." n33 Among the witnesses was Joe Sullivan, Chief Security Officer of Facebook. n34 Mr. Sullivan testified that Facebook's mission "is to give people the power to find, connect, and share information with their friends and the people around them." n35 He also testified about Facebook's new privacy framework, released in late 2009, in which it asked its more than 350 million users around the world to take active steps to preserve and protect their private information. n36 Facebook revamped its privacy settings and user controls in order to provide users with a "quick and easy three step process for reviewing and updating" their settings. n37 Thus, while users can now control within a few mouse clicks the very information that the consultant made available to the world, one change that Facebook did not make is the ability to hide everything from Facebook's advertising base by default. Accordingly, users must still make a conscious choice as to how much information they're willing to share. n38

At the July 28, hearing, it was telling that most witnesses did not testify about the consultant's harvesting and posting of Facebook names and profile URLs. Only the Electronic Privacy Information Center ("EPIC") testified that current laws such as the SCA needed to be changed. n39 EPIC recommended that "[S]ection 2701 of the Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA) should restrict more forcefully the ability of service providers such as Facebook to share user data with third parties without explicit 'opt-in' from users." n40

For practitioners, the current cybercrime laws and social media have had limited discussion in the media or in court cases. Practitioners should nonetheless advise their clients to take active steps to ensure that privacy controls are on when using social media.

Return to Text

n1 Garry Barker, TheAge, *Cybercrime in Your Facebook*, The Vine (July 19, 2010, 6 a.m.), at http://www.thevine.com.au/tech/news/cybercrime-in-your-facebook20100719.aspx.

n2 See http://www.bittorrent.com/.

n3 See http://www.ehow.com/about_4673906_what-torrent-file.html.

n4 Ian Paul, *The Facebook Data Torrent Debacle: Q&A*, PC World (July 29, 2010), at http://www.pcworld.com/article/202167/the_facebook_data_torrent_debacle_qanda.html. Facebook has over 500 million active users. http://www.facebook.com/press/info.php?statistics. For an overview of how Facebook works, see Madhurjya Bhattacharyya, *How Does Facebook Work*, Buzzle.com (June 15, 2010), at http://www.buzzle.com/articles/how-does-facebook-work.html. For some reactions to the story, see John Hudson, *Hacker Harvests 100M Facebook Profiles and Publishes Data: Who's At Risk?*, The Atlantic Wire (July 29, 2010), at http://www.theatlanticwire.com/opinions/view/opinion/Hacker-Harvests-100M-Facebook-Profiles-and-Publishes-Data-Whos-At-

n5 See http://www.facebook.com/directory. The directory lists by name the members who have a "Public Search Listing." When a member name is clicked, the specific Facebook page for that member is revealed, allowing the name and the URL of that member to be seen. The viewer must log in to Facebook to view information and photos on the member's page. Accessing a member's page from the list will also allow the viewer to click through to the target's friends' profiles, "even if those friends have made themselves non-searchable." *Facebook: 100 million users accounts data leaked on torrents*, DiTii.com (July 28, 2010), at http://www.ditii.com/2010/07/28/facebook-100-million-users-accounts-data-leaked-on-torrents/.

n6 Emily Price, *100M Facebook Profiles Now Available for Download*, PC World (July 28, 2010), at http://www.pcworld.com/article/202126/100m_facebook_profiles_now_available_for_download.html. For information that is available in the torrent download, see Rhonda Callow, *100 Million Facebook Users Added to a Publicly-Available Torrent File*, Sync Blog.com (July 28, 2010), at http://www.sync-blog.com/sync/2010/07/100-million-facebook-users-added-to-a-publicly-available-torrent-file.html. A link to the file is available at http://www.skullsecurity.org/blog/?p=887.

n7 Meghan Keane, *Marketers are downloading data on 100 million Facebook users*, Econsultancy (July 30, 2010), at http://econsultancy.com/us/blog/6343-marketers-are-downloading-the-leaked-list-of-100-million-facebook-users.

n8 *18 U.S.C. § 1030.*

n9 *18 U.S.C. § 1030*(a)(2)(C).

n10 A script was used to harvest the information from the site. *See* Ron Bowes, *Followup to my Facebook Research*, Skull Security (Aug. 12, 2010), at http://www.skullsecurity.org/blog/?p=898.

n11 See http://www.facebook.com/facebook.

n12 Members logged into Facebook can send private messages to their friends.

n13 Nick Bilton, *Researcher Releases Facebook Profile Data*, nytimes.com (July 28, 2010, 7:03 p.m.), at http://bits.blogs.nytimes.com/2010/07/28/100-million-facebook-ids-compiled-online/.

n14 Facebook Terms § 3.2, at http://www.facebook.com/terms.php?ref=pf.

n15 *See, e.g.*, *EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000).*

n16 Facebook, Terms, 3.10 at http://www.facebook.com/terms.php?ref=pf.

n17 *18 U.S.C. § 1030*(a)(5)(B).

n18 *18 U.S.C. § 1030*(e)(8).

n19 *259 F.R.D. 449, 2009 U.S. Dist. LEXIS 85780* (C.D. Cal. Aug. 28, 2009) and http://www.citmedialaw.org/threats/united-states-v-drew.

n20 *259 F.R.D. at 466.*

n21 *Id. at 467.* The court also stated: "However, if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution." *Id.* For a discussion of void-for -vagueness doctrine and the CFAA, see Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn L. Rev. 5 (May 2010),* at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187.

n22 *18 U.S.C. § 2701.* The Stored Communications Act was also enacted in 1986 as part of the Electronic Communications Privacy Act, *18 U.S.C. § 2510* et seq.

n23 *18 U.S.C. § 2701*(a)(1).

n24 Bhattacharyya, *supra* note 4.

n25 *2010 U.S. Dist. LEXIS 52832* (C.D. Cal. May 26, 2010). In *Crispin*, the defendants served subpoenas duces tecum on Black Market Art Company, Facebook, Media Temple, Inc. and MySpace, Inc. seeking "Crispin's basic subscriber information, as well as all communications between Crispin and tattoo artist Bryan Callan, and all communications that referred or related to Audigier, CAI, the Ed Hardy brand, or any of the sublicensee defendants." *Id.* at *4.

n26 *Id*. at *42. The court also analyzed whether Facebook was an electronic bulletin board under the SCA.

n27 *18 U.S.C. § 2701*(a)(2).

n28 Bowes, *Followup to my Facebook Research,* at http://www.skullsecurity.org/blog/?p=898 (emphasis in original). He also noted in his post, "And the URL might lead to nothing but a name and whatever picture the user chose -that's what Facebook shares at a minimum."

n29 *18 U.S.C. §§ 2510*-2522.

n30 *18 U.S.C. § 2511*(1)(a).

n31 *See, e.g., 18 U.S.C. §§ 1028* (Fraud and related activity in connection with identification documents, authentication features, and information), 1028A (Aggravated identity theft).

n32 FTC.gov, About Identity Theft, at: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last accessed Sept. 26, 2010) ("you" and "your" omitted).

n33 *Online Privacy, Social Networking, and Crime Victimization*, Hearing Before the H. Comm. on the Judiciary, 111th Cong. (July 28, 2010), transcript at http://judiciary.house.gov/hearings/hear_100728.html.

n34 *Id*. Other witnesses included Gordon M. Snow of the Federal Bureau of Investigation, Michael P. Merritt of the U.S. Secret Service, Marc Rotenberg of the Electronic Privacy Information Center, and Joseph Pasqua of Symantec Corporation.

n35 Joe Sullivan, Testimony of Joe Sullivan, at http://judiciary.house.gov/hearings/pdf/Sullivan100728.pdf.

n36 *Id*.

n37 Ruchi Sanghvi, *New Tools to Control Your Experience*, The Facebook Blog (Dec. 9, 2009, 7:04 a.m.), at http://blog.facebook.com/blog.php?post=196629387130.

n38 Facebook's Privacy Policy is at http://www.facebook.com/policy.php (last revised Apr. 22, 2010). *But*

see Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WSJ.com, Oct. 18, 2010, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

n39 Marc Rotenberg, Testimony and Statement for the Record, at http://judiciary.house.gov/hearings/pdf/Rotenberg100728.pdf.

n40 *Id.*

RELATED LINKS:

- 1-2A Computer Law § 2A.10;
- 1-2A Computer Law § 2A.11;
- 4-4B Computer Law § 4B.15;
- 4-84 Criminal Defense Techniques § 84.04;
- 1-2 Law of the Internet § 2.03;
- 1-7 Law of the Internet § 7.02.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Kirsten Koepsel is Director, Legal Affairs & Tax, Aerospace Industries Association in Arlington, VA.

Carey Lening is an intellectual property, privacy and technology attorney in Washington, DC.

Ron Weikers is Managing Partner of Weikers & Co. | Software-Law.com in Manchester, NH, and Adjunct Professor of Law at Franklin Pierce Law Center in Concord, NH. Any views expressed herein are solely the authors', and do not reflect the views of their respective employers.

The Effects and Means of Combating State-Sponsored Cyberthreats

2010 Emerging Issues 5326

The Effects and Means of Combating State-Sponsored Cyberthreats

By Carey Lening, Kirsten Koepsel and Ron Weikers

September 28, 2010

SUMMARY: Cyberattacks can be secret, mysterious, and amorphous, and dealing with them correspondingly harder to manage. This article concentrates on state-sponsored cyberattacks and cyberthreats. It discusses what forms they may take and what measures have been offered to deal with them. The authors are attorneys Carey Lening, Kirsten Koepsel, and Ron Weikers.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: State-sponsored cyberattacks have beleaguered information security specialists for quite some time, particularly those specialists managing attractive critical infrastructure targets such as government, transportation, energy, and banking networks. n1 Fifty-four percent of 600 IT and security professionals polled in a 2008 study reported that their organizations - all "critical infrastructure enterprises" - had experienced large attacks by "high-level adversaries" such as terrorists, organized crime rings, or nation-states. n2

Unlike their predecessors, hackers today are no longer content to target large government systems. The hypertechnical criminals of today have become masterful at marketing their tools and services as "hired guns" to a multitude of actors - ranging from nation-states to organized crime rings and drug traffickers. Simultaneously, the method and means of attack have themselves become commodities, with sophisticated tools such as "botnets," n3 distributed denials of service, n4 and Trojan attacks n5 widely bought and sold on criminal trading platforms and in online chatrooms. n6 The damage inflicted from cyberattacks has become so widespread that the Federal Bureau of Investigation estimated the total cost to businesses and government systems at $559 million annually. n7

A specific type of computer-based attack may qualify as either an act of state-sponsored "cyberwarfare" or a "cybercrime" depending on the relevant players. n8 This has led some to assert that we should do away with overly complex definitions and frameworks, and should instead assume that all attacks bear some form of state sponsorship.

METHODS, MOTIVATIONS, AND FORMS OF ATTACK.

While numerous definitions of cyberwarfare exist, former Special Advisor to the President on Cybersecurity Richard A. Clarke offers a useful place to start. He defines cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." n9 Ascertaining whether

any given attack qualifies as an instance of cyberwar versus the more garden-variety form of cyberattack, however, is fraught with difficulty, as the definition heavily depends upon knowledge of the attacker's intent, fellow conspirators, and identity. n10

Although types of attacks vary, generally three classes of activity make up the bulk of state-sponsored cyberwarfare: (1) attacks that are designed to spread propaganda (e.g., website vandalism and political spam bombing); (2) attacks that sabotage or disrupt software or hardware (e.g., viruses, botnets, DDoS attacks); and (3) attacks that steal or corrupt data (e.g., cyber-espionage, identity theft). U.S. counterintelligence officials speculate that there are about 140 different foreign intelligence organizations that use these techniques or otherwise attempt to infiltrate U.S. government and business information networks on a regular basis. n11 A brief timeline of confirmed notable attacks would include the following:

- 2001: A European Union "Special Committee of Inquiry" accused the United States, United Kingdom, Canada, Australia, and New Zealand of operating a large industrial espionage network against several EU member states and businesses. n12 The network, known as Echelon, was reportedly capable of monitoring wireless, e-mail, and fax data from around the world. Although no direct accusations of cyber-espionage were ever conclusively proven, according to the committee, strong evidence supported claims that the U.S. government tapped the phone lines of European aircraft maker Airbus Industries, which was negotiating a $6 billion contract with the Saudi Arabian government and national airline. n13
- 2004: Researchers at a major security firm detected a team of government-sponsored attackers in Guangdong Province, China, conducting cyber-espionage on networks owned by the U.S. Defense Information System Agency, the National Aeronautics and Space Administration, and the World Bank. The attacks - code-named "Titan Rain" - probed government websites hundreds of times each day and stole U.S. flight planning and other software. n14
- April 2007: Estonian government computer networks were inundated by a sustained DDoS botnet-style attack traced to Russian hackers. The attacks, which were initially thought to have been state sponsored, n15 flooded dozens of government servers, bogged networks down with bogus information requests, and blocked legitimate traffic, eventually leading the government to shut down a number of sites in order to handle the problem. n16
- April 2009: Reports began to surface in early 2009 that cyberspies had successfully penetrated the U.S. electrical grid and left behind software programs that could be used to cause future disruption of the system, according to current and former national-security officials. According to the same officials, the attacks occurred over a lengthy period and were pervasively spread across the United States. n17

Beyond the obvious damage and cost to systems and infrastructure, state-sponsored and other forms of organized cyberattack have the potential to affect a range of daily activities. For example, supervisory control and data acquisition (SCADA) systems, which monitor and regulate the operations of most critical infrastructure systems, such as power generation, water distribution, and traffic control, are often attractive targets. n18 SCADA systems automatically monitor and control physical processes based on data fed back. Most SCADA systems, however are routinely placed in remote, unsupervised locations, and are increasingly connected to local area networks or directly to the Internet.

POSSIBLE SOLUTIONS TO CYBERTHREATS

John C. Gannon, Chairman of the National Intelligence Council, noted that over the next fifteen years, the U.S. dependence on data and the free flow of information will also place the United States at an increased risk of foreign cyberthreats. n19 As such, a major challenge for the United States will be to find more effective means to boost awareness and responsiveness in order to reduce the threat of state-sponsored cyberattacks.

Awareness: Active vigilance is a starting point to keeping cyberattacks at bay. For example, both the government through the National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS) and private companies such as Verizon have developed information "cyber crisis centers," designed to track, analyze, share information about, and respond to potential attacks. n20 In 2004, the NCSD also established the National Cyber Alert

System (NCAS), a coordinated nationwide system managed by the U.S. Computer Emergency Readiness Team (US-CERT). n21

While monitoring is necessary, there is only so much that can be done. For example, Verizon's security center in Virginia reports that the company witnesses over one billion security events every day. Little can be done to thwart such attacks, as nearly three-quarters of those attacks come from outside the country, where the U.S. government's law enforcement powers are inadequate to meet the task. n22

Reduction: Another key is to work on reducing the likelihood that successful attacks can occur. To bolster networks in the United States, the government has been quietly cultivating some of its best security defenders from within major hacking groups. In 2009, for example, General Dynamics Information Technology put out a virtual "help wanted" sign on behalf of DHS, seeking individuals who could "think like the bad guy" and be able to understand the tools and techniques hackers use on a regular basis. n23 More recently, the Defense Advanced Research Projects Agency hired a former hacker, Peiter C. Zatko - known to the online world as "Mudge" - to manage the Strategic Technology Office, where he will evaluate funding for research projects to defeat cyber attacks. n24

Response: Although awareness and reduction of the likelihood of successful attacks are good starting points, they may not always be enough to prevent acts of cyberwarfare. Richard Clarke has noted that market forces and self-interest alone have produced lackluster results, and has called for a regulatory response to the cyberthreat in the form of standards and rules for when and how the standards should be implemented. n25

Others have advocated that a better approach is to simply do away with questions of whether or not a given attack is state sponsored at all. Former director of the National Security Agency General Michael Hayden (Retired), for example, has suggested that the United States forget about trying to determine whether a specific attack is state sponsored, and instead just hold nations responsible for all malicious activity that can be demonstrated to originate in them. n26

One proposed legislative response, recently introduced by Senators Joseph Lieberman (Independent-Connecticut), Susan Collins (Republican-Maine), and Thomas Carper (Democrat-Delaware), would be to grant the President broad emergency powers to force covered critical infrastructures, including telecom providers, financial institutions, and software companies, to "immediately comply with any emergency measure or action" DHS orders in cases of emergency or during acts of cyberwarfare. Senate bill 3480, introduced on June 10 and promptly dubbed by the press the Internet "Kill Switch Bill," n27 would also require covered critical infrastructures to develop and certify to a newly created "Director of Cyberspace Policy" sector-specific security measures and policies for handling cyber vulnerabilities. n28

Return to Text

n1 The "Critical Infrastructures" include structures, computer systems, and networks whose destruction or other compromise would have a debilitating effect on security, the national economy, public health or safety, or any combination thereof. Department of Homeland Security, Critical Infrastructure and Key Resources, http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

n2 McAfee In the Crossfire: Critical Infrastructure in the Age of Cyber War 4, available at http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf.

n3 A "botnet" or "bot network" is made up of large numbers of remotely controlled machines that have been compromised in some way, usually through malicious code delivered as part of an infected e-mail or website. Once infected, a PC will establish a secret communications link to a remote "botmaster" in preparation to receive new commands. The malicious code may also send back personal data and other information collected on the machine to the botmaster.

Attackers favor botnets because whole networks of compromised machines (or the tools to make them) can be readily purchased on the black market, require little or no technical expertise, and provide relatively unsophisticated attackers with an easy means to disrupt or block Internet traffic to victim computers through the power of distributed attack. Clay Wilson, Congressional Research Service Report for Congress RL32114, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 20 (Jan. 29, 2008), *available at* http://www.fas.org/sgp/crs/terror/RL32114.pdf.

n4 A "denial of service attack" (DoS) is an attack that is designed to make a particular computer or resource unavailable to its intended users. A distributed DoS (DDoS) occurs when a group of computers flood a single target for the same purpose. National Cyber Alert System, Cyber Security Tip ST04-015, Understanding Denial-of-Service Attacks, *available at* http://www.us-cert.gov/cas/tips/ST04-015.html.

n5 A Trojan horse attack consists of an "apparently useful program [that] contain[s] hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat." US CERT Advisory, CA-1999-02, Trojan Horses (Mar. 8, 1999), *available at* http://www.cert.org/advisories/CA-1999-02.html.

n6 For example, in March 2009, "Click," a BBC television show, acquired a botnet from an online chatroom and used it to demonstrate how botnets works. The program used the botnet to hijack almost 22,000 computers, and in turn launched a distributed denial of service attack against a backup computer network owned by security firm Prevx, which consented to the experiment. *Click: Is Your PC Doing a Hacker's Dirty Work*, BBC Networks (Mar. 12, 2009), *available at* http://news.bbc.co.uk/2/hi/programmes/click_online/7938503.stm.

n7 Press Release, Federal Bureau of Investigation, IC3 2009 Annual Report on Internet Crime Released (Mar. 12, 2010), *available at* http://www.fbi.gov/pressrel/pressrel10/ic3report_031210.htm.

n8 Nart Villeneuve, Blurring the Boundaries Between Cybercrime and Politically Motivated Attacks (Apr. 10, 2010), Internet Censorship Explorer, http://www.nartv.org/2010/04/10/blurring-the-boundaries-between-cybercrime-and-politicaly-motivated-attacks/.

For example, Villeneuve chronicles how the Kneber botnet was used both by criminal gangs to steal financial information and by another group to obtain sensitive government information on .mil and .gov accounts.

n9 Richard A. Clarke, Cyber War: The Next Threat to National Security and What to do About It (2010).

n10 Serge Krasavin, Computer Crime Research Center, What is Cyberterrorism? (Apr. 23, 2004), http://www.crime-research.org/analytics/Krasavin/. Estimates on criminal apprehension rates are equally depressing: One source claimed that only five percent of cybercriminals are ever arrested or convicted. Wilson, *supra* note 3, at 29.

n11 Wilson, *supra* note 3, at 12.

n12 Eur. Parl. Doc. (A5-0264) 103-06 (2001), *available at* http://www.fas.org/irp/program/process/rapport_echelon_en.pdf ; Martin Asser, *Echelon: Big brother without a cause?,* BBC News (July 6, 2000), *available at* http://news.bbc.co.uk/1/hi/world/europe/820758.stm.

n13 Eur. Parl. Doc. (A5-0264) 21; Paul Meller, *European Parliament Adopts 'Echelon' Report*, CNN.com (Sept. 7, 2001), *available at* http://archives.cnn.com/2001/TECH/internet/09/07/echelon.report.idg/. The State Department has denied such allegations.

n14 AFP, *Hacker attacks in US linked to Chinese military: researchers*, Breitbart (Dec. 12. 2005), at http://www.breitbart.com/article.php?id=051212224756.jwmkvntb&show_article=1.

n15 The Estonian attacks provide an excellent example of why the dividing line between state sponsorship and criminal act can be challenging. Although the attacks were thought initially to be a state-sponsored response to the Estonian government's decision to remove a Soviet-era war statue, later analysis revealed that there was no Russian government connection, and that the attacks were instead the product of a group of loosely associated attackers. Gadi Evron, *Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War*, 9 Geo. J. Int'l Affairs 121-26 (2008), *available at* http://www.bligoo.com/media/users/1/50369/files/Ataque%20Estonia.pdf.

n16 Carolyn Duffy Marsan, *Examining the Reality of Cyberwar in Wake of Estonian Attacks*, 24:33 Network World 24 (Aug. 27, 2007); Robert Vamosi, *Cyberattack in Estonia - What It Really Means*, CnetNews.com (May 29, 2007), http://news.com.com/Cyberattack+in+Estonia-what+it+really+means/2008-7349_3-6186751.html.

n17 Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, Wall St. J. Apr. 8, 2009, at A1, *available at* http://online.wsj.com/article/NA_WSJ_PUB:SB123914805204099085.html.

n18 *See* Scott Nance, *Debunking Fears: Exercise Finds 'Digital Pearl Harbor' Risk Small*, Defense Week (Apr. 7, 2003); Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Network*, Security Focus (Aug. 19, 2003), *available at* http://www.securityfocus.com/news/6767.

n19 John C. Gannon, **Remarks by John C. Gannon, Chairman, National Intelligence Council, to the Columbus Council on World Affairs (April 27, 2000),** ***available at*** https://www.cia.gov/news-information/speeches-testimony/2000/gannon_speech_05022000.html**.**

n20 The Verizon network in particular monitors activities coming in from over 150 countries around the world, across 700,000 miles of fiber optics. The NCSD oversees the Cyber Security Tracking, Analysis and Response Center, which conducts ongoing analysis of cyberspace threats and vulnerabilities, issues alerts and warnings for upcoming cyberthreats, and responds to major cybersecurity incidents. Terry McCarthy, *Cyber Attacks Jeopardize Superpower Status*, CBS Reports/USA Today (Apr. 22, 2010), *available at* http://www.cbsnews.com/stories/2010/04/22/eveningnews/main6422768.shtml.

n21 Specifically, the NCSD achieves its objectives by the coordinated efforts of three different programs: (1)The National Cyberspace Response System, which coordinates "cyber leadership, processes, and protocols that will determine when and what action(s) need to be taken as cyber incidents arise," including cybersecurity preparedness **and the NCAS; (2) the Federal Network Security branch, which serves as a single point of accountability for federal cyber-infrastructure security; and (3) cyber risk management programs, which "assess risk, prioritize resources, and execute protective measures critical to securing our cyber-infrastructure." www.dhs.gov/xabout/structure/editorial_0839.shtm.**

n22 McCarthy, *supra* note 20.

n23 Associated Press, *Wanted: computer hackers ... to help government* (Apr. 19, 2009), *available at* http://www.nationalterroralert.com/updates/2009/04/18/wanted-computer-hackers-to-help-government.

n24 Elinor Mills, *Hacker 'Mudge' gets DARPA Job*, C|Net News: InSecurity Complex (Feb. 10, 2010), http://news.cnet.com/8301-27080_3-10450552-245.html.

n25 Clarke initially denounced regulation as a means to combat attack. More recently, his view has changed, and he argues that regulation frequently represents the only real impetus for change in the IT industry. Richard Clarke, To Regulate or Not to Regulate? That Is the Question, Remarks at RSA Security Conference (Feb. 16, 2005).

n26 Kim Zetter, *Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible*, Wired.com (July 29, 2010), *available at* http://www.wired.com/threatlevel/2010/07/hayden-at-blackhat/#ixzz0x1Fq07WI.

n27 Declan McCullagh, *Lieberman defends emergency Net authority plan*, C|Net News (June 15, 2010), http://news.cnet.com/8301-13578_3-20007851-38.html.

n28 Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010), available at http://thomas.loc.gov/cgi-bin/query/z?c111:S.3480.

RELATED LINKS: The Cyber Security Research and Development Act is at
- 15 U.S.C. § 7401 et seq.

The National Institute of Standards and Technology research program on computer-system security is covered at
- 15 U.S.C. § 278h.

The Critical Infrastructures Protection Act of 2001 is codified at
- 42 U.S.C. § 5195c.

A criminal statute dealing withfraud and related activity involving a computer is at
- 18 U.S.C. § 1030.

See generally the LexisNexis Matthew Bender treatise
- Computer Law.

Also of possible interest is an article by Bruce Zagaris,
- World Summit Fixes on Proposed Cybercrime Prevention and Enforcement Initiatives, 26 International Enforcement Law Reporter 291 (July 2010).

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Carey Lening is an intellectual property, privacy, and technology attorney in Washington, DC.

Kirsten Koepsel is Director, Legal Affairs & Tax, Aerospace Industries Association in Arlington, VA.

Ron Weikers is Managing Partner of Weikers & Co. | Software-Law.com in Manchester, NH, and Adjunct Professor of Law at the University of New Hampshire School of Law. Any views expressed herein are solely the authors', and do not reflect the views of their respective employers.

3 of 18 DOCUMENTS

The Right of Privacy in Data Stored in "Cloud Computing"

2010 Emerging Issues 5252

The Right of Privacy in Data Stored in "Cloud Computing"

By Kirsten Koepsel, Carey Lening and Ron Weikers

August 10, 2010

SUMMARY: Cloud computing is an emerging area, but what privacy rights do users have? The Electronic Communications Privacy Act and its component, the Stored Communications Act, are difficult enough to apply to regular computers and e-mail. What are the rules for cloud computing? Do the statutes need to be amended? The authors analyze the issues, providers' practices, and the best practices for users.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Imagine being able to store in a "cloud" what you normally store on your personal computer or server. A user of a "cloud" can store documents, spreadsheets, photographs, business plans, tax and financial information, videos, health records, and sales numbers. n1 According to the research firm Gartner, cloud computing services revenue is expected to expand to $150.1 billion in 2013. n2 Cloud computing is "the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections." n3 Many daily Internet activities, such as e-mail, wiki applications, online tax preparation, and document sharing, are accomplished through "clouds" without the user realizing it. n4 Cloud computing services are sold on their convenience and accessibility to the user. What is unclear is whether there is a reasonable expectation of privacy in data stored in a "cloud."

Cloud computing

Google Documents, Amazon Web Services (AWS), and Mozy are examples of "cloud computing." n5 Google Docs allows the user to "create and share your work online," "upload your files from your desktop," and gain "access [from] anywhere." n6 With AWS a user can "requisition compute[r] power, storage, and other services --- gaining access to a suite of elastic IT infrastructure services as your business demands them." n7 Mozy allows the user to protect music, photos, and other computer files. n8 Users agree to terms of service prior to being able to access the "cloud" or store their documents or e-mails in the "cloud." Google's terms of service include a provision that "if Google disables access to your account, you may be prevented from accessing the Services, your account details or any files or other content which is contained in your account." n9 Google's terms of service also include references to content that the user posts, submits, or displays through the Services that allow Google

in performing the required technical steps to provide the Services to our users, [to] (a) transmit or distribute your

Content over various public networks and in various media; and (b) make such changes to your Content as are necessary to conform and adapt that Content to the technical requirements of connecting networks, devices, services or media. n10

AWS has similar terms of use and includes a paragraph that allows Amazon "the right but not the obligation to monitor and edit or remove any activity or content." n11 Unlike Google, AWS does not specifically define "content." Mozy has an End User License Agreement that is included in the installation portion of the MozyHome software. n12 Like AWS, Mozy does not define content.

Right of Privacy in information on computers

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated...." It is well settled that the right of privacy of individuals extends to protection of information on their own personal hard drives. n13 The expectation of a right of privacy was extended to Internet communications under the Stored Communications Act (SCA) n14 enacted as part of the Electronic Communications Privacy Act (ECPA) in 1986. n15 Under the SCA, two types of providers are regulated: of electronic communication services (ECS) n16 and of remote computing services (RCS). n17 Access to stored communications located at an ECS requires a search warrant for disclosure of the contents of electronic communications n18 in electronic storage n19 for 180 days or less to government entities. n20 Contents of electronic communications in electronic storage for more than 180 days at a RCS can be obtained by a search warrant, n21 a subpoena, n22 or a court order with prior notice to the subscriber. n23 Privacy protections such as a search warrant, subpoena, or court order apply only to public computers under the SCA. n24 An e-mail or a document is subject to different legal standards during its lifecycle. n25

The Ninth Circuit discussed electronic storage quite extensively in *Theofel v. Farey-Jones.* n26 As part of litigation, Farey-Jones sought access to ICA's e-mail via a subpoena of "all copies of emails sent to or received by anyone at ICA." n27 The Internet service provider, apparently not represented by counsel, explained that the amount of e-mail sought under the subpoena was substantial and eventually offered Farey-Jones a "free sample" of 399 messages. n28 Litigation ensued as to whether federal electronic privacy laws were violated. n29 As part of the analysis, the Ninth Circuit examined the legislative history of the SCA and what is "backup protection." The United States Department of Justice (DOJ) filed an amicus brief disputing the interpretation by the Ninth Circuit of the SCA. DOJ claimed that because "(B) refers to 'any storage of *such* communication,' it applies only to backup copies of messages that are themselves in temporary, intermediate storage under subsection (A)." n30 Ultimately, the Ninth Circuit decided that Farey-Jones had violated the SCA and that the "free sample" of messages had been stored "for purposes of backup protection" under *18 U.S.C. § 2510*(17(B).

Analysis

When the user puts information in the "cloud," she may not even know where the "cloud" is located or what expectation of privacy to have for her data and documents in the "cloud." n31 Information that the user puts in the "cloud" eventually "ends up on a physical machine owned by a particular company or person located in a specific country." n32 The stored information is then subject to the laws of the specific country in which the physical machine is located. n33 If the physical machine is located in the United States, then the SCA would govern the right of privacy in the contents. n34 If the user is lucky and the physical machine is located in the Ninth Circuit, she may receive different protection than for a machine located in another circuit. n35

At the same time, how the "cloud computing" service characterizes itself - as either an ECS or RCS - could impact what rights the user has in the data, and the wrong characterization could allow easier access, e.g. subpoena without notice to the customer. Most of the "cloud computing" companies, such as Google, Amazon, and Mozy, encourage long-term storage of e-mails and documents on their systems. But even then, it appears that the U.S. district courts and DOJ may not agree on what expectation of privacy the user would have in electronic storage. DOJ sees electronic

storage as "a split between two interpretations of 'electronic storage' -- a traditional narrow interpretation and an expansive interpretation supplied by the Ninth Circuit." n36 As a practical matter, federal law enforcement within the Ninth Circuit is bound by the Ninth Circuit's decision in *Theofel*, but law enforcement elsewhere may continue to apply the traditional interpretation of "electronic storage." n37

Is it time for the SCA (ECPA) to be updated to reflect the changes in technology since 1986? The Digital Due Process coalition is lobbying to have the ECPA updated. n38 The coalition believes that the "ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies." n39 Several members testified on May 5, 2010, before the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties at a hearing on Electronic Communications Privacy Act Reform. n40 Witnesses n41 testified that "cloud computing" is not "accorded the traditional protection of the judicial warrant" under the ECPA, n42 which has not been revised since 1986.

With the right of privacy unclear for data in "clouds," the customer would be wise to avoid storing information that he wishes to remain private or hope that he is able to meet the conditions that would require a subpoena or search warrant (e.g., don't store any e-mails over 180 days). The practitioner may also want to avoid storing data that is subject to other regulatory controls such as the Health Insurance Portability and Accountability Act (HIPAA) n43 or tax preparation laws, n44 particularly when the terms of service could allow the "cloud" supplier to monitor or make changes to the content. n45 The "cloud" provider would have little motivation to resist the subpoena as the user would. n46 But even then, the user needs to carefully review the terms of the agreement.

As Congressman Nadler stated in the press release on the proposed hearings for communication privacy reform,

The framers of the Constitution placed great emphasis on the right of all people to be "secure in their persons, houses, papers, and effects against unreasonable searches and seizures." The technology has changed since the 18th century, but the principle has not. Congress must ensure that however transmitted, and however stored, our communications are properly protected. n47

Return to Text

n1 Robert Gellman, World Privacy Forum, Privacy in the Clouds (Feb. 23, 2009) *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

n2 Bruce Gain, Cloud Computing & SaaS in 2010 (Jan. 1, 2010), *available at* http://www.processor.com/editorial/article.asp?article=articles/P3201/23p01/23p01.asp&guid=.

n3 Gellman, *supra* note 1, at 4.

n4 Electronic Privacy Information Center, Cloud Computing, http://epic.org/privacy/cloudcomputing.

n5 *See generally* Google Documents, *available at* https://www.google.com/accounts/ServiceLogin?service=writely&passive=1209600&continue=http://docs.google.com/?hl%3De a="">; Amazon Web Services, *available at* http://aws.amazon.com/ and http://aws.amazon.com/cloudfront/; Mozy, *available at* http://mozy.com/home.<>

n6 *See generally* Google Documents, *available at* https://www.google.com/accounts/ServiceLogin?service=writely&passive=1209600&continue=http://docs.google.com/?hl%3De a=""><a="">.<><>

n7 *See generally* Amazon Web Services, *available at* http://aws.amazon.com/what-is-aws/.

n8 *See generally* Mozy, *available at* http://mozy.com/home.

n9 Google, Google Terms of Service 4 (Provision of the Services) (Apr. 16, 2007), *available at* http://www.google.com/accounts/TOS?hl=en.

n10 < a=""><a="">*Id.*<><> at 11.3 (Content license from you). Content is defined in 8.1:

> You understand that all information (such as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images) which you may have access to as part of, or through your use of, the Services are the sole responsibility of the person from which such content originated. All such information is referred to below as the "Content".

n11 Amazon, Amazon Terms of Service, paragraph titled "Reviews, Comments, Communications and Other Content" (May 26, 2010), *available at* http://aws.amazon.com/terms/.

n12 Mozy, Mozy Terms, *available at* http://mozy.com/terms.

n13 J. Beckwith Burr, Wilmer Hale, The Electronic Communications Privacy Act of 1986: Principles for Reform 6 n.20 (citing *Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001)), available at* http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

n14 The SCA is also known as the Electronic Communications Privacy Act, depending on the commentator. *See generally* Orin Kerr, *A User's Guide to the Stored Communications Act - And a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1208 n.1 (2004)* (discussion of some names that SCA has been given).

n15 Pub. L. No. 99-508, *100 Stat. 1848.*

n16 *18 U.S.C. § 2510*(15) "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications."

n17 *18 U.S.C. § 2711*(2) "the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communication system."

n18 *18 U.S.C. § 2510*(12):

< a="">< a=""> <><>

"electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include -

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

< a="">< a=""> <><>

n19 *18 U.S.C. § 2510*(17): "electronic storage" means - (A) any temporary, intermediate storage of a wire or

electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

n20 *18 U.S.C. § 2703*(a).

n21 *18 U.S.C. § 2703*(b)(1)(A).

n22 *18 U.S.C. § 2703*(b)(1)(B)(i).

n23 *18 U.S.C. § 2703*(b)(1)(B)(ii).

n24 *18 U.S.C. § 2702.*

n25 *See* Burr, *supra* note 13, at 6 n.22 (citing Gellman, *supra* note 1). *See generally* U.S. Department of Justice Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence Manual (3d ed., Sept. 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf [hereinafter Searching and Seizing]. See specifically page 138 (Chapter 3, Stored Communications Act, Section F. Quick Reference Guide), *available at* http://www.cybercrime.gov/ssmanual/03ssma.html.

n26 *359 F.3d 1066* (9th Cir. 2003, amended 2004).

n27 < a=""><> a="">*Id.*<><>

n28 < a=""><> a="">*Id.*<><> The messages were posted on a website for viewing by Farey-Jones counsel.

n29 < a=""><> a="">*Id.*<><> The defendants also claimed violation of computer fraud statutes.

n30 < a=""><> a="">*Id.*<><> at 1076 (referring to the SCA).

n31 AWS, Google Documents, and Mozy do not provide a location of the "cloud" in their terms of service or agreement.

n32 Gellman, *supra* note 1, at 7.

n33 < a=""><> a="">*Id.*<><>

n34 *18 U.S.C. § 2701.*

n35 *See Theofel v. Farey-Jones, 359 F.3d 1066* (9th Cir. 2003, amended 2004).

n36 Searching and Seizing, *supra* note 24, at 123.

n37 Searching and Seizing, *supra* note 24, at 122-25 (C. Classifying Types of Information Held by Service Providers, 3. Contents and Electronic Storage).

n38 Digital Due Process at http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163. For a list of members, see http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163.

n39 http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

n40 http://judiciary.house.gov/hearings/hear_100505_1.html.

n41 < a=""><> a="">*Id.*<><> The witness list included: James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology; Albert Gidari Jr., Partner, Perkins Coie, LLP; Orin S. Kerr, Professor of Law, George Washington University Law School; and Annmarie Levins, Associate General Counsel, Microsoft Corporation. Written testimony is at http://judiciary.house.gov/hearings/hear_100505_1.html.

n42 James X. Dempsey, Electronic Communications Privacy Act Reform 2, *available at* http://judiciary.house.gov/hearings/pdf/Dempsey100505.pdf.

n43 Pub. L. No. 104-191, *110 Stat. 2033 (1996);* 45 C.F.R. Part 164. Business Associate Agreements would be required to transfer protected health information to a "cloud." *See also* Gellman, *supra* note 1, at 8-9.

n44 *26 U.S.C. §§ 6713*, 7216; 26 C.F.R §301.7216; *see also* Gellman, *supra* note 1, at 9-10.

n45 *See* Google Terms of Service, *supra* note 9.

n46 See Gellman, *supra* note 1, at 14-16 for a discussion of some data rules that could be in conflict with other regulations and laws.

n47 Press Release, Conyers, Scott, Nadler Plan Hearings on Communications Privacy Reform (Mar. 30, 2010), *available at* http://judiciary.house.gov/news/100330.html.

RELATED LINKS: For more complete discussions of the development and scope of the right of privacy, see generally
- Steve Posner, Privacy Law and the USA PATRIOT Act Chapter 2.

On search and seizure of computer information, see
- John Wesley Hall, Search and Seizure § 40.13;

- John Wesley Hall, Search and Seizure § 40.14.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Kirsten Koepsel is an intellectual property attorney and works as a Director, Legal Affairs & Tax, Aerospace Industries Association in Arlington, VA. **Carey Lening** is an intellectual property, privacy, and technology attorney in Washington, DC. **Ron Weikers** is Managing Partner of Weikers & Co. Software-Law.com in Manchester, NH, and Adjunct Professor of Law at Franklin Pierce Law Center in Concord, NH. Any views expressed here are solely the authors', and do not reflect the views of their respective employers.

4 of 18 DOCUMENTS

The Importance of Password Policies in Managing Information Security Risks

2010 Emerging Issues 5199

In the Matter of Twitter, Inc.: The Importance of Password Policies in Managing Information Security Risks

By J. ("Jay") T. Westermeier

July 15, 2010

SUMMARY: The Twitter consent order emphasizes the importance of password policies and management in connection with establishing and maintaining a comprehensive information security program. In this article, Jay Westermeier discusses the Twitter case and its importance in the evolution of "reasonable security" legal liability standards applicable to information security practices, especially in the context of password management practices.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: In the Matter of Twitter, Inc., n1 the Federal Trade Commission ("FTC") on June 24, 2010 entered into an agreement with Twitter, Inc. ("Twitter") containing a consent order. The FTC notes that this consent order is their thirtieth consent order relating to information security and their first information security order pertaining to social networking.

The Twitter consent order emphasizes the importance of password policies and management in connection with establishing and maintaining a comprehensive information security program. In this article we will discuss the Twitter case and its importance in the evolution of "reasonable security" legal liability standards applicable to information security practices, especially in the context of password management practices.

1. The Twitter FTC Complaint

In the Complaint, the FTC alleges that Twitter violated Section 5(a) of the FTC Act by falsely representing that it uses at least reasonable safeguards to protect user information and maintains at least reasonable safeguards to honor the privacy choices exercised by users, and by failing to provide reasonable and appropriate security to prevent unauthorized access to non-public user information and honor the privacy choices exercised by users who designated certain tweets as non-public.

The Complaint noted that since approximately July 2006, Twitter had operated a social networking website known as www.twitter.com. Using this Twitter website the Complaint states that users are able to send "tweets", which are brief messages of 140 characters or less to users who sign up to receive such messages via email and phone text. The Complaint observes that Twitter offers privacy settings through which a user may designate tweets as non-public. In addition, Twitter collects certain non-public user information, such as an email address, Internet Protocol ("IP")

addresses, mobile telephone number (for users who receive messages by phone), and a username for any Twitter account that a user has chosen to "block" from exchanging tweets with any user.

In the Complaint the FTC alleges that Twitter failed to provide reasonable and appropriate security to prevent unauthorized access to non-public user information and honor the privacy choices exercised by users designating certain tweets as non-public. As the result of Twitter's security failures Twitter failed to prevent unauthorized administrative control of the Twitter system. Many of Twitter's security failures related to passwords and other access controls.

Twitter allegedly failed to "establish or enforce policies to make administrative passwords hard to guess, including policies that: (1) prohibit the use of common dictionary words as administrative passwords; or (2) require that such passwords be unique - i.e., different from any password that the employee uses to access third-party programs, websites, and networks." n2

Twitter also allegedly failed to "establish or enforce policies sufficient to prohibit storage of administrative passwords in plain text in personal email accounts." n3

Another alleged password failure related to Twitter's failure to suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts. n4

There was also concern regarding the failure to change passwords periodically. Twitter allegedly failed to "enforce periodic changes of administrative passwords, such as by setting [these] passwords to expire every 90 days. n5

Three other alleged Twitter security failures were alleged relating to access controls. First, Twitter allegedly failed to "provide an administrative login webpage that is made known only to authorized persons and is separate from the login webpage provided to other users." Second, Twitter allegedly failed to "restrict each person's access to administrative controls according to the needs of that person's job." Third, Twitter allegedly failed to "impose other reasonable restrictions on administrative access, such as by restricting access to specified IP addresses." n6

The FTC Complaint alleges that between January and May 2009 intruders were able to exploit these password and access control security failures by Twitter on two occasions to obtain unauthorized administrative control of the Twitter system. By acquiring administrative control of the Twitter system the intruders were able to: (i) gain unauthorized access to nonpublic tweets and nonpublic user information, and (ii) reset any user's password and send unauthorized tweets from any user account. n7

In the Complaint the FTC references several particular instances relating to the actions the intruders were able to carry out based on the alleged security failures. On or about January 4, 2009 the Complaint states an intruder used an automated password guessing tool to derive an employee's administrative password, after submitting thousands of guesses into Twitter's public login webpage. The "guessed" password was a weak, lowercase, letter-only, common dictionary word. Using this password, the intruder was able to access non-public user information and non-public tweets for any Twitter user. The intruder was also able to reset user passwords. Some of these fraudulently -- reset user passwords were obtained by other intruders and used to send unauthorized tweets from user accounts, including: according to the Complaint, one tweet purportedly from Barack Obama, that offered his more than 150,000 followers a chance to win $500 in free gasoline, in exchange for filling out a survey. According to the Complaint unauthorized tweets were sent from eight other user accounts, including the Fox News account. n8

Another incident recited in the Complaint allegedly occurred on or about April 29, 2009 when an intruder was able to compromise a Twitter employee's personal email account by inferring the employee's Twitter administrative password, based on two similar passwords, which had been stored in the account, in plain text, for at least six months prior to the intruder's attack. Using this password, the intruder was able to access non-public user information and non-public tweets for any Twitter user and reset at least one user's password.

The Complaint contained two counts for alleged violations of the FTC Act. The first count related to false or

misleading representations pertaining to the security measures Twitter claimed to use to prevent unauthorized access to non-public user information. The second count related to Twitter's alleged failure to use reasonable and appropriate security measures to honor the privacy choices exercised by users. n9

2. The Twitter Consent Order

The Twitter Consent Order generally follows the FTC's earlier consent orders and settlement agreements in information security cases. In Part I of the consent order Twitter is prohibited from misrepresenting the security, privacy, confidentiality or integrity of any non-public consumer information which is defined broadly to mean non-public, individually-identifiable information from or about an individual consumer, including, but not limited to an individual consumer's: (a) email address; (b) Internet Protocol ("IP") address; (c) mobile telephone number; and (d) non-public communications made using Twitter's microbiology plant form. n10

Part II of the consent order requires Twitter to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, privacy, confidentiality, and integrity of non-public consumer information. Like the other FTC information security consent orders before this one Twitter's security program must contain administrative, technical, and physical safeguards appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the non-public consumer information. The consent order requires Twitter specifically to establish and maintain a comprehensive information security program with the five following components:

1. Accountability. Twitter must designate an employee or employees to coordinate and be accountable for the information security program.

2. Risk Assessment. Twitter must identify reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of non-public information or in the unauthorized administrative control of the Twitter system and assess the sufficiency of any safeguards in place to control these risks.

3. Safeguards and Testing. Twitter must design and implement reasonable safeguards to control the risks identified through risk assessment and regularly test or monitor the effectiveness of the safeguards' key controls, systems and procedures.

4. Service Providers. Twitter must develop and use reasonable steps to select and retain service providers capable of approximately safeguarding non-public consumer information they receive from Twitter, and require service providers by contract to implement and maintain appropriate safeguards.

5. Evaluation and Adjustment. Twitter must evaluate and adjust its information security program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its information security.

Part III of the consent order requires Twitter to engage an independent third-party professional to provide an assessment and report regarding Twitter's information security program certifying that it provides the protections required in Part II and that it is operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality, and integrity of non-public consumer information is protected. The consent order also includes reporting, compliance and record-keeping provisions.

3. Conclusions

The structure of the "comprehensive information security program" required of Twitter by the FTC is consistent with other consent orders and does not provide any new information. However, the Twitter case is instructive as to

certain practices relating to password policies and access controls. The Twitter case instructs that password policies should require: (1) use of strong passwords that are difficult to guess; (2) common dictionary words not be used as administrative passwords; (3) administrative passwords be unique and different from any password the employee uses to access third-party programs, websites, and networks; (4) administrative passwords not be stored in plain text in personal email accounts; (5) administrative passwords be suspended or disabled after a reasonable number of unsuccessful login attempts; and (6) administrative passwords be changed periodically by setting them to expire every 90 days. While these requirements reference for the most part administrative passwords they apply to passwords in general as well.

The lessons learned also apply to access controls. The administrative login webpage should be known only by authorized persons and be separate from the login webpage provided to other users. Each person's access to administrative controls should be restricted according to the needs of that person's job. Administrative access should be subject to reasonable restrictions, such as by restricting access to specified IP addresses.

The Twitter case references a number of important practices that should be adopted to improve information security protection, especially in the context of strengthened password policies and improving access controls. It is a very important case in the evolution of what constitutes "reasonable security" as a matter of law.

Return to Text

n1 In the Matter of Twitter, Inc., FTC File No. 0923093 (June 24, 2010).

n2 FTC Complaint, In the Matter of Twitter, Inc., FTC File No. 0923093 (available on FTC website), at 11.

n3 Id.

n4 Id.

n5 Id.

n6 Id.

n7 Id. at 12.

n8 Id.

n9 Id. at 13-17.

n10 FTC Agreement Containing Consent Order, In the Matter of Twitter, Inc., FTC File No. 0923093 (available on FTC website) at 3 and Part I.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Jay Westermeier is of counsel in the Reston, Virginia office of Finnegan, Henderson, Farabow, Garrett & Dunner, LLP. He is past President of the International Technology Bar Association (formerly known as the Computer Law Association); Life Fellow, American Bar Foundation; 2001 Burton Award for Legal Achievement; and a member or former member of the advisory boards for E-Commerce Law & Strategy, Computer Law Reporter, BNA's Computer Technology Law, BNA's Electronic Commerce & Law, GIS Law; The Commercial Law Advisor, Intellectual Property Counselor, Internet Law and Business, and Information Strategy: The Executives Journal. He is listed in Intellectual Asset Management magazine's "IAM250-The World's Leading IP Strategists" (2009-2010); The International Who's Who of Internet and e-Commerce Lawyers (2009-2010); The International Who's Who of Business Lawyers, 2008, 2010; Best Attorneys in America (Information Technology; 2003-2010); Virginia Super Lawyers (Intellectual Property; 2006-2010); Washington, D.C., Super Lawyers (Intellectual Property; 2007-2010); Super Lawyers Corporate Edition of Top Attorneys in Business Services (Intellectual Property; 2009), peer-rated "AV Preeminent[TM]" by Martindale-Hubbell, and many other honorary lists of distinction.

5 of 18 DOCUMENTS

The Impact of Social Media and Web 2.0 Services on the Federal Government

2010 Emerging Issues 5188

The Impact of Social Media and Web 2.0 Services on the Federal Government

By Carey Lening, Kirsten Koepsel and Ron Weikers

July 9, 2010

SUMMARY: Carey Lening, Kirsten Koepsel, and Ron Weikers discuss the burgeoning use of social media and Web 2.0 by the federal government. Just what tools is the government using? What is on the horizon? What are the risks? What guidance is there? What do managers, employees, and citizens need to do?

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: The use of online tools that integrate technology, social interaction, and content creation - commonly known as "social media" n1 - has transformed from the pastime of a few Internet enthusiasts in the early 1990s to one that currently occupies twenty-two percent of the collective online activity of hundreds of millions of users. n2 Internet users now spend a total of almost two billion hours on social media and blog sites yearly. n3 Through the use of tools such as Blogger, n4 YouTube, n5 and Twitter, n6 people around the world can now easily create and share information in ways that were previously relatively unknown.

Government, which is often slow to adopt new technologies, has recently begun to embrace social media, seizing the opportunity to connect with the public through tools that range from syndicated feeds and real-time updates via Twitter to mashups n7 and microblogs. n8 This has also led to involvement by government technologists, lawyers, and administrators as they grapple with ensuring compliance with existing laws, rules, and regulations amidst ever-changing technologies.

GOV 2.0

To date, two dozen federal governmental organizations, including the General Services Administration (GSA), the Environmental Protection Agency (EPA), the Department of Defense (DoD), and most branches of the military employ social media in some way. n9 While most agencies have taken a cautious approach by focusing on more "traditional" output channels of social media - e.g., blogs, syndicated feeds, and Twitter updates - others, such as the Department of Homeland Security (DHS), GSA, and U.S. Army have embraced the "social" in social media head-on.

For example, in 2009, DHS launched "Our Border," described as an "open online collaborative platform ... to address border issues you care about." n10 The site frequently features links to upcoming events, blog posts, and other commentary from agency officials and people concerned about border issues. n11

The GSA has also begun to use social-media tools, and has issued guidelines and policies regarding new technology. One tool, set to launch in the fall, is the much-anticipated FedSpace, which has been described as "a secure intranet and collaboration workspace for Federal employees and contractors." n12 According to the GSA, FedSpace will allow federal employees to communicate across agencies, and will incorporate various Web 2.0 tools, including wikis n13 and blogs, file-sharing, and a governmentwide employee directory. The agency also currently maintains a Twitter account n14 allowing members of the general public to keep track of social-media technologies used by the various different agencies.

Others are setting their sights even higher. The U.S. Army is currently looking for contractors to develop a "Second Life"-styled virtual world to simulate real-world peacekeeping operations and provide an online training ground for soldiers. n15 The goal of the virtual world, which is currently in the planning stages, in combination with advanced artificial intelligence, will be to support thousands of individual characters, or avatars, as they test possible peacekeeping strategies prior to applying them in the real world.

There are also a number of so-called "Gov 2.0" websites that have been developed independently of any particular agency, the most notable of which is GovLoop.com, which was created in 2008 as a place for members of the government community to gather, connect, and share information. n16 The site has over 30,000 local, state, and federal government users, and allows members to create and share their own blogs, group pages, and videos.

POTENTIAL PITFALLS OF SOCIAL MEDIA

Although the use of social media and Web 2.0 tools may facilitate active and relatively costless social engagement between the government and the public at large, such use may come with a number of additional risks, particularly for services not directly maintained by the government. By opening up networks to allow for public access on tools designed to offer a collaborative space, agencies potentially leave themselves vulnerable to problems ranging from the inadvertent disclosure of sensitive or personal information by employees, to undue influence and access, or even an increased threat of spreading viruses and malware to protected machines. Accordingly, agencies interested in exploring social-media solutions should carefully weigh the costs against the benefit of working with such tools prior to using any free or commercial solutions.

Disclosure of Personal or Secret Information:

One of the trickiest and most persistent problems that government faces is the disclosure of private or secure information by employees. In April 2010, for example, the website Wikileaks.org made headlines when it released classified military footage titled "Collateral Murder," showing an Army helicopter strike that claimed the lives of several Iraqis and two Reuters cameramen. n17 According to hacker-turned-journalist Adrian Lamo, Specialist Bradley Manning confessed via online chat to leaking the footage, n18 along additional documents and materials from the State Department. n19

While the problem of disclosure is hardly new, n20 social-media tools - particularly tools incorporating geo-location and other location-awareness features, such as FourSquare.com n21 or Twitter - only increase the likelihood that important information may be leaked to the public. n22 As more agencies begin to incorporate social-media tools into their daily collaborative activities, in order to mitigate against information leaks, appropriate policies and practices must be in place governing who can speak and what can be said on behalf of the given agency.

Trojans, Malware, and Phishing:

Another major concern that agencies must contend with involves malware and phishing attacks, particularly those that occur via social-media channels. In some respects, combating the threat of malicious code or unauthorized access is more challenging because today's attackers harness the very validation and trust frameworks that social networking sites were designed to create.

In April 2009, the "Mikeyy" worm, named after its seventeen-year-old creator, Mike Mooney, infected Twitter over the course of three days. The worm encouraged users to click on a link to a rival service, causing the worm to infect the victim's account and also spread to the victim's followers. n23 Similar attacks have also become a regular feature against Facebook users, n24 leading Facebook to require all application developers to verify their accounts with the site. n25

From a policy perspective, it may prove more challenging for governmental bodies to simply issue an edict forbidding users from clicking on or opening links sent from friends, colleagues, or associates. It may be necessary for the government to combine education with policy and technology antivirus tools, e-mail scanning and website verifiability to combat such threats. It will also be important for each agency to carefully regulate and control the types of access users will be able to have, and how much control they may have over their personal machines.

MITIGATING RISK THROUGH EFFECTIVE POLICY AND GUIDANCE

Despite the pitfalls, the approach taken by most agencies thus far has been to embrace rather than avoid social media and Web 2.0 technologies. However, while use continues to grow, so far only a handful of agencies have articulated publicly available social-media policies and/or guidelines governing social-media use. n26

One of the best-known examples of a comprehensive social-media policy is the guideline and handbook issued by the GSA. n27 The GSA's approach is notable in that, rather than define protocols and behavior for specific social-media platforms, the documents apply to "various activities that integrate technology, social interaction, and content creation." n28 The GSA guidelines note that communications shared over social media are assumed to be in the public domain, and that officials should have "no expectation of privacy" when making posts on social networking sites. n29 The GSA guidelines also provide clear, easy-to-follow language on what employees should and should not disclose. For example, Section 5(f), which governs copyright and sensitive information, cautions the following:

Respect copyright, fair use and financial disclosure laws. Always protect sensitive information, such as protected acquisition and personally identifiable information. Do not publish or report on conversations that are meant to be pre-decisional or internal to GSA unless given permission by management.

The GSA's *Social Media Handbook* in some respects is even more comprehensive, and covers everything from activities on external sites to intellectual property, privacy, and even lobbying. n30

However, one factor that remains somewhat elusive is whether social-media and Web-2.0 providers are obligated to comply with various governmental laws on persistent cookies and privacy. n31 The Office of Management and Budget has released a number of guidelines that discuss the role of government and social-media tools. For example, OMB's *Guidance for Agency Use of Third-Party Websites and Applications*, issued in June 2010, modifies an earlier memorandum n32 that limited the use of third-party websites that collected "personally identifiable information" (PII) on members of the public. Under the new guidance, agencies are now permitted, subject to certain limitations, n33 to "use third-party websites and applications to engage openly with the public." The guidance is notable in that it requires agencies using third-party sites to also provide comparable alternatives to allow open communication with the agency. n34

Along these lines, there is also the question of whether the Privacy Act of 1974 n35 governs services such as Facebook and Twitter. The Act, like the OMB memorandum and the GSA *Guidance*, requires executive-branch agencies (and agency contractors n36) to comply with certain practices regarding the use of PII. n37 Specifically, federal agencies that maintain PII must do so in an accurate, timely, and complete manner. n38 The Act also limits the kinds of information that agencies can collect, n39 and imposes certain use limitations on that information. n40

However, while language in these sources and the various amended terms of service agreements all clearly articulate the agencies' various responsibilities, there is little or no mention of what requirements service providers may be bound to, or even whether a service provider is considered a contractor under language governing the roles of

government contractors. If social-media and Web-2.0 providers are considered "contractors" under the various agency guidance documents or the Privacy Act, a serious review and revision of existing terms of service agreements made between such sites and the government may be necessary. n41 In the end, it may even force substantial changes to the way many of the websites handle PII, or their interactions with the government sector generally.

In addition to strong agreements between providers and the government, effective (and repeat) training programs focused on the use of social media will be necessary. As technological tools evolve, so too do the tools of harm. In the end, government employees, as well as service providers, will need to become more aware, and more proactive about warding off security threats, whether they come in the form of a malicious piece of code or an inadvertent disclosure. Comprehensive, clear, and continued education will be necessary to ensure that this culture becomes ingrained.

Return to Text

n1 "Social media," in the context of this article, refers to media that are primarily designed for social interaction, and use highly accessible (frequently no-cost or low-cost) and scalable publishing techniques. By contrast, the phrase "Web 2.0" refers to web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration over the Internet.

n2 Nielsen News, *Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online*, June 15, 2010, http://blog.nielsen.com/nielsenwire/online_mobile/social-media-accounts-for-22-percent-of-time-online/.

n3 *Id*.

n4 Blogger.com is a platform that allows users to create their own "weblogs" for free.

n5 YouTube.com is a website that allows users to upload, share, and view user-created videos.

n6 Twitter.com is a social networking and blogging system that enables users to share information by sending text-based posts of up to 140 characters.

n7 "Mashups" combine data, music, media, software, or a combination of these elements from two or more

sources to create a new work or service.

n8 "Microblogs" differ from traditional blogs in that content is usually much smaller; it may consist of short sentence fragments, images, or embedded videos and links.

n9 Many sites, including the U.S. Department of Housing and Urban Development, U.S. Agency for International Development, and DHS use third-party sites, such as Facebook or Twitter, or streaming news feeds commonly known as "RSS" (Really Simple Syndication). Others, such as the National Aeronautics and Space Administration, have established their own "Facebook-like" secure social pages. John S. Monroe, *Spacebook Brings Secure Social Networking to NASA*, Federal Computer Week, June 17, 2009, http://fcw.com/articles/2009/06/17/web-nasa-spacebook-social-media.aspx.

n10 "Our Border: Purpose," http://ourborder.ning.com/notes/Purpose.

n11 Examples of citizen-created topics include the increased violence affecting border towns, and how Customs and Border Protection, the agency responsible for border security, can be improved.

n12 General Services Administration, FedSpace: New Social Intranet for Federal Employees and Contractors, http://www.usa.gov/webcontent/resources/tools/fedspace.shtml.

n13 Wikis are multi-user, collaborative blogs comprising interlinked web pages.

n14 http://twitter.com/GovNewMedia.

n15 Elizabeth Montalbano, *Army to Develop Virtual World for Training*, InformationWeek, June 8, 2010, http://www.informationweek.com/news/government/enterprise-architecture/showArticle.jhtml?articleID=225500028. According to the FedBizOpps.gov website, which tracks open bids for government contracts, the Army is not alone. Over the last six months, both the U.S. Air Force and the U.S. Department of Agriculture have solicited bids from contractors to create their own virtual-world environments.

n16 GovLoop.com, Frequently Asked Questions, http://www.govloop.com/page/frequently-asked-questions.

n17 Ellen Nakashima, *Online contact says he turned in analyst who wanted to leak information*, Washington Post, June 8, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/07/AR2010060702381.html?nav%3Demailpage&sub=AR (print version is *Army intelligence analyst held in Wikileaks incident,* Wash. Post, June 8, 2010, at A1). Manning was charged on July 6, 2010. Nathan Hodge, *Soldier Faces Charges Over Wikileaks Video*, WSJ.com, July 6, 2010, http://online.wsj.com/article/SB10001424052748704862404575350943573085092.html.

n18 Kevin Poulsen & Kim Zetter, *I Can't Believe What I'm Confessing to You: The Wikileaks Chats*, Wired.com, June 10, 2010, http://www.wired.com/threatlevel/2010/06/wikileaks-chat/.

n19 Kevin Poulsen & Kim Zetter, *Wikileaks Commissions Lawyers to Defend Alleged Army Source*, Wired.com, June 11, 2010, http://www.wired.com/threatlevel/2010/06/wikileaks-to-lamo/.

n20 See Wikipedia, *United States Government Security Breaches*, http://en.wikipedia.org/wiki/United_States_government_security_breaches#2000s.

n21 FourSquare.com (http://foursquare.com) is a location-based software tool and website that encourages users to "check-in" at venues and compete with others for awards.

n22 In 2009, the DoD pondered banning access to all social media sites for military personnel, citing the increased risk of information disclosure and threat of malicious code being released on military systems. However, a September 2009 draft proposal strongly urged a more relaxed policy towards social media. *See* Noah Schactman, *Draft Policy Would Ok Troops' Tweets*, Wired.com, Sept. 29, 2009, http://www.wired.com/dangerroom/2009/09/draft-policy-would-ok-troops-tweets/.

n23 Ian Paul, *Twitter Worm: A Closer Look at What Happened*, Network World, Apr. 14, 2009, http://www.networkworld.com/news/2009/041409-twitter-worm-a-closer-look.html.

n24 *See* Gregg Keizer, *Rogue Facebook apps launch 'beach babes' attack*, Computerworld, May 22, 2010, at http://www.computerworld.com/s/article/9177158/Rogue_Facebook_apps_launch_beach_babes_attack; Ellen Messmer, *Facebook's 'Secret Crush' Malicious Widget Tricks Users*, Network World, Jan. 3, 2008, http://www.networkworld.com/news/2008/010308-facebook-secret-crush.html; Stan Schroeder, *WARNING: Facebook Clickjacking Attack Spreading Through News Feed*, Mashable.com, May 21, 2010, http://mashable.com/2010/05/21/facebook-malware-dont-laugh/.

n25 See Facebook Developer Blog, June 2, 2010, http://developers.facebook.com/blog/post/386.

n26 Chris Boudreaux has compiled a wonderful resource of local, state, federal, and nonprofit organizations that actively use and employ social-media policies: Chris Boudreaux, Social Media Governance, http://socialmediagovernance.com/policies.php. While Boudreaux's list includes only eight federal agencies, most agencies have opted to work with the GSA's Office of Citizen Services to craft appropriate agreements that address agency-specific concerns with existing free Web 2.0 providers. A full list of the complying agencies can be found at https://forum.webcontent.gov/?page=TOS_TYagencyPOCs. According to the site, "[the] GSA led this effort because the existing standard Terms of Service on most social media sites do not comply with federal law and in many ways are not compatible with agency expectations and practices. Working with providers to amend their standard TOS for federal users eliminates those problems." https://forum.webcontent.gov/?page=TOS_FAQs. A list of providers who offer free social media products under so-called "federal-friendly" terms is available at https://apps.gov/cloud/advantage/main/start_page.do.

n27 GSA, CIO 2106.1, GSA Social Media Policy (July 17, 2009), *available at* http://www.gsa.gov/graphics/staffoffices/socialmediapolicy.pdf; GSA, CIO P2106.2, GSA Social Media Handbook (July 17, 2009), *available at* http://www.gsa.gov/graphics/staffoffices/socialmediahandbook.pdf.

n28 GSA, CIO 2106.1, GSA Social Media Policy 1.

n29 *Id*. at 2.

n30 GSA, CIO P2106.2, GSA Social Media Handbook, Chs. 3, 10, 11 & 14. The GSA Guidelines offer detailed guidance for creating a GSA-sponsored blog, including the steps necessary to establish, name, host, and post on them. GSA Social Media Handbook, Ch. 2.

n31 See OMB, M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf; GSA, CIO P2106.2, GSA Social Media Handbook. Both the *Guidance* and the *Handbook* say that such provisions apply to "executive branch departments and agencies ('agencies') and their contractors."

n32 OMB, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22/.

n33 According to the guidance, prior to making use of third-party services each agency should evaluate (and should continually monitor) how factors such as the third-party website's privacy policy, use of external links, embedded applications, and information collection affect existing privacy obligations under the Privacy Act of 1974, *5 U.S.C. § 552a* and its notes. Where "personally identifiable information" is collected, agencies will also be required to perform an analysis, or "Privacy Impact Assessment," on how such PII is handled by the agency and any privacy risks that may be involved. Guidance for Agency Use of Third-Party Websites 4-5. Finally, agencies will be required to post both the PIA and updated privacy policies on their respective websites and as part of the third-party application or website. *Id*. at 5-6.

n34 *Id*. at 3.

n35 *5 U.S.C. § 552a*.

n36 *5 U.S.C. § 552a(m)*. "Government Contractors.--When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system."

n37 *5 U.S.C. § 552a(e)(1)*-(7); OMB, Guidance for Agency Use of Third-Party Websites 4-5; *see* GSA, CIO P2106.2, GSA Social Media Handbook 12 (Ch. 11).

n38 *5 U.S.C. § 552a*.

n39 Section 552a(e)(1)-(7). Agencies must limit the collection and retention of information about

individuals. Specifically, the agencies must:

- Collect only that which is relevant and necessary to the agencies' purposes and functions.
- Collect information directly from the subject individual to the extent practicable.
- Give the individual a Privacy Act statement each time they request individually identifiable information.
- In certain instances, refrain from collecting an individual's Social Security number and information relating to the exercise of First Amendment rights.

n40 *5 U.S.C. § 552a(b)(1)*. Once information is obtained, the agency must gain the individual's permission before disclosing records to employees other than "officers and employees ... who have a need for the record in the performance of their duties."

n41 For example, in response to an April 30, 2009, Freedom of Information Act request by the Electronic Privacy Information Center to the GSA (*available at* http://epic.org/privacy/socialnet/gsa_foia_4-30-09.pdf), EPIC noted that contracts disclosed between the government and the various sites did not address privacy obligations required of the companies providing service; rather, they pertained only to the government's obligations. EPIC Forces Disclosure of Government Contracts with Social Media Companies, Privacy Terms Missing, Aug. 12, 2009, http://epic.org/privacy/socialnet. According to a letter issued by the GSA to EPIC, to date "no specific Web 2.0 guidance [on this issue] currently exists." E-mail from Zachariah I. Miller, Intergovernmental Solutions Division, GSA, to EPIC (May 29, 2009), http://epic.org/privacy/socialnet/gsa/files/GSA_EPIC_Letter.pdf.

RELATED LINKS: For more on cyberlaw, visit the Lexis.com

- Cyberlaw area of law page.

For more on privacy implications, go to the Lexis.com

- Privacy area of law page.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Carey Lening is an intellectual property, privacy, and technology attorney in Washington, DC.

Kirsten Koepsel is an intellectual property attorney and works as a Director, Legal Affairs & Tax, of the Aerospace Industries Association in Arlington, Virginia.

Ron Weikers is Managing Partner of Weikers & Co. Software-Law.com in Manchester, New Hampshire, and Adjunct Professor of Law at Franklin Pierce Law Center in Concord, New Hampshire. Any views expressed here are solely the authors', and do not reflect the views of their respective employers.

6 of 18 DOCUMENTS

Whether the Federal Government Should Regulate the Protection of Personal Data

2010 Emerging Issues 5105

Whether the Federal Government Should Regulate the Protection of Personal Data

By Kirsten Koepsel, Carey Lening and Ron Weikers

June 10, 2010

SUMMARY: The area of data security has been so dynamic the last several years, with so many different states propounding different standards, that it may be time for the federal government to set a uniform standard for protecting personal data. The authors discuss various laws and standards, including existing and proposed federal measures.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Over the past several years, States have become increasingly proactive about data breaches n1 and enacted laws or issued regulations on privacy and data-security requirements. To date, forty-six States require some form of notification to affected persons when a security breach occurs and unencrypted personal information has potentially been accessed by an unauthorized person. n2 Although the measures vary in their scope and severity of consequence, most require that any covered entity suffering a data breach notify an affected party (usually a state resident) "immediately" or without "unreasonable delay" upon first becoming aware of the breach. n3

As technological advances and cost-cutting measures continue to shift the locus of personal information from filing cabinets to electronic databases, state governments rush to respond by enacting tougher laws that impose additional encryption n4 and heightened information-security requirements on businesses that maintain or use sensitive or personally identifiable customer information. A comparison of several of the most recent state measures, however, shows that these requirements may be challenging for businesses to comply with. Moreover, the large diversity of state requirements creates the real possibility that entities that store personal information about residents of multiple states may be required to comply with roughly fifty different data-security and privacy requirements. An important question thus comes to mind: Should the federal government create a uniform standard and regulate all personal/sensitive information with regard to encryption, user authentication, and authorization?

State Requirements

Washington State is the most recent State to update its data-privacy laws. n5 In March, the state legislature passed H.B. 1149, which requires that any "processor or business" that fails to take "reasonable care" to protect against unauthorized access to computerized "account information" (i.e., a Washington-State resident's credit- or debit-card information) must reimburse an affected financial institution for the costs incurred in replacing or reissuing new credit or debit cards to the affected customers. n6 The law excuses from liability any processor, business, or vendor that

encrypts customer data, and any entity that is otherwise "certified compliant" with current payment-card-industry security standards. n7

Nevada also enacted a recent law governing encryption of electronic data. n8 In March 2009, Nevada passed S.B. 227, which extends encryption protection to credit-, debit-, or charge-card information. n9 However, the act, which revises Nevada's identity-theft law, not only defines the standards for encryption, but also requires "appropriate management and safeguards of cryptographic keys" to be used by covered entities. n10 Security measures for personal information of Nevada citizens are to be "reasonable ... to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." n11

By contrast, Massachusetts issued a broad regulation in 2009, which strives for a risk-based approach to information security and the protection of personal information. n12 Unlike for Washington and Nevada, protection under the Massachusetts regulation extends to any entity that owns or licenses personal information about a Massachusetts resident, both in paper and in electronic form, including "laptops or other portable devices." n13 Although the definition of encryption n14 is rather weak, encryption is required for "all transmitted records ... that will travel across public networks ... transmitted wirelessly" n15 and for "all personal information stored on laptops or other portable devices." n16

For States requiring encryption, effective management of cryptographic keys is still difficult. n17 Keys are used to decode encrypted data and must match if the encrypted data is to be readable. Moreover, if a given key is lost or corrupted, the data is lost. These factors are further complicated by the fact that current technology requires that each key be managed independently until the industry is able to develop standardized communications between encryption systems. n18

Federal Law Requirements

A number of federal laws impose upon data owners and licensees affirmative duties of security and protection for specific classes of people or data. But unlike for some States, there is no all-encompassing federal law for the general class of personally identifiable information. For example:

- The Fair Credit Reporting Act requires the protection of credit-related financial information. n19
- The Safeguard Rule of the Gramm-Leach-Bliley Act requires financial institutions to safeguard customer information. n20
- The Children's Online Privacy Protection Act of 1998 guards against the involuntary collection and use of personal data regarding children under the age of thirteen. n21
- The Health Insurance Portability and Accountability Act of 1996 requires health providers to protect the security and privacy of individually identifiable health information, but it does not require encryption. n22

Protection of personal information held by the federal government itself has been codified by the Privacy Act of 1974 n23 and the Federal Information Security Management Act ("FISMA") of 2002. n24 The purpose of the Privacy Act was to "provide certain safeguards for an individual against an invasion of personal privacy by requiring . . . adequate safeguards are provided to prevent misuse of such information." n25 Under the Privacy Act, governmental agencies must "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats...." n26

FISMA was enacted to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources...." n27 FISMA also requires that "each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices." n28

OECD and EU Requirements

By comparison to the United States, the Organization for Economic Co-operation and Development ("OECD") has

long recognized a need to protect personal information and data. The OECD issued recommendations in 1980, and determined early on that the "development of automatic data processing, which enables vast quantities of data" to be transmitted within seconds across borders and across continents, "made it necessary to consider privacy protection." n29

The OECD recommendations are based on seven principles governing the security and privacy of personal data. n30 The security principle requires that "[p]ersonal data should be protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data." n31 All seven principles are incorporated into the 1995 European Union ("EU") Directive "on the protection of individuals with regard to the processing of personal data and on the free movement of such data." n32

Personal data under the EU Directive is more expansive than in the United States, and includes "factors specific to [the individual's] physical, physiological, mental, economic, cultural or social identity." n33 The EU Directive also includes an article on security of processing information "to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access," but does not mandate how such security is accomplished. n34

Analysis

For practitioners who have clients that are owners, licensees, or processors of data, the morass of state, federal, and international requirements could represent a data-management nightmare. The relatively new Washington, Nevada, and Massachusetts measures promote data privacy and security, but do not set consistent standards. Just as encryption requirements vary among them, so do the storage media to be protected.

It should be noted that all three of these state measures can be read to impose data and security requirements not only on businesses located within the respective states, but also on entities located outside of the respective jurisdictions that maintain residents' personal data. n35 The practical consequences are that the States regulate interstate commerce by imposing requirements across state lines, thereby encroaching upon Congress's interstate commerce powers. n36

At the federal level, the Privacy Act applies only to the federal government. FISMA applies not only to the government but also to contractors possessing "any information system used or operated by an agency or a contractor of an agency or other organization on behalf of an agency" and used for national security, including intelligence activities. n37 An April 2010 Office of Management and Budget memo now requires agencies to report monthly on their monitoring of security-related information, including security training, identity management, and access. n38

The EU, for its part, recognized the possibility of an obstructed flow of personal data if each country was allowed to set its own security and privacy laws without guidance. n39 To compensate, the EU adopted an approach that favors harmonization of at least some baseline standards for protection across the member states. n40 A 2002 study reviewing implementation of the Directive specifically examined its different articles, including Article 17, Security of Processing. n41 The study found that the EU members generally "stipulate the data security and confidentiality requirements set out in Arts. 16 and 17 of the Directive, often in terms identical or close to those used in those articles." n42

So, what should be done in the United States? If state action is not coordinated and the federal government has thus far avoided imposing encryption or authentication requirements on business, then disparate state measures could become *de facto* policy across the country by virtue of private entities holding data of multiple states' residents. n43 Perhaps the EU Directive's or the OMB Memo's approach represents a good direction for the federal government. They present different options: The EU Directive, for example, leaves it up to each of the member states to determine specific provisions on the protection of data, whereas the OMB Memo specifically details a standard for encryption, user authorization, and prevention of unauthorized access.

On May 4, 2010, Representative Rick Boucher released a draft bill for public comment that aims to preserve privacy protections for individuals, both on- and offline. n44 If enacted, the law would "require notice to and consent of

an individual prior to the collection and disclosure of certain personal information relating to that individual." n45 The draft legislation also requires disclosure of privacy practices, collection and use of information, and disclosure of information to unaffiliated parties. n46 The Federal Trade Commission would be responsible for implementation and enforcement.

Another bill, introduced by Senator Dianne Feinstein on January 6, 2009, entitled the "Data Breach Notification Act," would require data holders who experience a breach to notify data owners. n47 A data holder would be required to obtain U.S. Secret Service certification if the holder seeks exemption from the notification requirement due to potential hindrance of a law enforcement investigation. n48 The bill would also presume no risk of misuse of breached databases that have been encrypted, thus implicitly imposing an encryption requirement. n49

Currently, the United States is heading down two paths - one for government information-security systems and one for commercial information-security systems. They do not appear to be converging on similar requirements for encryption, user authentication, and authorization.

Return to Text

n1 The Privacy Rights Clearinghouse maintains a comprehensive overview and chronology of data breaches and the relevant state laws that have developed in response. The *Chronology of Data Breaches* tracks *reported* breaches from 2005 to the present and is available at http://www.privacyrights.org/ar/ChronDataBreaches.htm (last modified May 28, 2010).

n2 For a list of States with security-breach laws, including the District of Columbia, Puerto Rico, and the Virgin Islands, please see the National Conference of State Legislatures' State Security Breach Notification Laws page at http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/I (last modified Apr. 12, 2010). *See also* Scott & Scott, State Data Breach Notification Laws, http://www.scottandscottllp.com/main/uploadedFiles/resources/Publications/state_data_breach_notification_law.pdf (last modified Oct. 20, 2009). Alabama, Kentucky, New Mexico, and North Dakota have not enacted any form of data-security breach law.

n3 Scott & Scott, *supra* note 2.

n4 *See, e.g.*, 201 Mass. Code Regs. § 17.02 (a/k/a 201 C.M.R. § 17.02).

n5 See H.B. 1149, 2009-2010 Leg., 61st Legs. 2010 Reg. Sess. (Wash. 2010). HB 1149 will be effective July 1, 2010.

n6 H.B. 1149, Sec. 2(3)(a).

n7 H.B. 1149, Sec. 2(2). Under the act, "encrypted" is defined as "enciphered or encoded using standards reasonable for the breached business or processor taking into account the business or processor's size and the number of transactions processed annually."

n8 *2009 Nev. 1603*, 2009 Nev. ALS 355 (codified at Nev. Rev. Stat. §603A.215, *available at* http://www.leg.state.nv.us/NRs/NRS-603A.html).

n9 Nev. Rev. Stat. § 603A.215; subsection 5(a) defines "data storage device."

n10 Nev. Rev. Stat. § 603A.215(5)(b)(1) and (2). The statute requires that any encryption technology used be set "by an established standards setting body, including but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology...." Data collectors must also comply with the current version of the Payment Card Industry Data Security Standard, available at http://www.pcisecuritystandards.org. See also the National Institute of Standards and Technology Special Publication *Guideline for Implementing Cryptography in the Federal Government*, (SP) 800-21, at http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf, for additional cryptographic guidelines.

n11 Nev. Rev. Stat. § 603A.210(1).

n12 201 Mass. Code Regs. § 17.03. The regulations, first published in 2008, became fully effective March 1, 2010, after hearings and amendments. They were based on Mass. Ann. Laws, ch. 93H, §§ 1 to 6, enacted in 2007.

n13 201 Mass. Code Regs. §§ 17.02 & 17.04.

n14 201 Mass. Code Regs. § 17.02.

n15 201 Mass. Code Regs. § 17.04(3).

n16 *Id.* at 17.04(5).

n17 *See* Beth Pariseau, *Lack of Data Encryption Standards Hampering Storage Security*, SearchStorage.com (Aug. 20, 2009), at http://searchstorage.techtarget.com.au/articles/34929-Lack-of-data-encryption-standards-hampering-storage-security; *see also* Alan Earls, *KMIP Encryption Key Management Standard Close to Adoption*, SearchStorage.com (July 30, 2009), at http://searchstorage.techtarget.com.au/articles/34271-KMIP-encryption-key-management-standard-close-to-adoption (providing an overview of Key Management Interoperability Protocol).

n18 Earls, *supra* note 17.

n19 *15 U.S.C. § 1681* et seq.

n20 *15 U.S.C. §§ 6801-6809*.

n21 *15 U.S.C. §§ 6501*-6506.

n22 Pub. L. No. 104-191, *110 Stat. 1936 (1996).*

n23 *5 U.S.C. § 552a*.

n24 E-Government Act of 2002, Pub. L. No. 107-347, title III, *116 Stat. 2899* (among other things, adding *44 U.S.C §§ 3541* to *3549*).

n25 Pub. L. No. 93-579, § 2(b), *88 Stat. 1896* (codified as a note to *5 U.S.C.S. § 552a*).

n26 *5 U.S.C. § 552a(e)(10)*.

n27 *44 U.S.C. § 3541*.

n28 *44 U.S.C. § 3545*; *see also* Federal Information Security Management Act ("FISMA") Implementation Project at http://csrc.nist.gov/groups/SMA/fisma/index.html (overview of implementation of FISMA and security controls).

n29 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980), *available at* http://www.oecd.org/documentprint/0,3455,en_2649_34255_1815186_1_1_1_1,00.html.

n30 *Id*. The seven principles are notice, purpose, consent, security, disclosure, access, and accountability.

n31 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *supra* note 29.

n32 See Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

n33 *Id*. at art. 2(a).

n34 *Id*. at art. 17.

n35 *See, e.g.*, 201 Mass. Code Regs. § 17.05(1).

n36 *See* U.S. Const., art. 1, § 8.

n37 *44 U.S.C. § 3542(b)(2)(A)*.

n38 OMB Memorandum for the Heads of Executive Departments and Agencies, M-10-15 (April 21, 2010), at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-15.pdf. Monthly reporting will begin January 1, 2011.

n39 Council Directive 95/46/EC, art. 8, 1995 O.J. (L 281) 31.

n40 However, compliance with the law has not always been achieved. *See* European Union Agency for Fundamental Rights, Data Protection in the European Union: The Role of National Data Protection Authorities (May 7, 2010), at http://fra.europa.eu/fraWebsite/attachments/Memo-data-protection-070510_en.pdf.

n41 Douwe Korff, EC Study on Implementation of Data Protection Directive 95/46/EC (2002), at http://ssrn.com/abstract=1287667. *See generally* http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm (studies since 1997 on data protection).

n42 Korff, *supra* note 41, at 142.

n43 Nevada law does recognize that "if a state or federal law requires a data collector to provide greater protection to records . . . and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provision of this section." Nev. Rev. Stat. § 603A.210.

n44 H.R. __, [Staff Discussion Draft] (May 3, 2010) at 1, *available at* http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf.

n45 *Id*. (purpose clause).

n46 Press Release, Congressman Rick Boucher, Boucher, Stearns Release Discussion Draft Of Privacy Legislation: Measure Confers Privacy Rights On Internet Users (May 4, 2010), at http://www.boucher.house.gov/index.php?option=com_content&view=article&id=1957:boucher-stearns-release-discussion-draft

n47 S. 139, 111th Cong. § 2 (2009).

n48 S. 139, § 3(a).

n49 S. 139, § 3(b)(2).

RELATED LINKS: For more complete discussions of the development and scope of the right of privacy, see generally
- Steve C. Posner, Privacy Law and the USA PATRIOT Act, Ch. 2.

For more information on state data-privacy measures, see
- Joseph J. Lazzarotti on State Data Privacy and Security Laws, 2008 Emerging Issues 1879 (updated in 2010).

Keep current with the following publications, available on Lexis.com:
- David Bender, Computer Law 2A.11;
- Mealey's Litigation Report: Data Identity and Security;
- LexisNexis 50 State Comparative Legislation/Regulations: Non-Customer Personal Data Security-Breach and Notice.

For information related to HIPAA, see
- LexisNexis Matthew Bender's treatise Medical Records Privacy Under HIPAA;
- Heather Fesko & Philip McGuigan, HIPAA Security Breaches, 2009 Emerging Issues 4065 (July 2009).

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Kirsten Koepsel is an intellectual property attorney and works as Director, Legal Affairs & Tax, for the Aerospace Industries Association in Arlington, VA.

Carey Lening is an intellectual property, privacy, and technology attorney in Washington, DC.

Ron Weikers is Managing Partner of Weikers & Co. Software-Law.com in Manchester, NH, and Adjunct Professor of Law at Franklin Pierce Law Center in Concord, NH. Any views expressed here are solely the authors', and do not reflect the views of their respective employers.

7 of 18 DOCUMENTS

Increased FDA Internet Scrutiny of Web Traffic Tools

2010 Emerging Issues 5097

Increased FDA Internet Scrutiny of Web Traffic Tools: Internet Sales Require Special Attention to Regulatory Compliance

By Paul McGrady, Justin Prochnow, Alex Furman and Alan Sutin

June 4, 2010

SUMMARY: The Internet makes it easier for fraudsters and unethical individuals and companies to take advantage of victims and flaunt the law on a broad scale. However, even legitimate businesses and advertisers are sometimes either unaware of the law or believe that the law applies only partially or not at all for actions on the Internet. Attorneys at Greenberg Traurig break down the rules to avoid unwanted FDA scrutiny.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: The Internet not only allows businesses to target large numbers of customers around the world, it makes it easier for fraudsters and unethical individuals and companies to take advantage of victims and flaunt the law on a broad scale. One of the areas where Internet technologies have been frequently used to take advantage of consumers is in the area of drugs and nutritional products. The sale of such products is highly regulated, but the applicable laws, rules and regulations frequently are not followed when these products are sold on the Internet. Much of the Internet activity is blatant fraud. However, even legitimate businesses and advertisers are sometimes either unaware of the law or believe that the law applies only partially or not at all for actions on the Internet, with the result that they inadvertently find themselves in legal hot water.

Legitimate businesses frequently encounter legal problems because they do not understand how Internet technologies work, and they entrust their search engine optimization (SEO) to consultants who are given almost free reign to craft domain names, meta tags and other website traffic generation devices. However, federal agencies have become very sophisticated in the use of these technologies and are increasing the enforcement against companies that engage in these technologically advanced Internet activities.

For example, some search engines "rent" search terms that trigger advertisements to the highest bidder - even when search terms do not appear in the advertisement text and regardless of who owns the trademark rights to the search terms. Registrars sell domain names containing the marks of others or containing medical claims without first reviewing the registration request to see if the domain name would violate prior trademark rights or FDA regulations if put to use in conjunction with the domain name registrant's business. Often times, it is the SEO consultant who is selecting meta tags to mark a website, search terms to trigger advertisements, and domain names to drive both direct navigation and search engine traffic to a website. Such consultants may be expert at increasing traffic counts to a website, but may have

little appreciation for the legal consequences of their actions.

The FDA's Enforcement on the Internet: *U.S. v. Tony T. Pham and Techmedica Health, Inc.*

A recent case involving the fraudulent sale of dietary supplements provides an illustration of how one company attempted to use advanced Internet technologies to avoid detection and prosecution by the FDA. Following several years of investigation resulting in a 2008 indictment, Tony T. Pham pleaded guilty on July 2, 2009 to his role in a conspiracy to fraudulently market dietary supplements over the Internet through his company, Techmedica Health, Inc. While the heart of the FDA's investigation and indictment was the fraud perpetrated in the marketing of dietary supplement products that made illegal claims that the products could diagnose, treat, mitigate, cure or prevent diseases, the case also serves as verification of the FDA's increased scrutiny of Internet activity and awareness of technological advances employed by companies to sell products.

In the course of its investigation, the FDA uncovered Pham's use of various technologies to advance the scheme, including the use of "mirror image technology" pursuant to which any attempt to access the company's website that originated from an FDA computer would be directed to a "sanitized" version of the websites that did not contain the illegal and fraudulent claims. The indictment against Pham also alleged that the company improperly used meta tags to guide consumers to the company's websites. As part of his guilty plea, Pham agreed to forfeit $12 million in profits from 2005 and 2006 from the products and is facing up to 25 years in federal prison.

The FDA's Broad Review of Internet Activity

The case against Pham and Techmedica evidences the FDA's increasing vigilance over websites promoting products in the drug, medical device, food and beverage, dietary supplement and cosmetic industries. In 2000, the FDA began issuing "cyber" warning letters via the Internet to companies and/or individuals that maintain websites promoting products that the FDA perceives make claims contrary to law. In determining whether a product is properly marketed and sold, the FDA looks to the intended use of the product. Recently, the FDA has found evidence of intent to sell products as drugs in non-traditional areas, including technological means used to guide Internet traffic to a particular website, in addition to the standard media, such as the product labels and labeling.

The FDA has identified certain meta tags and domain names that indicate an intent to sell a particular product based on its use or effectiveness for treating or preventing a disease or a disease condition. For example, the FDA has warned of the use of meta tags such as "high blood sugar", "diabetes" or "hyperglycemic", when these meta tags direct consumers to a website promoting dietary supplements. As another example, the FDA has found evidence of intent to sell products as drugs in the use of meta tags such as "skin cancer treatment" or "melanoma", when these meta tags have directed consumers to a website promoting a skin cream product. The FDA has also identified domain names with symptom or treatment-related terms as evidence of intent to sell products as drugs. Domain names such as "www.cholesterblock.com", "www.altcancercream.com", and "www.glycogone.com" were previously identified by the FDA in warning letters as further evidence in support of the FDA's contentions that the true intent of the company was to sell products as drugs.

Responding to the Increased Scrutiny

The recent FDA investigations into Internet activity indicate the FDA's belief that its regulations lose little in translation between enforcement on product shelves and enforcement on the Internet. The FDA has determined that advertising using meta tags and domain names can evidence the intent of a company to sell a product for a particular purpose in much the same way as a product label or magazine advertisement. The recent FDA attempts to limit meta tag usage and domain name selection are likely to be followed by other agencies, which can be expected to impose additional restrictions on the technological tools of marketing on the Internet.

With this increased scrutiny on Internet activities, businesses that market online need to guide and review their marketing efforts carefully. Businesses should audit the practices of their SEO and other Internet consultants, especially

if businesses are marketing products or services that are regulated by an agency, and ensure that appropriate safe guards also appear in their service agreements with such SEO consultants. Counsel knowledgeable about a particular agency's regulations and counsel experienced in Internet law can guide these contract negotiations and audits of SEO practices and keep businesses compliant with agency regulations, even in the face of the enhanced agency scrutiny.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

This *Commentary* was prepared by **Paul McGrady** in Greenberg Traurig's Chicago office and author of *McGrady on Domain Names* (a Matthew Bender-LexisNexis title), **Justin Prochnow** and **Alex Furman** in Denver, and **Alan Sutin** in New York. Questions about this information can be directed to:

* **Paul McGrady -** 312-456-8426 (mcgradyp@gtlaw.com)

* **Justin Prochnow -** 303-572-6562 (prochnowjj@gtlaw.com)

* **Alex Furman -** 303-685-7417 (furmana@gtlaw.com)

* **Alan Sutin -** 212.801.9286 (sutina@gtlaw.com)

8 of 18 DOCUMENTS

What Advertisers Need to Know About Running Contests and Advertising

2010 Emerging Issues 5050

What Advertisers Need to Know About Running Contests and Advertising on Facebook and Twitter

By Ed Chansky, Alan Sutin, Kristen Fancher and Andy Moore and Tracie Chesterman

May 20, 2010

SUMMARY: Recently, both Facebook and Twitter have enhanced their advertising and promotions guidelines. This Commentary describes the primary features of Facebook's new rules regarding contests and sweepstakes, as well as the key concerns for companies using Facebook and Twitter for advertising purposes.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: I. Introduction

Over the last few years, social media websites and services have exploded in growth. Facebook has transformed from a networking tool primarily used by college students in the United States to having over 350 million users worldwide as of November 2009. In 12 months, Twitter has gone from having approximately 3.5 million unique visitors a month to having over 23 million unique visitors to its website as of October 2009.

Given their tremendous growth, both Facebook and Twitter have become appealing and increasingly important advertising and promotional tools for companies. In fact, some companies have even hired full-time employees and "twinterns," whose jobs involve sending messages about special promotions via Facebook and Twitter.

Recently, both Facebook and Twitter have enhanced their advertising and promotions guidelines. This *Alert* describes the primary features of Facebook's new rules regarding contests and sweepstakes, as well as the key concerns for companies using Facebook and Twitter for advertising purposes.

II. Facebook's New Promotions Guidelines

Facebook's new Promotions Guidelines, which became effective on November 4, 2009, distinguish between ***administering*** or operating a contest, sweepstakes or other similar promotion through a Facebook page (regulated), and merely ***publicizing*** a promotion through Facebook (generally allowed). The Facebook Guidelines can be found at www.facebook.com/promotions_guidelines.php.

A. Administering a Promotion Through Facebook

A sponsor ***administers*** a promotion through Facebook if it operates or allows access to any aspect of a contest,

sweepstakes, or other similar promotion via its Facebook page, including collecting entries, conducting a drawing, and/or notifying winners.

There are two ways to do this: one permissible, the other not.

1. Permissible Promotions

Under the Guidelines, a sponsor may administer a promotion through Facebook only by using a third-party application developed specifically to host the promotion and that operates independently from Facebook's own "native" functionality. The following conditions apply:

a. The sponsor must be an existing Facebook advertiser with a Facebook account representative.

b. The promotion must be approved at least seven days in advance by Facebook.

c. The third-party application must be placed either under a separate tab on the sponsor's page or under a separate web address.

d. The entry page and official rules must state that Facebook does not sponsor the promotion and is not liable for the promotion.

e. Entry is limited to persons 18 or older.

f. The promotion must not involve or relate to gambling, alcohol, tobacco, firearms, dairy products, gasoline, or prescription drugs.

g. Foreign countries that would prohibit or restrict the promotion must be voided.

Subject to the above conditions, the sponsor may require entrants to post photos or other content to the third-party application (i.e., not directly to a Facebook page) as part of the entry process, collect contact information through the third-party application to notify winners, and limit participation to people who are already "Fans" of the sponsor's page, if the sponsor so wishes.

2. Prohibited Promotions

A clear purpose of the Guidelines is to distance Facebook from responsibility or liability for the conduct of any advertiser sweepstakes, contest or other promotion. Accordingly, a sponsor ***cannot*** use "native" Facebook functionality (as opposed to a third-party application) to administer a promotion, and the following promotional practices are prohibited:

a. Automatic entry by becoming a "Fan" of the sponsor's page.

b. Requiring posting of a photo or other content directly to a Facebook page (rather than to a third-party application page).

c. Requiring an entrant to sign up for a Facebook account.

d. Notifying winners through Facebook.

B. Publicizing a Promotion Through Facebook

Merely ***publicizing*** the existence of a sweepstakes, contest or other similar promotion that is conducted at a completely different location, such as the advertiser's own website, is generally permitted and does not require approval from Facebook. Such advertising may occur via Facebook "wall posts," on the sponsor's page, or via status updates on

that page.

C. CAN-SPAM and General Considerations for Facebook Promotions

A sponsor may be held responsible for not complying with the CAN-SPAM law as the sender of a forwarded electronic message if the sponsor compensates the consumer (including giving additional sweepstakes entries) to "refer-a-friend" or otherwise to forward a commercial electronic message. The issue can get complicated on Facebook where users have several different ways to share information. Some of those ways merely involve posting information to the user's own "wall" or profile page, which arguably should not be covered by CANSPAM.

Other methods involve sending messages to friends in a manner more akin to traditional e-mail, which poses a greater risk of triggering the CAN-SPAM laws. This is an emerging area where careful attention to the technology, as well as legal advice, are important.

In addition to its specific Promotions Guidelines, Facebook also has general guidelines for advertising. Most of Facebook's Advertising Guidelines are based on common sense, but also include requirements to abide by certain privacy and other standards established by Facebook. Facebook's complete Advertising Guidelines can be found at www.facebook.com/ad_guidelines.php.

III. Twitter's Advertising Policies and Best Practices

Unlike Facebook, Twitter has not yet created specific guidelines for sweepstakes, contests or similar promotions. In response to concerns about unbridled spam, however, Twitter has adopted an evolving set of principles and general guidelines that affect advertising, particularly use of automated messaging. (See "Automation Rules and Best Practices Guidelines" at http://twitter.zendesk.com/forums/26257/entries/18311.)

Twitter normally ***allows*** the following forms of advertising:

a. Promoting your own business or website.

b. Posting unpaid customer recommendations.

c. Sending sponsored or compensated links and updates that you manually post or approve.

d. Messages that are sponsored by a third party, if you manually post or approve each such message before transmission.

The following types of advertising are ***prohibited*** on Twitter:

a. Pre-scheduled advertising messages.

b. Repeated posting of the same advertisements.

c. Failing to disclose the fact of compensation or sponsorship when posting a message that has been paid for by a third party.

As a general principle, companies advertising on Twitter are well-advised to proceed cautiously and to be cognizant of the emerging guidelines and customs for advertising via social media.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Ed Chansky - 702.599.8016 (chanskye@gtlaw.com)

Alan Sutin - 212.801.9286 (sutina@gtlaw.com)

Kristen Fancher - 678.553.2457 (fancherk@gtlaw.com)

Andy Moore - 702.599.8037 (mooread@gtlaw.com)

Tracie Chesterman - 212.801.6957 (chestermant@gtlaw.com)

All are attorneys with Greenberg Traurig, LLP

Principles of the Law of Software Contracts, as Adopted (May 19, 2009)

2010 Emerging Issues 5008

Chapter 3: PERFORMANCE

By The Council of The American Law Institute

May 19, 2009

SUMMARY: No text.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Chapter 3

PERFORMANCE

TOPIC 1

INDEMNIFICATION AND WARRANTIES

Summary Overview

Implied Intellectual Property Indemnification: In transactions involving the transfer of software, the transferee reasonably relies on the validity of the rights granted by the transferor. Virtually always, these include the right to use the software; sometimes, they include other rights such as copying, modifying, and/or further distributing the software in one form or another. If the transferor does not have the authority to grant the rights contained in the agreement, the transferee's bargain is severely undermined, if not entirely worthless. Thus, it is important to safeguard the transferee's bargain by providing it with some assurance that its rights under the agreement will be meaningful and, if not, that it will be made whole.

However, it can be quite difficult for software providers to warrant against intellectual property infringement, particularly patent infringement. Patents on software are both difficult to find and ubiquitous. Additionally, in the open-source context, transferees commonly understand that the code is provided without a warranty against infringement. Requiring such a warranty in that context could frustrate the collaborative development effort that has characterized the open-source movement. Even in cases in which commercial software firms provide software, companies may be unwilling to provide the warranty because the software in one product may be comprised of code from many sources.

The U.C.C. and UCITA addressed this set of issues by providing a disclaimable warranty of noninfringement. Many, if not most, transferors commonly disclaim this warranty. Thus, many if not most, transferees have no assurance that they will be made whole in the event they lose the right to use the software because of an infringement claim.

This approach raises perhaps only theoretical concerns in the consumer context. Particularly between a commercial transferor and a consumer, the commercial transferor has the advantage (even if slight especially with respect to patents) in knowing whether its product infringes an intellectual property right. By permitting disclaimer of the warranty, the U.C.C. and UCITA effectively place the risk of loss on the consumer. But the lack of suits for infringement against consumers suggests that, indeed, this risk is largely theoretical.

In balancing all of these considerations, § 3.01 provides for indemnification of the transferee under the conditions specified in the Section and permits the transferor to disclaim the indemnification. The Section essentially respects freedom of contract. The approach departs from U.C.C. Article 2 and its counterpart in UCITA. As noted above, both of those Acts provide a warranty of noninfringement. The widespread disclaimer of this warranty suggests that another approach may be preferable.

Section 3.01 also provides certain remedies (some akin to warranty protection) to transferees who have provided monetary compensation for the software if a court enjoins the software's use or holds it infringing. These remedies apply if and to the extent that they have not been excluded in the agreement. These remedies may provide some protection to transferees who may lose the right to use a product held infringing. The transferee must give notice of its desire for a remedy and the choice of remedy is within the sole control of the transferor. Transferor remedial options include purchasing the right to allow the transferee to continue using the software, modifying or replacing the software so that it is noninfringing, or giving the transferee a refund and possibly paying damages.

Although this approach is different from that of the U.C.C. and UCITA, as with those acts, § 3.01 respects the customs that have developed in the industry. The hope is that by changing the applicable default rule from a warranty to the narrower obligation of implied indemnification, more transferors will be willing to offer a tailored indemnity rather than disclaiming liability altogether. Of course, nothing in the Section precludes a transferee from negotiating express warranties and remedies.

To the extent that transferors routinely disclaim indemnity, courts should be particularly concerned if infringement suits against consumers based on their exercising rights under the agreement were to become widespread. In such cases, courts might opt to use public policy or unconscionability to analyze whether a disclaimer should be enforced.

The Principles do not imply indemnification by the transferor if the transferor did not receive money or the right to payment of a monetary obligation in exchange for the software. This would be the case for many collaborators in the open-source community who routinely exchange code without requiring monetary compensation in return. Open-source developers often are a large, diverse group and individual contributors may not have access to counsel to assist them in evaluating copyright or trade-secret claims or searching for patents, many of which may be invalid. An indemnification duty therefore may have a chilling effect on participation in open-source projects.

Quality Warranties: Software continues to grow in complexity and importance and the ramifications of its failure, not surprisingly, have also become more serious. n1 Rules relating to the quality of software therefore are controversial because both software transferors and copyholders have much at stake. Software transferors assert the inevitability of defects n2 and the necessity of insulating themselves through disclaimers and remedy limitations from inordinate liability. n3 Business copyholders point out the potential for catastrophic losses if defective software grounds their business to a halt. n4 Consumers complain about the uselessness of defective software.

Generally, most people agree that software products are complex, with defects almost inevitable, so that the law should not require perfection. n5 Some quality protection for copyholders is not unreasonable, however. At present, most courts apply Article 2 warranty law to software exchanges, either directly, on the theory that software constitutes

goods, or by analogy. n6 Most of these cases involve exchanges of custom software between businesses in situations where the software failed spectacularly. Few of these decisions have focused on the nature of software and its differences from goods. n7

U.C.C. Article 2 enforces express warranties, creates implied quality warranties, and authorizes disclaimers of warranties and limitations of remedy. n8 In both consumer- and business- software markets, transferors generally take advantage of the warranty-disclaimer and remedy- limitation tools offered by Article 2, so that copyholders rarely enjoy much quality protection. n9 Although debatable, critics of the Uniform Computer Information Transactions Act (UCITA) claim that the Act narrows warranty protection still further.1 n10 These Principles follow the treatment of warranties in Article 2, but with appropriate accommodations for special problems pertaining to software,1 n11 some of which may not yet have but are likely to surface in litigation. For example, the question of the meaning of a warranty and whether the warranty is broken must take into account software's tendency to contain "bugs."1 n12 Further, questions of disclaimer in the software context must accommodate freedom of contract *and* policing for market failures. The latter problem arises most often in consumer or small-business contracts containing take-it-or-leave-it standard terms that nobody reads,1 n13 but it can also affect deals between software transferors and larger business copyholders that may lack skills pertaining to and general understanding of software technology or may lack sufficient bargaining power.1 n14 The latter businesses may expect disclaimers, but they may be unfairly surprised to learn that all of the representations, promises, and sales documentation presented to them may be worthless if their software is defective.

Although many provisions of UCITA are controversial, its treatment of warranties is helpful in identifying and responding to some of the distinctive issues raised by software contracts. Accordingly, these Principles also adopt what is best and most effective about UCITA's coverage of warranties, while establishing the Principles' own domain. For example, UCITA's treatment of the meaning of the implied warranties of merchantability and fitness for a particular purpose mirrors Article 2, but usefully adapts to software exchanges.

On the other hand, in some respects UCITA is too dependent on Article 2's treatment of warranties. In fact, some Article 2 warranty rules incorporated in UCITA are hopelessly confused and controversial. For example, UCITA adopts the U.C.C.'s "basis of the bargain test" for express warranties, which has created neither uniformity nor clarity in sales-of-goods law. These Principles therefore forge a new approach that drops the basis-of-the-bargain concept in favor of a test based on whether the copyholder could reasonably rely on the words or conduct.1 n15 But the idea is not radical. The original drafters of the U.C.C. probably had this approach in mind when they created the basis-of-the-bargain test.1 n16

These Principles avoid or clarify other Article 2 warranty imbroglios as well. For example, the Principles clarify Article 2's approach to the creation of express warranties in U.C.C. § 2-313 and their negation in U.C.C. § 2-316(1). Under § 2-313, written and oral statements pertaining to the quality of the software, descriptions, samples, and models may create express warranties. Section 2-316 directs courts to construe language or conduct creating such warranties and language or conduct negating them as "consistent" unless unreasonable.1 n17 By directing courts to seek a consistent interpretation of conflicting language, such an approach seems to endorse a seller's practice of creating express warranties on the one hand and disclaiming them on the other. But, in practice, courts have not applied § 2-316 very coherently, which should be no surprise given the vagaries of the statutory language.1 n18

These Principles clarify the approach when language of warranty and negation exist by enforcing the express warranty in transfers of both custom-designed and general-market software if a reasonable person in the transferee's shoes would not expect a disclaimer.1 n19 Custom-software transfers may involve sophisticated business copyholders who can bargain for terms, such as a term that allows testing of the software before acquiring it. In addition, such businesses may be sophisticated about the nature of software and knowledgeable about how to protect themselves, for example, by insisting on detailed maintenance agreements that may take the place of or supplement warranties as the primary mode of recourse for bugs in the software.2 n20 These businesses may expect express warranty disclaimers, which are therefore enforceable. But, as already noted, some business copyholders may lack the skills and know-how pertaining to software technology and the bargaining power to receive adequate protection.2 n21 These copyholders

may be unfairly surprised to learn that their transferor does not intend to stand by its representations, promises, and other express warranties. In addition, advocates of copyholders of generally available software assert the need for quality protection, especially because these copyholders typically cannot inspect their software and must rely on the transferor's competence and representations.2 n22 These Principles protect such transferees from unexpected disclaimers of express warranties.

Implied quality warranties. These Principles retain the implied warranty of merchantability in both customized and generally available software exchanges. Transferors argue, however, that the merchantability warranty (warranting that the software is "fit for its ordinary purpose") makes little sense because software programs cannot be compared and resemble a unique service.2 n23 This argument is more persuasive in custom markets where the copyholder's purpose may be unique. Still, even such software should satisfy average standards in the trade in terms of speed, compatibility with hardware and other software, reliability, and functionality.2 n24 If even these indicia are difficult to evaluate, the merchantability warranty amounts only to an obligation to transfer software of average quality and workmanship. Software that does not operate much of the time, or that corrupts other programs would be easy examples of unmerchantable software.2 n25 Further, transferors can disclaim the warranty if uncomfortable with the software's unpredictability or potential liability.2 n26

General-market software, on the other hand, usually has an ordinary purpose shared by its users, such as word processing or virus protection, and the case for an implied warranty of merchantability is strong here.2 n27 However, in response to the concern of software transferors that excessive potential liability would stifle development of new software, including, for example, free software distributed over the Internet,2 n28 transferors can disclaim the merchantability warranty under
§ 3.06. Transferors' disclosure obligations set forth in Chapter 2, Topic 2, of these Principles, the requirements for disclaimers in this Chapter, and the policing tools of unconscionability and public policy help protect copyholders from unfair disclaimers of implied warranties.2 n29

These Principles also retain the implied warranty of fitness for a particular purpose.3 n30 Under Article 2, an implied fitness warranty arises if the seller, having reason to know why the buyer wants the goods, "selects or furnishes" the goods for the buyer, who relies on the seller's "skill or judgment."3 n31 This fitness warranty applies both to general-market software selected, for example, by a sales agent and custom-designed software, but it is especially important in the latter case because copyholders often rely on the transferor's superior skills and expertise. A fitness warranty also may apply when the transferor selects software to run on the copyholder's already-existing hardware and the copyholder relies on the transferor's decision. The transferor warrants that the software will be compatible with the transferee's already-existing system, not that the software is free from defects. The transferor can also disclaim the fitness warranty.

Finally, under these Principles, software transferors who receive money for the software are liable for material defects of which they are aware at the time of the transaction if they do not disclose them.3 n32 This warranty is mandatory.3 n33 Such liability is comparable to the common-law disclosure duty of contracting parties. Warranties can also arise from a course of dealing or usage of trade.

Other law. Both Article 2 and UCITA defer to federal and state consumer-protection warranty law, although critics of UCITA worry that UCITA's recognition of licensing and software's intangible nature might "pull[] software outside of the scope of the Magnuson-Moss Warranty Act and of analogous" state consumer-protection laws.3 n34 Magnuson-Moss is important, for example, because sellers governed by it cannot disclaim implied warranties if they make an express one.3 n35 These Principles increase the likelihood that courts will apply Magnuson-Moss to packaged software because nothing turns on transferors labeling their transactions as licenses.3 n36

Open-source software and quality warranties. These Principles do not carve out special quality warranty rules for the transfer of open-source software (other than in § 3.05(b) for the reasons explained there). Nevertheless, several aspects of open-source software might suggest a different approach. For example, many often-dispersed developers

frequently contribute to open-source software, including anything from minor and cosmetic changes such as fixing obvious code errors to changes that drastically modify the software's functionality.3 n37 Individual transferors therefore may have little control over its quality. In addition, despite its usefulness for particular tasks, open-source software authors sometimes do not intend an "ordinary purpose" for the software other than allowing other authors to enhance or change the software. Finally, some open-source publishers may consider themselves as engaging in nothing more than a hobby, not releasing commercial software. Despite these differences from proprietary software, open-source transferors can avoid making express warranties and can disclaim implied warranties and limit remedies. Further, open-source transferors can look to course of dealing and usage of trade to support their claim of the absence of warranties.3 n38 The nature of open-source production and distribution should limit the expectations of transferees, which in turn will narrow the reach of warranties. For example, a transferee who downloads open-source software from an Internet site that offers free downloads normally should expect "as is" software, whereas a transferee who purchases open-source software from a proprietary site would have greater expectations in the absence of enforceable disclaimers. Finally, a hobbyist should not be liable for the merchantability warranty of § 3.03 if the hobbyist does not "deal in software of the kind transferred" or "hold itself out by occupation as having knowledge or skill peculiar to the software."

§ 3.01 Implied Indemnification Against Infringement

(a) Except as provided in (d) or as excluded or modified under (e), a transferor that deals in software of the kind transferred or holds itself out by occupation as having knowledge or skill peculiar to the software, and that receives money or a right to payment of a monetary obligation in exchange for the software, must indemnify and hold the transferee harmless against any claim of a third party based on infringement of an intellectual property or like right which right exists at the time of transfer and is based on the laws of the United States or a State thereof. The transferor must pay those costs and damages incurred by the transferee that are specifically attributable to such claim or those costs and damages agreed to in a monetary settlement of such claim.

(b) If a court enjoins the transferee's use of the software or holds the software infringing or otherwise in violation of a like right under subsection (a), the transferor may be liable for damages under § 4.05 and must at its own expense and on reasonable notice from the transferee of its desire for a remedy provide the transferee with one of the following remedies as the transferor chooses:

(1) procure for the transferee at no cost to the transferee the continued right to use the software under the terms of the applicable agreement;

(2) replace or modify the software with noninfringing software of substantially equivalent functionality; or

(3) cancel the applicable agreement and refund to the transferee the fees actually paid by the transferee for the infringing components of the software. If the infringement renders the software substantially unusable, the transferor must refund the entire fee. In either case, the transferor must also reimburse the transferee for incidental expenses incurred in replacing the software, but the transferor may deduct from the amounts due to the transferee under this Section a reasonable allowance for the period of time the transferee used the software.

(c) The indemnification law of the state whose law applies to the agreement under § 1.13 or under otherwise applicable law applies to the duty of indemnification of subsection (a).

(d) Unless otherwise agreed, a transferor has no obligations under subsections (a) and (b) if

(1) the transferee uses or modifies the software in a manner not permitted by the terms of the agreement where such use or modification gives rise to the claim; or

(2) the infringement arises from the transferor's compliance with (i) transferee-provided detailed functional specifications; and (ii) a transferee-provided method or process for implementation of those specifications, unless the transferor knows of potential infringement or a claim of infringement at the time of transfer and does not notify the transferee that compliance with the specifications and method or process may result in an infringement.

(e) Indemnification under subsection (a) and the duties of subsection (b) may be excluded or modified

(1) if the exclusion or modification is in a record, is conspicuous, and uses language that gives the transferee reasonable notice of the modification or notice that the transferor has no obligation to indemnify the transferee; or

(2) by course of performance, course of dealing, or usage of trade.

Comment:

a. Nature and scope of the implied indemnity. This Section indemnifies the transferee against claims of infringement and the like and replicates some of the sample indemnification provisions set forth in H. Ward Classen, A Practical Guide to Software Licensing for Licensees and Licensors 256-257 (2d ed. 2007).

The indemnity arises only if the transferor: (i) deals in software of the kind or holds itself out by occupation as having knowledge or skill peculiar to the software; (ii) receives money or the right to payment of a monetary obligation for the software; and (iii) the indemnification is not disclaimed. Parties that satisfy (i) would qualify as merchants under the definition in U.C.C. § 2-104(1). Transferors that "deal" in software, for example, release or distribute generally available software on the retail market or provide custom software. Transferors who have "knowledge or skill peculiar" to the software include software troubleshooters and maintenance craftspeople. For the implied indemnification to arise, the transferor must receive money or its equivalent in return. "Money" is defined by the U.C.C.: a "medium of exchange currently authorized or adopted by a domestic or foreign government. . . ." U.C.C. § 1-201(b)(24) (2008) (former U.C.C. § 1-201(24)). "A right to payment of a monetary obligation" is intended to encompass transactions that do not involve an immediate exchange of currency but in which the transferor receives a monetary equivalent. For example, if the transferee pays by credit or debit card, check or draft, or commits to pay for related consideration such as services, the transferor receives the right to payment of a monetary obligation. Open-source collaborators that do not receive money or the right to payment of a monetary obligation in exchange for the software do not indemnify the transferee under the Principles. See Summary Overview, Chapter 3, Topic 1.

Section 3.01 protects the transferee against damages arising from infringement of intellectual property rights such as patent, copyright, and trademark, and misappropriation of trade secrets (an example of what the term "like right" as used in § 3.01(a) covers) within the United States or any State of the United States. The parties can agree to extend the obligation to other territories by enumerating the names of those other countries or using such terms as "worldwide." The default rule, however, should not impose the obligation outside of the United States. Some rights, like patent and trademark, are quite territorial by nature, and the transferor may not have secured protection in other countries. Also, the transferor may simply not be in a position to know whether the software infringes outside the U.S. because, for example, it may not market outside the U.S. or it may lack the resources to determine the software's status outside of the U.S.

The obligation of subsection (a) extends only to claims under U.S. federal or state law regarding rights that existed at the time the software is transferred. Thus, for example, the transferor does not indemnify the transferee against infringement of a patent that is issued after the software is transferred. The parties can, of course, agree to a broader indemnification obligation than that provided for in this Section.

Illustrations:

1. A, a merchant, transfers to B word-processing software suitable for use on a particular operating system. Use of the software on that operating system violates a patent held by C. C sues B for patent infringement. Assuming that there is no disclaimer in the agreement, B pays money or its equivalent for the software, and B complies with the relevant state indemnification law regarding notification to A and participation in the suit, B is entitled to indemnification of costs and expenses awarded against it. If the software is held infringing, B is also entitled to a remedy under § 3.01(b).

2. A transfers word-processing software to B. B uses the software to infringe another's copyright by typing in verbatim the contents of a book and saving the resulting document in a file. C, the copyright owner, sues B for copyright infringement. A has no obligation to indemnify B.

3. B ordered a computer system from A. A is in the business of marketing computer-hardware and office-software packages. B asked for word-processing capability with its system. A delivered a system that contained C's word-processing product under terms that authorized B to make copies of it. C owns the copyright in the word-processing software and had authorized A to distribute copies of it, but not to authorize anyone else to make copies. C learns that B is making copies of its software. C brings a rightful claim of copyright infringement against B. At the time A delivered the software, A had exceeded the scope of its license with C by authorizing B to make copies. This likely constitutes infringement, and thus A is obligated to indemnify B (if B complied with relevant state law on indemnification, B paid money or its equivalent for the software, and the agreement did not contain a disclaimer).

b. Remedies. As explained in the Summary Overview to this Topic, § 3.01 departs from Article 2 and UCITA. Both of those Acts provide a warranty against infringement. Generally, an approach under warranty law would permit a transferee to recover breach-of-warranty damages whether or not the transferee was actually sued by the rightholder. Of course, this rarely occurs since most providers disclaim the warranty. Given the considerations noted in the Summary Overview, these Principles protect those transferees that suffer out-of-pocket costs and obligate the transferor to provide a remedy. As set forth below, the choice of which remedy to provide is the transferor's and the remedies generally are not as extensive as warranty damages. This more limited liability may provide an enhanced incentive to providers to offer tailored indemnity rather than to disclaim all liability.

Under subsection (b), a "merchant" transferor that receives money or a right to the payment of a monetary obligation for the software owes a duty to its transferee if use of the software is enjoined or the software is held infringing by a court of competent jurisdiction. In such cases, the transferor at its own expense must obtain for the transferee (who must notify the transferor of its desire for a remedy) the right to continue to use the software or must modify or replace the software to make it noninfringing. These "remedies" are not the same as those that would be associated with a warranty of noninfringement. Rather, they sound more in specific performance and may ultimately be more or less expensive than breach-of-warranty damages depending on the circumstances. A final option for the transferor is to refund the amount paid under the agreement and to pay incidental expenses the transferee incurred in replacing the software less allowance for use. This final option sometimes would lead to damages equivalent to those for breach of a warranty of noninfringement. The transferor may also sustain liability for damages under § 4.05.

Through its indemnification scheme, this Section attempts to mitigate transferors' potential large unanticipated monetary liability that could accrue if transferors were required to make a warranty of noninfringement. At the same time, transferees using software determined to be infringing or whose use has been enjoined are in need of protection. By providing the transferor with options from which to choose, the Principles balance the interests of both parties. To the extent that providers routinely disclaim all obligations, courts should strictly construe the requirements for an effective disclaimer and assess disclaimers for unconscionability.

Illustration:

4. Assume the same facts as in Illustration 1. Assume also that A transferred software that is the subject of the infringement holding to D, E, and F, whom C does not sue. The rights of these transferees, if any, are determined by their agreement with A.

c. Other applicable law. Indemnification law is complex. This Section does not attempt to draft a law of indemnification with respect to such matters as, for example, when the transferee must notify the transferor of the claim, who controls the litigation, who may settle the claim, when indemnity must be paid, and whether attorneys' fees are recoverable. Instead, subsection (c) directs courts to apply state law to these details.

Illustration:

5. Assume the same facts as in Illustration 1, except that C has not sued B. Rather, C has sent a letter to B threatening such a suit. A is obligated to handle the matter at its own expense. State law determines who may settle the dispute. State law also determines whether A has an obligation to indemnify B if B reaches an agreement with C under which it pays C a fee and A does not consent to that agreement.

d. Limitation of subsection (d). The obligation of § 3.01(a) does not arise if the transferee uses or modifies the software in a way that is not permitted by the agreement and that use or modification causes infringement. In interpreting what is permitted by the agreement, the parol- evidence and interpretation principles of Chapter 3, Topic 2, of the Principles apply. Thus, for example, the wording of a user manual may explain or supplement the permitted uses under the written terms.

Also, the obligation does not arise if the transferee has provided the transferor with functional specifications and a method or process for implementation of those specifications and infringement occurs as a result. (The intent here is that for the obligation to fail to arise, the functional specifications must be detailed.) If, however, the transferor knows that compliance with the

specifications and the method or process for implementing them may result in infringement and does not notify the transferee of that fact, the transferor's indemnification obligation arises.

Illustrations:

6. A transfers word-processing software to B under terms that permit B to modify it. B modifies the program and combines it with another. The resulting combination violates C's patent rights. A has no obligation to indemnify B in a suit against it brought by C.

7. Assume the same facts as in Illustration 1, except that B provides A with detailed functional specifications for the word-processing program, along with the method or process for implementing those specifications in the software. A writes the software in compliance with those specifications, and the method or process provided by B and the use of the resulting software infringes C's patent. A was not aware of the potential infringement or of any

infringement claim. A is not obligated to indemnify B against a patent-infringement claim brought by C.

e. Disclaimer of indemnification. This Section permits disclaimer of the indemnification obligation of subsection (a) and the duty of subsection (b). Unlike Article 2 and UCITA's treatment of disclaimers of the warranty of noninfringement, but consistent with the disclaimer provisions in
§ 3.06(c) and (d) of these Principles, § 3.01(e) requires a disclaimer to be conspicuous and in a record as conditions of enforcement, unless usage of trade, course of dealing, or course of performance support enforcement of the disclaimer

in the absence of a record. (For a discussion of the meaning of "conspicuous," see § 3.06, Comment *b*.) Unlike UCITA, this Section does not provide safe harbors for the language of a disclaimer in the "black letter." Note that the Section requires that the language give the transferee reasonable notice that the transferor has no obligation to indemnify the transferee.

Illustrations:

8. A transfers software to B under an agreement that states, "There are no warranties, express or implied, written or oral, including but not limited to any implied warranty of merchantability or fitness for use or for a particular purpose, with respect to any software provided hereunder." The disclaimer, even if located and depicted in such a way as to be conspicuous, does not give the transferee reasonable notice of the transferor's intent to disclaim the indemnification obligation. The disclaimer of the indemnification obligation

therefore would be ineffective.

9. A transfers software to B under a record that states, "A shall not be obligated to defend or indemnify B against any claim of infringement or the like." Assuming that the

disclaimer is conspicuous, it is enforceable.

REPORTERS' NOTES

Comment a. Nature and scope of the implied indemnity. See H. Ward Classen, A Practical Guide to Software Licensing for Licensees and Licensors 256-257 (2d ed. 2007).

The wording referring to a right to payment of a monetary obligation is drawn from U.C.C. Article 9's definition of account. See U.C.C. § 9-102(a)(2) (2007). It is, however, used more broadly here than in Article 9. Here, it encompasses all rights to payment of a monetary obligation (e.g., including instruments and chattel paper).

For an example of state law regarding interpretation of indemnity provisions, see Cal. Civ. Code § 2778 (West 2007); N.D. Cent. Code § 22-02-07 (2007) (adopting California's approach); see also generally 23 N.Y. Jur. 2d Contribution, Indemnity, and Subrogation § 100 (2007); F. Inge Johnstone & Christopher Yeilding, The Recovery of Attorney's Fees in Contractual Indemnity Suits, DRI for Def., Dec. 2004, at 16.

Comment b. Limitation of subsection (d). For a non-software case analogous to *Illustration 7*, see *Bonneau Co. v. AG Indus., Inc., 116 F.3d 155 (5th Cir. 1997)* (holding that where a distributor furnished specifications for eyeglass display stands to the manufacturer, the manufacturer could not be held liable to the distributor for infringement of third-party patents).

Illustration 3 is based loosely on *Camara v. Hill, 596 A.2d 349 (Vt. 1991)* (finding a breach of a § 2-312 warranty of noninfringement where the transferor provided its customer with "nonoriginal copies" of programs); see also generally *Major League Baseball Promotion Corp. v. Colour-Tex, Inc., 729 F. Supp. 1035, 1041 (D. N.J. 1990):*

Under copyright law, a person is innocent of infringement if he possesses a sublicense issued by a licensee upon the due authority of the copyright owner. *Pathe Exchange v. International Alliance, 3 F. Supp. 63, 65 (S.D.N.Y. 1932);* . . . . A licensee who has failed to satisfy a condition of the license or has materially breached the licensing contract has no rights to give a sublicensee under which the sublicensee can take cover in a copyright infringement case, and

therefore, both the licensee and the sublicensee can be held liable for acting without authorization and thereby infringing the licensor's copyright.

For non-software, warranty cases analogous to *Illustration 6*, see *Chemtron, Inc. v. Aqua Prods., Inc., 830 F. Supp. 314 (E.D. Va. 1993)* (no breach of warranty where buyer purchased goods from another and combined them into an infringing device); *Motorola, Inc. v. Varo, Inc., 656 F. Supp. 716 (N.D. Tex. 1986)* (no breach of warranty where buyer's use of the good infringed).

§ 3.02 Express Quality Warranties

(a) In this Section, "transferee" includes both an "immediate transferee" that enters an agreement with the transferor and a "remote transferee" that receives the software or access to the software in the normal chain of distribution.

(b) Except as provided in subsection (d), the transferor creates an express warranty to the transferee as follows:

(1) An affirmation of fact or promise made by the transferor to the transferee, including by advertising or by a record packaged with or accompanying the software, that relates to the software and on which a reasonable transferee could rely creates an express warranty that the software will conform to the affirmation of fact or promise.

(2) Any description of the software made by the transferor to the transferee on which a reasonable transferee could rely creates an express warranty that the software will conform to the description.

(3) Any demonstration of software shown by the transferor to the transferee on which a reasonable transferee could rely creates an express warranty that the software will conform to the demonstration.

(c) A transferor can create an express warranty without using formal words, such as "warrant" or "guarantee," or without intending to create an express warranty. However, a mere opinion or commendation of the software does not create an express warranty.

(d) A distributor or dealer that merely transfers software covered by a warranty in a record made by another party, which warranty identifies the maker of the record as the warrantor, is not liable for breach of the warranty. The distributor or dealer is liable for any express warranties of its own or if it adopts the maker's warranty.

Comment:

a. Generally. Under § 3.02(a), a transferor potentially is liable for express warranties to any transferee in the distributional chain, including intermediates and the end user in that chain, or to transferees who download or obtain access to the software directly from the transferor over the Internet. However, under § 3.02(b), before a warranty arises, the transferor must make a warranty to the transferee, such as by making a promise directly to a party, by including a warranty in a record in a package opened by the end user, or by advertising to the public. In addition, under subsection (d), parties in the distributional chain who do not author a warranty are not liable under it unless they adopt the maker's warranty. A party adopts a warranty when a reasonable transferee would believe the party intends to stand behind or appropriate as one's own the warranty made by another party.

b. "Basis of the bargain" test omitted. Section 3.02(b) does not use the "basis of the bargain" test of U.C.C. §

2-313(1)(a), (b), and (c) and UCITA § 402 in the special context of software transfers. If the transferor makes a statement that constitutes an affirmation of fact, promise, or description, the statement constitutes an express warranty, not if the statement constitutes a "basis of the bargain," but if the transferee could reasonably rely on the statement. Section 3.02(b) does not require actual reliance on the express warranty. The same treatment applies to descriptions and demonstrations. The foggy "basis of the bargain" test has triggered lots of litigation and numerous attempts by drafting committees to replace or refine it. The approach here adopts the best approximation of what the original U.C.C. drafters and courts applying the test attempted to achieve.

Comment 3 to U.C.C. § 2-313, in explaining the "basis of the bargain" test, states that "no particular reliance on [an affirmation of fact or promise] need be shown in order to weave them into the fabric of the agreement." Although the Code does not require "particular" reliance, "basis of the bargain" must mean something. Section 3.02(b) more succinctly dictates that an affirmation of fact or promise (or description or demonstration) constitutes an express warranty if a reasonable transferee could rely on it. Just as in the U.C.C., the transferee does not have to prove actual reliance. As such, affirmations of fact about the software, descriptions of the software, and other language or conduct indicating commitment and not puffing ordinarily will constitute express warranties even if a transferee could not see the warranty until after paying for the software because, for example, the warranty is in the software package. See § 3.02(c) and Comment *f*. As elsewhere, "reasonableness" is an objective test, but it should take into account the relative sophistication of the transferee.

Illustrations:

1. B, a manufacturer of computer products, foresees the need for additional computer capability. B becomes interested in replacing its "Prime" operating system with an "Ultrix" system, but wants to continue using certain business-applications software for accounting and inventory tracking needs. This software is not compatible with the Ultrix system. B acquires software called "uniVerse " from transferor A after A tells B that uniVerse will allow B to run its accounting and inventory software on the Ultrix system. A reasonable transferee could rely on A's statement because it responds specifically to B's concerns and needs and is clear and unconditional. If B's accounting and inventory software do not run on the Ultrix system, A has breached an express warranty if all of the other express-warranty requirements have been met. (See also § 3.04, Illustration 3.)

2. B, a manufacturer of sporting goods, negotiates with A to install a new computer system for use in B's business. A suggests the installation of a "turn-key" system-a system that includes all necessary hardware and software, and is ready to function upon delivery. During the negotiations, B becomes concerned about the proposed software's response time. A prepares a "Response Time Report" for B. The Report states that the general response time "likely is about 4-5 seconds or, at worst, about 10 seconds." B then purchases the system. After delivery, B discovers that the software's response time is almost 40 seconds so that it is substantially useless for B's business needs. A is in breach of an express warranty because the Response Time Report, although expressing some uncertainty about the response time, promised a maximum response time of 10 seconds. A reasonable transferee could rely on A's promise.

c. Advertising. Under § 3.02(b)(1), an express warranty can arise based on advertising. The test for whether a warranty arises is no different than for any other language: Could a reasonable transferee rely on an advertiser's quality claims or would the reasonable transferee balk because the language is not specific, verifiable, and/or is devoid of commitment? In the context of advertising, some degree of skepticism about the information content is in order. Put another way, readers should more readily understand that with advertising, puffing and sales talk are more likely. Still, software providers' lawyers not infrequently peruse draft advertising for statements that could form express warranties because of the knowledge that reasonable readers could rely on advertising in some circumstances.

Illustration:

3. B sees an advertisement in a newspaper for A's X-400 computer system. The advertisement states that the system includes "compatible" software. B purchases the system, but the software is not compatible with the hardware. A's advertisement created an express warranty that A's software would be compatible.

d. Warranty by description. Section 3.02(b)(2) follows § 2-313(1)(b) of the U.C.C. Comment 5 to § 2-313(1)(b) states in part:

A description need not be by words. Technical specifications, blueprints and the like can afford more exact description than mere language . . . . Of course, all descriptions by merchants must be read against the applicable trade usages . . . .

Descriptions include generic names such as "word-processing software" or the like. A transferor that describes the software as capable of word processing or calls the software "word- processing software" has made an express warranty to that effect. The test is whether, in light of the circumstances, a reasonable transferee could rely on the description. Relevant circumstances include any applicable usage of trade or course of dealing.

Illustration:

4. B shops for software for her 10-year-old grandson's birthday. She acquires software with packaging that describes the software as "fun and exciting software games for grownups and kids." However, the software consists of a spreadsheet program suitable only for accountants. A has breached an express warranty because B could reasonably rely on A's description of the software as games meant for children. However, a reasonable transferee could not rely on the "fun and exciting" general statement.

e. Warranty by demonstration. Section 3.02(b)(3) comes from UCITA § 402. A Comment to the UCITA section adds: "Ordinarily the parties understand that what is being demonstrated on a

small scale or tested on a beta model is not necessarily representative of actual performance or of the eventual product." UCITA § 402, Comment 5.

A transferor can avoid the creation of a software warranty by demonstration by clarifying that the software to be transferred may be different from what the transferor is showing or demonstrating. Further, if a reasonable copyholder would understand that the software may not perform according to the demonstration in light of the manner in which the copyholder will use the software, no express warranty as to that use would arise because a reasonable copyholder could not rely on the demonstration for that use.

Illustration:

5. B, a manufacturer of movie DVDs, wants to acquire software to "clean" the visuals of old television shows for purposes of releasing them on DVD in "remastered" form. A manufactures software for that purpose and demonstrates it to B at its office. A shows B a short video clip A produced using a modern digital camera, which the software cleans in five minutes. As a result, B acquires the software. Later, B brings an action for breach of express warranty, alleging that the software took almost eight hours to clean a 45-minute TV episode recorded in the 1960s. B's claim should fail because a reasonable transferee would understand that the software's speed in cleaning modern digital video may not correspond to the speed the software cleans video recorded in the 1960s.

f. Express warranty or opinion. These Principles look to U.C.C. Article 2's approach to determining whether a statement by the transferor constitutes an "affirmation of fact or promise" or nothing more than the transferor's nonactionable opinion about the software. As with § 2-313 of the U.C.C., the goal of § 3.02(c) is to enforce actual commitments by the transferor, not language that would tip off reasonable listeners or readers that the transferor is merely pitching a sale. The challenge in sorting out the transferor's language is no different than ascertaining the legal significance of any communication between contracting parties: What would a reasonable transferee believe is the

meaning of the transferor's communication? As such, § 3.02(c) is an iteration of the "reasonable transferee" test of § 3.02(b).

Factors helpful in ascertaining what a reasonable transferee would believe include whether the transferor uses language of commitment, the degree of specificity of the communication, and whether the statement can be verified. For example, an exclamation that software "will work wonders" to increase a business's appeal is vague, unverifiable, and lacks commitment. On the other hand, a transferor that proclaims that software used for sorting data "will cut the time for sorting the data in half," may make an express warranty to that effect.

The circumstances in which a transferor makes a statement are also helpful in determining whether a statement is a warranty or puffing. For example, a transferor's statement made during early discussions of the transferee's need for custom software, before the nature of the needs are even clear, would not constitute an express warranty. Definitive statements made closer to signing a contract should be treated differently. Further, written statements are more likely definitive than oral ones.

Illustrations:

6. Same facts as Illustration 1. A tells B that uniVerse will allow B to run its accounting and inventory software on the Ultrix system. A reasonable transferee could rely on A's statement because the statement is clear, specific, and verifiable. If B's accounting and inventory software do not run on the Ultrix system, A has breached an express warranty.

7. B, a sporting-goods vendor, contracts with A, a software provider, to acquire 100 copies of A's software that creates advertisements for placement in newspapers. Prior to the transaction, A tells B that placing advertisements generated by its software will "increase business." A's statement is vague, general, and unverifiable. A is not liable for breach of an express warranty if A's software fails to generate advertisements that increase B's business.

g. Coupling of remedial promises and express warranties. Software transferors often link warranties and remedies by excluding most or all warranties and substituting a particular level of service. For example, a transferor may transfer software "as is," but promise to supply updates or to service error-prone software within a certain time period. Technically, the promise of service is a "remedial promise" and not an express warranty. As such, enforcement depends on Chapter 4 of these Principles and general contract law. Nevertheless, factors set forth in this Section for determining the creation of an express warranty (for example, specificity and commitment) and factors set forth in § 3.06(a) for determining whether an express warranty survives a disclaimer (reasonable expectations) are probative of whether the agreement contains an enforceable remedial promise.

Illustrations:

8. A, a software transferor, transfers custom software to B, an automobile manufacturer, for use in the manufacture of B's cars. A warrants that the software will substantially perform according to certain specifications, but not that it is error free. A also promises that for a period of one year it will remedy any defects in the software having a material effect on B's operation. A has made an express warranty that the software will substantially satisfy the specifications and a remedial promise that it will remedy any material defects for one year. Enforcement of the remedial promise depends on the remedy provisions of these Principles and general contract law.

9. Same facts as Illustration 8, except that A promises only that for one year A will fix any errors in the software that are identified through specific acceptance tests set forth in the contract. The contract also states that A will remedy any errors caused by B's system alterations at A's time and materials rates. A has made a remedial promise that it will fix identified software errors and will remedy other errors for a charge.

h. Makers of warranties. Under § 3.02(d), distributors or dealers that do not author a warranty in a record are not liable for it unless they adopt the maker's warranty. A party adopts a warranty when a reasonable transferee would

believe the party intends to stand behind or appropriate as its own the warranty made by another party. In addition, a distributor or dealer is liable for its own warranties. In the case of a dealer, software displayed for sale as a particular kind of software, for example, means that the dealer has adopted the maker's express warranty by description that the software is the particular kind of software with its average qualities.

Illustration:

10. B, a consumer, acquires from a retail store A's software for calculating complex mathematical problems. Prior to the transfer, a salesperson in the store explained A's warranty. The store is not liable for breach of A's express warranty because a reasonable transferee would not believe that the store adopted A's warranty simply as a result of the salesperson's explanation. If the software package describes the software as an "e-calculator" and the store displays the software, the store has adopted A's warranty of description.

REPORTERS' NOTES

Comment a. Generally. Section 3.02(a) and (b) combine U.C.C. Amended Article 2, §§ 2-313, 2-313A, and 2-313B. U.C.C. § 2-313A, Comment 1, states that "[u]se of 'obligation' rather than 'express warranty' [in § 2-313A] avoids any inference that the obligation arises as part of the basis of the bargain as would be required to create an express warranty under section 2-313." But these Principles drop the "basis of the bargain" test, so no distinction is necessary between express warranties made to the immediate transferee and made to remote transferees. Under § 3.02, the test is whether the transferor directs an affirmation of fact, promise, etc. to the immediate or remote transferee and whether that transferee reasonably could rely on the alleged warranty.

Comment b. "Basis of the bargain" test omitted. A leading treatise on licensing law fails to clarify the "basis of the bargain" test:

The comments to the Article 2 section indicated that [the basis of the bargain test] was intended to supplant the pure reliance standard, but the language used in effect merely reduces the need for a finding of 'explicit,' 'but for' reliance in the sense that it is the reason that the contract was formed. . . . The basis of the bargain test requires that *a nexus of influence* between warranty and bargain exist. The issue is what that nexus must be. Since the advent of Article 2, debate has raged in both the academy and the courts as to whether the phrase "part of the basis of the bargain" was intended to abrogate the reliance requirement that the predecessor to Article 2 . . . explicitly imposed.

Raymond T. Nimmer & Jeff Dodd, Modern Licensing Law § 8:33 (2005).

Although there is much case law on "basis of the bargain," the cases have failed to create a coherent concept out of an ambiguous statutory term. Far from it-the case law, as recent as 2008, is sufficiently incoherent that the better approach is to abandon the concept altogether. See, e.g., *Cole v. Gen. Motors Corp., 484 F.3d 717, 726 (5th Cir. 2007)* ("There is a clear split of authority among the jurisdictions as to whether a buyer must show reliance on a statement or representation for it to be considered part of the 'basis of the bargain.'") (citing Barkley Clark & Christopher Smith, The Law of Product Warranties § 4:16 (2d ed. 2002)); *Kelleher v. Lumber, 891 A.2d 477, 500 (N.H. 2005)* ("Authorities are divided as to whether a buyer's reliance upon the affirmation is a necessary element of proving that the affirmation was part of the basis of the bargain under section 2-313 of the UCC. . . ."); id. ("The extent to which the law has been changed to remove the reliance requirement is unclear."); *Compaq Computer Corp. v. Lapray, 135 S.W.3d 657, 675 (Tex. 2004)* ("Although the official comments to section 2-313 provide that 'no particular reliance on such statements need be shown in order to weave them into the fabric of the agreement,' it appears that this suggestion is not uniformly followed.") (internal citation omitted); *id. at 676* ("Still other states have not decided whether reliance is required, nor what the 'basis of the bargain' actually means."); *Parkinson v. Guidant Corp., 315 F. Supp. 2d 741, 752 (W.D. Pa. 2004)*

("[I]t is recognized that '[w]hat constitutes "basis of the bargain" is hard to define'. . . .") (quoting *Liberty Lincoln-Mercury Inc. v. Ford Motor Co., 171 F.3d 818, 825 (3d Cir. 1999); McManus v. Fleetwood Enters., Inc., 320 F.3d 545, 550 (5th Cir. 2003)* ("There is a split of authority as to whether [the "basis of the bargain"] wording (from the UCC) is meant to dispense with the common law's requirement of reliance in express warranty cases."); *Torres v. Northwest, 949 P.2d 1004, 1013 (Haw. Ct. App. 1997)* ("The UCC does not define 'basis of the bargain,' and one scholar has expressed that the term '[m]ost probably . . . is an indefinable concept.' As a result, much litigation has arisen over the years regarding the meaning and proper application of the 'basis of the bargain' test.") (citing 3 M. Foran, Williston on Sales § 17-7, at 12 (5th ed. 1994); *Hobco, Inc. v. Tallahassee Assocs., 807 F.2d 1529, 1533 (11th Cir. 1987)* ("Under Florida law, an express warranty may arise only where justifiable reliance upon assertions or affirmations is part of the basis of the bargain."); *Keith v. Buchanan, 220 Cal. Rptr. 392, 397 (Ct. App. 1985)* ("Some [commentators] have indicated that [the "basis of the bargain" test] shifts the burden of proving non-reliance to the seller, and others have indicated that the code eliminates the concept of reliance altogether."); see also *Elias v. Ungar's Food Prods., Inc., 252 F.R.D. 233, 239 (D. N.J. 2008)* ("As a rule, no proof of the buyer's reliance on the warranty is necessary other than that the seller's statements were of a kind which naturally would induce the purchase."); *Keith v. Buchanan, 220 Cal. Rptr. 392, 397-398 (Ct. App. 1985)* ("It is clear from the new language of this code section that the concept of reliance has been purposefully abandoned."); *Allied Fid. Ins. Co. v. Pico, 656 P.2d 849, 850 (Nev. 1983)* ("If, however, the resulting bargain does not rest at all on the representations of the seller, those representations cannot be considered as becoming any part of the 'basis of the bargain' within the meaning of [the code]."); *Winston Indus., Inc. v. Stuyvesant Ins. Co., Inc., 317 So. 2d 493, 497 (Ala. Civ. App. 1975)* ("As this court perceives it, the determining factor in this case under the newly enacted Uniform Commercial Code is not reliance by the purchaser on the seller's warranty, but whether it is part of the 'basis of the bargain.'").

UCITA retains the "basis of the bargain" test. UCITA § 402, Comment 2 (2002) explains the approach: "In practice, affirmations of fact describing the [software] and made by the licensor about it during the bargaining are ordinarily part of the bargain unless they are mere puffing, predictions, or otherwise not an enforceable commitment. No specific reliance on the specific statement need be shown in order to weave it into the fabric of the agreement."

For a discussion of sales-of-goods cases involving warranties that come packed in a box after a sale, see, e.g., *Rite Aid Corp. v. Levy-Gray, 894 A.2d 563 (Md. 2006)* (warranty that came after sale actionable as part of the "basis of the bargain"; requiring actual knowledge of the warranty and reliance would negate all consumer warranties).

Comment c. Advertising. "The targets of advertising, all of us, understand that advertising provides a distorted view of reality, depicting what we aspire to, not where we are or what we really expect to happen." Raymond T. Nimmer & Jeff Dodd, Modern Licensing Law § 8:33, n.16 (2005); see also Elliott Alderman, UCITA: Why Consumers Should Read The Fine Print, http://www.aldermanlawoffice.com/indexpage_6/Articles_4.shtml (last visited Aug. 19, 2009) (2002) ("[L]awyers carefully review licensors' advertising copy to ensure that there are no loose factual statements that could form an express warranty."); *Jesmer v. Retail Magic, Inc., 863 N.Y.S.2d 737 (App. Div. 2008)* (express warranty created by brochure); Barbara Chretien-Dar, Note, Uniform Commercial Code: Disclaiming the Express Warranty in Computer Contracts-Taking the Byte Out of the UCC, *40 Okla. L. Rev. 471, 481 (1987)* ("Express warranties can . . . be created by advertisements or brochures, prior proposals, or letters, although these more easily approach puffing than specific oral statements.").

Comment d. Warranty by description. Diane W. Savage, Performance Warranties in Computer Contracts, 8 No. 12 Computer Law., Dec. 1991, at 32, 33, available at http://library.findlaw.com/1997/Nov/1/128553.html (last visited Aug. 19, 2009) ("[A] generic product name, such as 'automobile' or 'haybaler,' constitutes an express warranty that the automobile will carry passengers and the haybaler will bale hay."); Paul S. Hoffman, Software Warranties and the Uniform Commercial Code, 6 No. 4 J. Proprietary Rts. 7, 7 (1994) ("If I agree to sell you my 1984 Volvo in 'as is' condition, I have still made several warranties: . . . that it is a Volvo; that it is a 1984 model; and probably that it has an engine and the normal parts necessary to make it a 1984 Volvo . . . .").

Comment e. Warranty by demonstration. See Matthew J. Smith, Comment, An Overview of the Uniform

Computer Information Transactions Act: Why UCITA Should be Renamed "The Licensors' Protection Act," *25 S. Ill. U. L.J. 389 (2001)* (demonstration warranty must take "into account differences that would appear to a reasonable person in the position of the licensee between the sample, model, or demonstration and the [software] as it will be used.") (quoting UCITA § 402(a)(3) (2000)); see also *NMP Corp. v. Parametric Tech. Corp., 958 F. Supp. 1536, 1545-1546 (N.D. Okla. 1997)* ("Apparently [plaintiff] NMP wanted Pro/E to perform highly complex tasks . . . at a certain speed, but never questioned whether the software would perform at the same rate at which it did during the demonstration when utilized on larger assemblies . . . ."); *Logan Equip. Corp. v. Simon Aerials, Inc., 736 F. Supp. 1188, 1198 (D. Mass. 1990)* ("While plaintiff may well have taken the [demonstration of the] Ontario Hydro boomlift as an example of [defendant] SAI's skill and expertise in the equipment design field, the 42-foot unit cannot have created an express warranty which survived the generation of a new set of agreed-upon specifications for [defendant's] proposed 80-foot machine.").

Comment f. Express warranty or opinion. See *Keith v. Buchanan, 220 Cal. Rptr. 392, 395 (Ct. App. 1985)* ("In deciding whether a statement made by a seller constitutes an express warranty under this provision, the court . . . must determine whether the seller's statement constitutes an 'affirmation of fact or promise' . . . or whether it is rather 'merely the seller's opinion or commendation of the goods' under section 2-313, subdivision (2)."). On sorting out warranties from sales "puffing," see James J. White & Robert S. Summers, Uniform Commercial Code 347 (5th ed. 2000); *Boud v. SDNCO, Inc., 54 P.3d 1131, 1135 (Utah 2002)* ("To qualify as an affirmation of fact, a statement must be objective in nature, i.e., verifiable or capable of being proven true or false."); see also *Keith, 220 Cal. Rptr. at 395* ("Commentators have noted several factors which tend to indicate an opinion statement. These [include] a lack of specificity in the statement made. . . ."); *Snow's Laundry & Dry Cleaning Co. v. Ga. Power Co., 6 S.E.2d 159, 162 (Ga. Ct. App. 1939)* ("For a representation to be construed as a warranty the statement made must be affirmed as a fact; it must be understood by the parties as having that character; it must be positive and unequivocal and not merely a vague, ambiguous and indefinite statement of the seller regarding the property."); cf. *Bologna v. Allstate Ins. Co., 138 F. Supp. 2d 310, 323 (E.D.N.Y. 2001)* ("Here, Allstate's assertion, 'You're in good hands with Allstate,' is general, subjective, and cannot be proven true or false. . . . [Defendant's] allegation that Allstate's slogan created an express warranty which Allstate thereafter breached . . . must fall . . . .").

On the time when a statement is made, see *Westfield Chem. Corp. v. Burroughs Corp., 21 UCC Rep. Serv. 1293 (Mass. Dist. Ct. 1977),* discussed in Barbara Chretien-Dar, Note, Uniform Commercial Code: Disclaiming the Express Warranty in Computer Contracts-Taking the Byte Out of the UCC, *40 Okla. L. Rev. 471, 480-481 (1987)* ("[E]arly planning stages are less conducive to reasonable reliance.").

On written statements versus oral ones, see White & Summers, supra, at 347 (5th ed. 2000).

Comment g. Coupling of remedial promises and express warranties. See, e.g., *Rockland Trust Co. v. Computer Assocs. Int'l, Inc., 2007 WL 2746804* (D. Mass.) (best efforts obligation to make software comply with specifications); see generally Paul S. Hoffman, Software Warranties and the Uniform Commercial Code, 6 No. 4 J. Proprietary Rts. 7, 13 (1994) ("Software warranties are often defined in a reverse way by specifying the remedy or level of service.").

Comment h. Makers of warranties. Section 3.02(d) is based on Magnuson-Moss Warranty Act Regulation , *16 C. F. R. § 700.4 (2009)*. The regulation looks to state law for the meaning of "adoption." Generally, "adoption" requires explicit incorporation of a warranty into the sales contract. See, e.g., *Felde v. Chrysler Credit Corp., 580 N.E.2d 191, 197 (Ill. App. Ct. 1991).* Mere "delivery, presentation, or explanation" of a manufacturer's warranty by a dealer generally does not constitute "adoption" of that warranty. *Lytle v. Roto Lincoln Mercury & Subaru, Inc., 521 N.E.2d 201, 204*[#8209]206 (Ill. App. Ct. 1988) (dealer's signing the inside of manufacturer's warranty booklet not an adoption of the warranty).

Illustration 1 is based on *Vmark Software, Inc. v. EMC Corp., 642 N.E.2d 587 (Mass. App. Ct. 1994).*

Illustration 2 is based on *USM v. Arthur D. Little Sys., Inc., 546 N.E.2d 888 (Mass. App. Ct. 1989).*

Illustration 3 is based on *Hundred East Credit Corp. v. Eric Shuster Corp., 515 A.2d 246 (N.J. Super. Ct. App. Div. 1986).*

Illustration 4 is based on the "automobile and haybaler" example in Diane W. Savage, Performance Warranties in Computer Contracts, 8 No. 12 Computer Law. 32, 33 (1991), available at http://library.findlaw.com/1997/Nov/1/ 128553.html (last visited Aug. 19, 2009) ("computer litigation is on the increase").

Illustration 5 is based on *NMP Corp. v. Parametric Tech. Corp., 958 F. Supp. 1536 (N.D. Okla. 1997).*

Illustration 6 is based on *Vmark Software, Inc. v. EMC Corp., 642 N.E.2d 587 (Mass. App. Ct. 1994).*

Illustration 7 is based on *Westfield Chem. Corp. v. Burroughs Corp., 21 U.C.C. Rep. Serv. 1293 (Mass. Dist. Ct. 1977).*

Illustrations 8 and 9 are based on examples in Paul S. Hoffman, Software Warranties and the Uniform Commercial Code, 4 J. Proprietary Rts. 7, 12-14 (1994).

Illustration 10 is based on *Lytle v. Roto Lincoln Mercury & Subaru, Inc., 521 N.E.2d 201, 205*[#8209]206 (Ill. App. Ct. 1988).

§ 3.03 Implied Warranty of Merchantability

(a) Unless excluded or modified, a transferor that deals in software of the kind transferred or that holds itself out by occupation as having knowledge or skill peculiar to the software warrants to the transferee that the software is merchantable.

(b) Merchantable software at minimum must

(1) pass without objection in the trade under the contract description; (2) be fit for the ordinary purposes for which such software is used; and

(3) be adequately packaged and labeled.

Comment:

a. Makers of the merchantability warranty. Transferors that deal in software or whose occupation demonstrates their special knowledge or skill with respect to the software make the implied merchantability warranty. Such parties would qualify as merchants under the definition in U.C.C. § 2-104(1). Transferors that "deal" in software, for example, release or distribute generally available software on the retail market or provide custom software. Transferors who have "knowledge or skill peculiar" to the software include software troubleshooters and maintenance craftspeople.

As noted in the Summary Overview to this Topic, the Principles do not carve out exceptions to most of the quality warranty provisions for open-source developers on the theory that exceptions are not necessary. Many developers who have little control over quality often contribute to open- source software, and sometimes they do not intend an "ordinary purpose" for the software other than allowing experimentation and development by other authors. These Principles support these developers' right to avoid making express warranties and, with few exceptions, to exclude implied warranties and limit remedies. Further, the nature of open-source production and distribution should limit the expectations of transferees, which, under the rules of disclaimer pertaining to course of dealing and usage of trade, see § 3.06 of these Principles, will narrow the reach of warranties. Finally, a hobbyist should not be liable for the merchantability warranty of § 3.03 if the hobbyist does not "deal in software of the kind transferred" or "hold itself out by occupation as having knowledge or skill peculiar to the software." For example, by definition a hobbyist does not

"deal in software," nor is the hobbyist's "occupation" engineering the particular software.

Illustrations:

1. B Company condenses news stories into "digests" for cell-phone subscribers. A Company offers software on the retail market for this purpose. A transfers the software to B. Unless properly excluded, A makes an implied warranty to B that A's software is merchantable.

2. B, a consumer, takes her broken computer to A, an experienced computer repairperson. After repairing the computer, A suggests that B acquire "defragmentation" software, designed in part by A but published by C, to improve the performance of B's computer. B acquires the software from A. Unless properly excluded, A makes an implied warranty that the software is merchantable because A holds himself out by occupation as having knowledge or skill peculiar to the software.

3. B, a three-person business that manufactures sporting goods, downloads and installs an open-source software operating system from A, an Internet site that offers free downloads of open-source software. The general public license includes a provision excluding the implied warranty of merchantability. The disclaimer is enforceable if it satisfies § 3.06 of these Principles. Even in the absence of such a disclaimer, B reasonably should expect A to transfer the software "as is" in light of its denomination as open-source software and the absence of a charge for it.

b. Meaning of merchantability. At its most basic, merchantability means quality that is customary or commonly accepted in the trade. Just as an air conditioner must cool air to be merchantable, software must give directions to a computer to perform a function, not cause the computer to crash. Still, in less extreme circumstances, the meaning of "merchantability" in the software context is controversial because of the nature of software and the near inevitability of some "bugs" in newly released software. Further, few cases address, no less delineate, the meaning of software merchantability, at least in part because the warranty is so often disclaimed.

Under § 3.03(b)(2), the software must be fit for its ordinary purpose as understood in the trade. Courts generally rely on this test in sale-of-goods cases and similar treatment is likely in the software context. In situations where a software publisher creates custom software for a rare or unique purpose, or the software is experimental, the notion of "ordinary purpose in the trade" obviously does not work well. It amounts to no more than an obligation that the software fit the description of software, i.e., that it consists of instructions for a computer to reach a result and is of average quality. However, software generally will have an ordinary purpose in retail markets, and the merchantability standard can apply in a fashion similar to hard goods. In either market, merchantability does not require perfection, but only quality equivalent to recognized industry standards with respect to criteria such as reliability, compatibility with other software and hardware, speed, and functionality. Further, merchantable software should function up to this level on computers that have other common applications installed. On the other hand, software may be merchantable even though its performance suffers because of factors independent of the software, such as a computer's hardware or the configuration of the hardware and the computer's operating system.

A Comment from UCITA § 403, Comment 3.a (2002) is helpful in filling out the meaning of merchantability:

To be fit for ordinary purposes does not require that the program be the best or most fit for that use or that it be fit for all possible uses. To an extent greater than for goods, computer programs are often adapted and employed in unlimited or inventive ways or ways that go well beyond the uses for which they were distributed. The focus of the implied warranty is on the ordinary purposes for which programs are used.

Software is merchantable therefore if it meets average standards, which may well include some flaws. The question is whether average software in the industry includes such flaws. A helpful analogy comes from the early days of color televisions. New color televisions frequently required removal of the chassis to adjust for color malfunctions. A color television that required adjustment as described may well have been merchantable despite being prone to the malfunction, at least until manufacturers perfected them.

Courts in sale-of-goods cases have noted that merchantability is a contract-law test that focuses on the purchaser's disappointed expectations. Liability is strict in the sense that a transferor may be liable in the absence of any fault if the goods are not merchantable. This test differs from certain design-defect cases under the law of products liability involving liability for personal injury and damage to property other than the product itself, which cases consider the reasonableness of the manufacturer's design choices. Thus, a transferor may be strictly liable under § 3.03 of these Principles for a bug in the software that is not reasonably discoverable at the time of supply if the software is not fit for its ordinary purpose, even though the transferor may not be liable for personal injury or property damage under products-liability law. Of course, a transferor would not be liable even under the merchantability test for a bug that shows up after transfer if the transferee reasonably should expect the bug. In such a case, the software is fit for its ordinary purpose.

Illustration:

4. A licenses software products on the open market for a fee. B is a printing business. A transfers graphical-design software to B. B later discovers that the software does not support the .TRO file format, a recent advance in visual quality. Other software supports .TRO without sacrificing other features. A has not breached the implied warranty of merchantability because its software is fit for its ordinary purpose even though it is not "the best" software available.

Subsections (b)(1) and (b)(3) of § 3.03 follow U.C.C. § 2-314(2). Under § 3.03(b)(1), the software, as described in the contract, must satisfy the requirements of the particular trade. UCITA § 403(a)(2)(A) includes a separate implied warranty of adequate packaging and labeling running to distributors. UCITA's reasoning is straightforward: "If the transfer is to a person acquiring the program for re-distribution, the program must be . . . capable of re-distribution." UCITA § 403, Comment 3.b. Software inadequately packaged or labeled ordinarily cannot be distributed successfully. Adequacy should be measured by "ordinary commercial expectations." Id. Section 3.03(b)(3) refers to the software's packaging and labeling, not to the tangible medium that stores the software, such as a disk or CD-ROM.

c. Privity. Current law is unclear on whether the implied warranty of merchantability applies to consumer claims against manufacturers with whom the consumer has no privity of contract. U.C.C. § 2-314 requires a "contract of sale," suggesting that only the immediate seller, usually a dealer, is liable to the consumer if the goods are not merchantable. In addition, UCITA § 403 provides that a merchant licensor makes a merchantability warranty to the end user but, according to Comment 1, limits coverage to parties in a "contractual relationship" or parties that qualify as third-party beneficiaries under UCITA's rules. However, the Magnuson-Moss Warranty Act, 15 U.S.C. §§ 2301-2312, has increased the reach of the merchantability warranty to include non-privity manufacturers or suppliers in the chain of distribution if the manufacturer or supplier has made an express warranty. Further, some state courts have relaxed the privity requirement.

Many software-quality claims do not raise privity issues. Direct transfers of custom-designed software by a transferor to the end user obviously avoid the privity problem. So do transfers between end users and transferors if the end user downloads the software directly from the transferor over the Internet. Even if the transfer involves packaged software that moves through a chain of distribution ultimately to an end user, privity issues may not arise if the transferor supplies a contract to the end user that accompanies the software. In the software case where privity is an issue, the black letter of the Principles retains the privity requirement, but courts may expand the reach of the merchantability warranty. Further, remote transferees can look to § 3.07 of these Principles dealing with third-party beneficiaries, which may extend warranty coverage.

Illustrations:

5. For a fee, B, a consumer, downloads software from A's website that increases the general speed of all downloads. A is the publisher of the software. A and B are in privity of contract. The software fails to function. Unless

properly excluded, A has breached the implied warranty of merchantability.

6. Same facts as Illustration 5, except that B acquires the software at a local store. The software program includes A's "clickwrap" presentation of terms that requires B to click "I accept" before installing the software. A and B are in privity of contract. The software fails to function. Unless properly excluded, A has breached the implied warranty of merchantability.

d. Disclaimers. Section 3.06 recognizes disclaimers of the implied warranty of merchantability in order to balance publishers' concern about excessive liability in light of the nature of software with the end users' reasonable expectation that the software will be fit for ordinary use. Although currently software publishers routinely disclaim the merchantability warranty, market pressure may persuade some to offer merchantability protection to end users.

REPORTERS' NOTES

Comment a. Makers of the merchantability warranty. U.C.C. § 2-104(1) provides in part: "'Merchant' means a person who deals in goods of the kind or otherwise by his occupation holds himself out as having knowledge or skill peculiar to the practices or goods involved in the transaction . . . ." "Merchants" are "professional[s] in business." U.C.C. § 2-104(1), cmt. 2. This definition should exclude the software "hobbyist." For elaboration on what constitutes a "merchant," see J. White & R. Summers, Uniform Commercial Code 362 (2002).

Under UCITA, transferors of "free software" make no implied warranties. See § 410, discussed in Matthew D. Stein, Rethinking UCITA: Lessons From the Open Source Movement, *58 Me. L. Rev. 157, 199 (2006).*

Comment b. Meaning of merchantability. Merchantability means that "[c]ourts may rely on what is customary in the trade, or what is common among goods of the same price and in the same general class." Robert W. Gomulkiewicz, The Implied Warranty of Merchantability in Software Contracts: A Warranty No One Dares to Give and How to Change That, 16 J. Marshall J. Computer & Info. L. 393, 396 (1997). "The implied warranty of merchantability ensures that the resources obtained in the contract function consistently with quality standards in the trade." Raymond T. Nimmer & Jeff Dodd, Modern Licensing Law § 8:26 (2005). "Few cases in modern litigation involve standards of merchantability in reference to either software or hardware because the implied warranty is ordinarily disclaimed and replaced by other standards." Id. at § 8:27.

UCITA § 403, Comment 3.a (2002) provides:

Merchantability does not require a perfect program, but only that the subject matter be generally within the average standards applicable in commerce for programs having the particular type of use. The presence of some defects may be consistent with merchantability standards. Uniform Commercial Code § 2-314 . . . explains the concept in terms of "fair average," i.e., goods that center around the middle of a belt of quality-some may be better and some may be worse, but they cannot all be better and need not all be worse. That approach applies here. While perfection is an aspiration, it is not a requirement of an implied warranty for goods, computer programs or any other property. Indeed, a perfect program may not be possible at all.

See also Nimmer & Dodd, supra at § 8:26.

Merchantability criteria include reliability, compatibility with other software and hardware, speed, and functionality. Douglas E. Phillips, When Software Fails: Emerging Standards of Vendor Liability Under the Uniform Commercial Code, *50 Bus. Law. 151, 155-156 (1994)* (reliability means "'the probability of failure-free operation of a computer program for a specified time' in a given environment," and software "'failure'" occurs when software "'has not met user requirements in some way.'") (quoting Victor R. Basili & John D. Musa, The Future Engineering of Software: A Management Perspective, in Software Mgmt. 9-10 (4th ed. 1993); John D. Musa et al. Software Reliability: Measurement, Prediction, Application 5 (Prof. ed. 1990)).

For a discussion of the wisdom of applying merchantability standards to unique software, see Ajay Ayyappam, UCITA: Uniformity at the Price of Fairness?, *69 Fordham L. Rev. 2471, 2488-2489 (2001).*

Cases on the meaning of merchantability include *Vision Graphics v. EI du Pont de Nemours, 41 F. Supp. 2d 93 (D. Mass. 1999)* ("The computer software system and upgrades, to be merchantable, must have been capable of passing without objection in the trade under the contract description, and fit for the ordinary purposes for which they were intended.") In *Vision Graphics*, the plaintiff, Vision Graphics, complained that the computer system at issue would not accept certain "raw" files. Although plaintiff alleged that defendant promised to support and upgrade the system so that it would accept the files, the court found that such a feature was not

an ordinary purpose for which such system was intended. While it may be true that Vision Graphics' long-term objective was to have the system [accept the files], this feature was certainly not part of the ordinary purpose of the system at the time when the contract was executed. The ordinary purpose of the system was to handle tasks relating to computer graphics. There is no evidence in the record showing that the system failed to accomplish such tasks.

Some evidence of the existence of a defect at the time of delivery is an essential element of a cause of action for breach of the implied warranty of merchantability. . . . Vision Graphics does not allege that the system was defective at the time of delivery, and the system continues to perform as it did at the time of installation.

Id. at 99; see also *Montgomery County v. Microvote Corp., 320 F.3d 440 (3d Cir. 2003)* (vote-tracking software not merchantable when it miscounted votes and incorrectly selected winners); *Kaczmarek v. Microsoft Corp., 39 F. Supp. 2d 974, 977 (N.D. Ill. 1999)* ("[N]othing inherently wrong" with software that is not fully Y2K compliant); *Neilson Bus. Equip. Ctr., Inc. v. Italo V. Monteleone, M.D., P.A., 524 A.2d 1172 (Del. 1987)* (computer system for record keeping not merchantable).

The following software-merchantability cases were collected by Gomulkiewicz, supra at 397 n.24, in 1997:

L.S. Heath & Son, Inc. v. AT&T Info. Sys., Inc., 9 F.3d 561 (7th Cir. 1993); Mesa Bus. Equip., Inc. v. Ultimate Southern California, Inc., 1991 WL 66272 (9th Cir.); Step[#8209]*Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91 (3d Cir. 1991); Sierra Diesel Injection Servs, Inc. v. Burroughs Corp., 874 F.2d 653 (9th Cir. 1989); Neilson Bus. Equip. Ctr., Inc. v. Italo V. Monteleone, 524 A.2d 1172 (Del. 1987); McCrimmon v. Tandy Corp., 414 S.E.2d 15 (Ga. Ct. App. 1991); Harris v. Sulcus Computer Corp., 332 S.E.2d 660 (Ga. Ct. App. 1985); Communications Groups, Inc. v. Warner Communications, Inc., 527 N.Y.S.2d 341 (N.Y. Civ. Ct. 1988); Microsoft Corp. v. Manning, 914 S.W.2d 602 (Tex. Ct. App. 1995).*

Few recent cases involve merchantability issues because software publishers almost universally disclaim the warranty. For cases finding successful disclaimers, see, e.g., *Inter-Mark USA, Inc. v. Intuit, Inc., 2008 U.S. Dist. LEXIS 18834,* at *21-26 (N.D. Cal.); *Performance Chevrolet, Inc. v. Market Scan Info. Sys., Inc., 402 F. Supp. 2d 1166 (D. Idaho 2005); M. Block & Sons, Inc. v. Int'l Bus. Machs. Corp., 2004 WL 1557631* (N.D. Ill.); *Lewis Tree Serv., Inc. v. Lucent Tech. Inc., 239 F. Supp. 2d 322 (S.D.N.Y. 2002); Telecom Int'l Am., Ltd. v. AT & T Corp., 280 F.3d 175 (2d Cir. 2001);* Hou[#8209]*Tex, Inc. v. Landmark Graphics, 26 S.W.3d 103 (Tex. App. 2000); Against Gravity Apparel, Inc. v. Quarterdeck Corp., 267 A.D.2d 44 (N.Y. App. Div. 1999).*

For a discussion of problems with early color televisions, see *Wilson v. Scampoli, 228 A.2d 848 (D.C. 1967)* (seller allowed to cure even though the seller expressly warranted that the television would be free from all defects because of the frequency of the need for adjustment of new color televisions).

For a discussion of the meaning of "defect" in the contract context and its relation to merchantability, see *Denny v. Ford, 662 N.E.2d 730, 736 (N.Y. 1995)* ("the UCC's concept of a 'defective' product requires an inquiry only into whether the product in question was 'fit for the ordinary purposes for which such goods are used' . . . . The latter inquiry focuses on the expectations for the performance of the product when used in the customary, usual and reasonably foreseeable manners.").

With respect to § 3.03(b)(3), UCITA § 403(a)(2)(A) (2002) set forth an implied warranty specific to distributors:

(a) Unless the warranty is disclaimed or modified, a licensor that is a merchant with respect to computer programs of the kind warrants:

* * *

(2) to its distributor that:

(A) the program is adequately packaged and labeled as the agreement requires * * * .

Comment c. Privity. See Magnuson-Moss Warranty Act, *15 U.S.C. § 2308* (a supplier, which, under § 2301(4), includes "any person engaged in the business of making a consumer product directly or indirectly available to consumers," who makes an express warranty cannot disclaim implied warranties).

Many states still require privity to recover for economic loss in implied-warranty cases. See, e.g., *Harris Moran Seed Co., Inc. v. Phillips, 949 So. 2d 916, 922 (Ala. Civ. App. 2006)* ("In Alabama, a vertical nonprivity purchaser who has suffered only direct or consequential economic loss cannot recover from a remote manufacturer under an implied warranty theory."); Anunziato v. e*Machines, Inc., 402 F. Supp. 2d 1133, 1141 (C.D. Cal. 2005)* ("In California, a plaintiff alleging breach of warranty claims must stand in vertical privity with the defendant.") (internal quotations omitted); *Mydlach v. DaimlerChrysler Corp., 846 N.E.2d 126, 140 (Ill. App. Ct. 2005)* ("In order for a plaintiff to file a claim for economic damages under the UCC for the breach of an implied warranty, he or she must be in vertical privity of contract with the seller."); *Monticello v. Winnebago Indus., Inc., 369 F. Supp. 2d 1350, 1361 (N.D. Ga. 2005)* ("In Georgia, a warranty of merchantability clearly arises out of a contract of sale of goods, [and] can only run to a buyer who is in privity of contract with the seller.") (internal quotations omitted); *Haugland v. Winnebago Indus., 327 F. Supp. 2d 1092, 1097 (D. Ariz. 2004)* ("[V]ertical privity of contract between Plaintiff and Defendants is required to assert a U.C.C. implied warranty of merchantability claim . . . ."); *Tex Enters., Inc. v. Brockway Standard, Inc., 66 P.3d 625, 628 (Wash. 2003)* ("[A] plaintiff may not bring an implied warranty action under the UCC without contractual privity.").

But other states do not require privity. See, e.g., *Pack v. Damon Corp., 434 F.3d 810, 820 (6th Cir. 2006)* ("[W]e conclude that Michigan has abandoned the privity requirement for implied[#8209]warranty claims. . . ."); *Goodman v. PPG Indus., Inc., 849 A.2d 1239, 1246 n.6 (Pa. Super. Ct. 2004)* ("[U]nder the Pennsylvania Commercial Code, privity of contract is not required between the party issuing a warranty and the party seeking to enforce the warranty."); *Paramount Aviation Corp. v. Agusta, 288 F.3d 67, 74 (3d Cir. 2002)* ("[W]hat is called 'vertical privity' is not a requirement of a warranty claim under New Jersey UCC law.").

Comment d. Disclaimers. See Cem Kaner, Why You Should Oppose UCITA, 17 Computer Law. 20, 23-24 (2000) (acknowledging need to "reduce publisher risk for losses caused by previously undiscovered defects or defects that were disclosed . . . ."); see also Michael L. Rustad, Making UCITA More Consumer Friendly, 18 J. Marshall J. Computer & Info. L. 547, 550-551, 583-584 (1999) (suggesting minimum adequate remedy for breach of warranty).

Illustration 1 is based on *Teragram Corp. v. Marketwatch.com, Inc., 444 F.3d 1 (1st Cir. 2006).*

Illustration 2 is based on *Lively v. IJAM, Inc., 114 P.3d 487, 492 (Okla. Civ. App. 2005)* (plaintiff who is "knowledgeable in computers and computer software and, additionally, work[s] as a computer technician for local businesses" may be a merchant under the U.C.C.).

Illustration 4 is based on *Vision Graphics v. EI du Pont de Nemours, 41 F. Supp. 2d 93 (D. Mass. 1999).*

Illustrations 5 and 6 are based on *Moore v. Microsoft Corp., 741 N.Y.S.2d 91 (App. Div. 2002).*

§ 3.04 Implied Warranty of Fitness for a Particular Purpose

(a) Unless excluded or modified, if a transferor at the time of contracting has reason to know any particular purpose for which the transferee requires the software and the transferee relies on the transferor's skill or judgment to select, develop, or furnish the software, the transferor warrants that the software is fit for the transferee's purpose.

(b) Unless excluded or modified, if an agreement requires a transferor to provide or select a system of hardware and software and the transferor at the time of contracting has reason to know that the transferee is relying on the skill or judgment of the transferor to select the components of the system, the transferor warrants that the software provided or selected will function together with the hardware as a system.

Comment:

a. Generally. Section 3.04(a) follows U.C.C. § 2-315 and UCITA § 405(a). Under § 2-315, an implied-fitness warranty arises if the seller warrants that goods are fit for a particular purpose, the seller has reason to know the buyer's purpose for wanting the goods, and the buyer relies on the seller's "skill or judgment" to "select or furnish" the goods. The goal of § 2-315 is to protect the buyer's reasonable reliance. Under Article 2, goods can be merchantable (fit for their *ordinary* purpose), but not fit for a *particular* purpose. The key to the "fitness for a particular purpose" warranty, reliance, is not necessary for a merchantability claim to succeed. UCITA § 405(a) is comparable to U.C.C. § 2-315.

Illustration:

1. B, a retailer, tells A, a software developer, that B seeks to acquire software that would facilitate inventory record-keeping, billing, and invoicing. Further, B desires a "single-entry system" that automatically would delete items from inventory when B enters a sales invoice. A tells B that A's new software constitutes a "single-entry system." B therefore acquires the software, but then discovers that the software requires "double-entry." Unless validly excluded, A has breached the implied warranty of fitness for a particular purpose (and also an express warranty).

Section 3.04(a) applies both to general-market software selected by a software transferor and custom-designed software. Transferors of general-market software reasonably may fail to comprehend a transferee's purpose. Nevertheless, the implied-fitness warranty can arise even in general-market transactions if the transferor reasonably should know the transferee's purpose and the transferee relies on the transferor in selecting the particular software.

Illustration:

2. A, a software publisher, transfers to B, owner of a printing business, a copy of A's ClearImage software. Prior to the transfer, B informed A's sales agent that B wanted software that would produce images equal in quality to PhotoClear, the leading software of its type. Further, B told the agent that the software must run on B's Ultra95 operating system. A recommended ClearImage to B and assured B that the software would run on Ultra95. B discovers that ClearImage is incompatible with Ultra95. Unless validly excluded, A has breached an implied warranty of fitness for a particular purpose.

Section 3.04(a) is especially important in the context of custom-designed software because transferees, often lacking in software expertise, frequently rely on the transferor's skill and judgment. If the transferee is educated about software issues, and does not rely on the transferor, however, no implied warranty of fitness arises. As an exception, a sophisticated transferee may rely on the transferor's representations about functions, features, and operation of particular software. In such a case, an implied warranty of fitness may arise.

Illustrations:

3. B, a manufacturer of computer products, foresees the need for additional computer capability. B becomes interested in replacing its "Prime" operating system, but wants to continue using certain business-applications software for accounting and inventory-tracking needs. B explains its needs to A, a software manufacturer, and requests assistance. A
produces operating-system software that it claims will allow B to run its accounting and inventory software. If B's accounting and inventory software do not run on the new operating-system software, B has a claim for breach of the implied warranty of fitness for a particular purpose.

4. B, a supermarket, acquires custom software from A, a software developer, to perform B's cash-register functions on hardware already owned by B. B describes its needs to A, and A writes the software and loads it on the machine. If the software is not compatible with the computer and does not function properly, A has breached the implied warranty of fitness for a particular purpose.

b. Software and hardware selected by the transferor as a system. Section 3.04(a) sets forth a warranty that the software is fit for the transferee's purpose. Section 3.04(b), on the other hand, creates a warranty only that software acquired with hardware will work with the hardware as a system. The Section follows UCITA § 405(c). The transferor does not warrant that the system satisfies any quality needs, only that the software is compatible with the hardware. For example, a "turn-key" system is a package of hardware, software, and services sold together as a package or unit. A transferor selects or develops the software and loads the software on the computer hardware. The transferee may rely on the transferor for the delivery of a working system. If the software is not compatible with the hardware, the implied warranty in § 3.04(b) is broken. In addition, if the software is otherwise materially defective, § 3.04(a) may apply.

Illustration:

5. B, a supermarket, acquires from A a turn-key system consisting of a special-purpose computer and non-embedded software for performing B's cash-register functions. A selected the computer and software and loaded the software on the machine before delivery. If the software does not function properly on the cash register, A has breached the implied warranty that the software is compatible with the hardware. If the software is otherwise defective, A may have breached the implied warranty of fitness for a particular purpose.

c. The transferor's reasonable efforts. UCITA § 405(a)(2) provides: "If from all the circumstances it appears that the licensor was to be paid for the amount of its time or effort regardless of the fitness of the resulting information, the warranty . . . is that the information will not fail to achieve the licensee's particular purpose as a result of the licensor's lack of reasonable effort." These Principles do not include a comparable provision. If fitness of the software was not a condition precedent to payment, then no warranty of fitness would arise-the transferee was not relying on the transferor to furnish software that is fit. Nevertheless, under common law, the transferor must make reasonable efforts to reach the desired results. Further, the transferor has a duty to act in good faith, which duty incorporates the obligation to make reasonable efforts.

REPORTERS' NOTES

Comment a. Generally. Reliance on the transferor is "especially common in the computer industry where many transactions involve custom products and buyers with less experience, or no experience, with the technology. If the buyer is unable or unwilling to obtain outside advice, the seller may undertake the role of consultant and trigger the fitness warranty." Raymond T. Nimmer & Jeff Dodd, Modern Licensing Law § 8:28 (2005). "While the buyer might rely on the sales agent in a general sense, the retail setting seldom supports an implied warranty of fitness and never

supports such a warranty in the classic or straightforward retail sale. The sales environment itself refutes any claim of reasonable reliance on the seller's expertise. The seller's interest in limiting its obligations is strongest here because there are no means to assess thoroughly the buyer's needs and this is apparent to both parties." Id.

Cases decided under Article 2 of the U.C.C. that set forth the purpose and direction of § 2-315 include *Metowski v. Traid Corp., 104 Cal. Rptr. 599, 604 (Ct. App. 1972)* (implied warranty of fitness "arises only where the purchaser at the time of contracting intends to use the goods for a particular purpose; the seller at the time of contracting has reason to know of this particular purpose; the buyer relies on the seller's skill or judgment to select or furnish goods suitable for the particular purpose; and the seller at the time of contracting has reason to know that the buyer is relying on such skill or judgment."); see also *Wallman v. Kelley, 976 P.2d 330, 334 (Colo. Ct. App. 1998)* (no implied-fitness warranty where purchaser decided to buy before conversation with seller); *Keith v. Buchanan, 220 Cal. Rptr. 392, 399 (Ct. App. 1985)* ("The major question in determining the existence of an implied warranty of fitness for a particular purpose is the reliance by the buyer upon the skill and judgment of the seller to select an article suitable for his needs.").

Comment b. Software and hardware selected by the transferor as a system. Commentary on UCITA § 405(c) captures the distinction sought here: § 3.04(b) "is limited to an assurance that the system components will function together as a system. This warranty does not, in itself, serve as a warranty that the system will meet the licensee's needs. . . ." Raymond T. Nimmer & Jeff Dodd, Modern Licensing Law § 8:28 (2005).

Comment c. The transferor's reasonable efforts. For cases delineating the obligation to use best efforts, see, e.g., *Mergentime Corp. v. Wash. Metro. Area Transp. Auth., 400 F. Supp. 2d 145, 228 (D. D.C. 2005)* (failure to use "best efforts" by contractor constitutes default); *New Valley Corp. v. U.S., 119 F.3d 1576, 1584 (Fed. Cir. 1997)* ("The waiver provision was intended to immunize the government from a claim for non[#8209]performance only where it had complied with its contractual duty to use its best efforts. . . ."); *USM v. Arthur D. Little Sys., Inc., 546 N.E.2d 888, 896 (Mass. App. Ct. 1989)* (obligation to use "best efforts" should be construed as in addition to, not in lieu of, transferor's other warranties).

Illustration 1 is based on *Hollingsworth v. The Software House, Inc., 513 N.E.2d 1372 (Ohio Ct. App. 1986).*

Illustration 2 is based on *Innovative Office Sys., Inc. v. Johnson, 906 S.W.2d 940 (Tex. App. 1995).*

§ 3.05 Other Implied Quality Warranties

(a) Unless modified or excluded, implied warranties may arise from course of dealing or usage of trade.

(b) A transferor that receives money or a right to payment of a monetary obligation in exchange for the software warrants to any party in the normal chain of distribution that the software contains no material hidden defects of which the transferor was aware at the time of the transfer. This warranty may not be excluded. In addition, this warranty does not displace an action for misrepresentation or its remedies.

Comment:

a. Course of dealing and usage of trade. Section 3.05(a) follows U.C.C. § 2-314(3). The purpose of the subsection is to clarify that software warranties may arise based on the parties' past dealings or based on a trade practice. These warranties are implied warranties and can be excluded. The definitions of course of dealing and usage of trade may be found in U.C.C. § 1-303 (2008).

Illustration:

1. Over the past 15 years, B, a small business, regularly has acquired various software products from A, a small

software provider. During that time, as is customary, A's technicians have resolved many compatibility issues with B's system at A's own cost. The parties' course of dealing and the trade custom establish an implied warranty that A's software is compatible with B's system and a remedial promise that A will resolve any problems at its own cost.

b. Hidden defects. Subsection (b) creates a nonexcludable implied warranty that the software "contains no material hidden defects of which the transferor was aware at the time of the transfer." The subsection memorializes existing law, including the contract obligation of good faith, the contract duty to disclose, and fraudulent-concealment law. See the Reporters' Notes to this Section citing numerous cases and the Restatement Second of Contracts. The subsection applies if the transferor receives "money or a right to payment of a monetary obligation in exchange for the software." Money is defined by the U.C.C.: a "medium of exchange currently authorized or adopted by a domestic or foreign government." U.C.C.§ 1-201(b)(24) (2008) (former U.C.C. § 1-201(24)). A right to payment of a monetary obligation means that the transaction does not involve an immediate transfer of currency, but the transferor receives a monetary equivalent in exchange for the software, such as a payment by credit or debit card or check or draft, or a contractual commitment to pay for related consideration such as services. See also U.C.C. § 9-102(a)(2). Section 3.05(b) does not apply if the transferor works for a large organization that compensates the transferor for its general efforts, but the transferor does not receive money or a monetary obligation directly from the transferee in exchange for the software.

The nature of software means that end users should not expect perfection. Several Sections of these Principles shield software providers from inordinate liability, such as by enforcing disclaimers and remedy limitations. However, software transferors should have a duty to disclose known material hidden defects in order to allocate those risks to the party best able to accommodate or avoid them. Hidden material defects, known to the software transferor but not disclosed, shift costs to the transferee who cannot learn of the defects until it is too late and therefore cannot protect itself.

Section 3.05(b) requires that the transferor know of the defect at the time of the transfer, the defect is material, and it is hidden. The *time of the transfer* is the time of conveyance of rights in the software or of authorization to access software. See § 1.01(m). If a transferor delivers a new version of software pursuant to an existing contract, the time of the transfer of the new version is the time of delivery. However, the transferor makes a § 3.05(b) warranty only with respect to the new version. The transferor is not liable under this Section for material defects in the original version if it did not know of them at the time of the transfer of the original version.

A *material* defect consists of a software error serious enough to constitute a material breach of the contract. Section 3.11 of these Principles and the well-established common-law material-breach doctrine, which ask whether the injured party received substantially what it bargained for and reasonably expected, inform the court's decision on whether a defect is material. Software that requires major workarounds to achieve contract-promised functionality and that causes long periods of downtime or never achieves promised functionality ordinarily would constitute a material defect.

A *hidden* material defect means that the defect would not surface upon any testing that was or should have been performed by the transferee. See § 3.06(e) of these Principles. Negligence on the part of transferors in failing to discover defects is not covered by the Section and is the subject of products-liability law. Nor does the subsection displace the law of misrepresentation, which applies to affirmative statements meant to deceive. As with fraudulent-concealment law, ordinarily § 3.05(b) should require an intent to deceive, which may be inferred if a transferor licenses software it knows is materially defective and knows the user cannot discover it upon an inspection.

Disclosure of a material hidden defect occurs when a reasonable transferee would understand the existence and basic nature of the defect. Disclosure ordinarily should involve a direct communication to the transferee, if feasible. A mere posting of defects on the transferor's website may be insufficient depending on the circumstances. Ultimately, the type of disclosure that would make a reasonable transferee aware of the defect is heavily context dependent and should

be developed by the courts.

Putting together the requirements of transferor actual knowledge of the defect at the time of the transfer, transferee reasonable lack of knowledge, and a defect that constitutes a material breach means that a transferor would not be liable if the transferor has received reports of problems but reasonably has not had time to investigate them, if the transferee's problems are caused by uses of which the transferor is unaware, if the transferor learns of problems only after the transfer, and if the problems are benign or require reasonable workarounds to achieve functionality.

On the other hand, an "as is" clause or the like would not insulate a transferor from liability. Unlike other implied warranties, the warranty of no hidden material defects may not be excluded. Case law supports the proposition that a party cannot contract away responsibility for fraud. Further, a reasonable transferee, assuming the good faith of the transferor, would believe an "as is" clause means that the transferor does not intend to make any express warranties or implied warranties of merchantability or fitness, not that the licensor may know that the software is materially defective so that the software will be largely worthless to the licensee. But a transferor can disclose the material defect to insulate itself from liability. In addition, presumably software providers, influenced by reputational concerns, would hesitate to exclude liability for defects of which they are aware. Instead, they would disclose defects to insulate themselves from liability under subsection (b).

The Principles take no position on transferor liability for failing to disclose material hidden defects if the transferor does not receive money or a right to payment of a monetary obligation for the software, such as many collaborators in the open-source community. Open-source development is often a large, diverse group effort, and individual contributors often contribute to a work-in-progress. These developers may have no knowledge whether a specific bug in the software is important for a particular application. Further, open-source software typically is available for download at any time, notwithstanding its nature as a work-in-progress. Such characteristics make it unwise to extend the non-disclaimable warranty to these open-source collaborators as a matter of law. But at minimum, tort or other law applies to open-source collaborators who intentionally include malicious, hidden code that corrupts the software.

Illustrations:

2. B, a manufacturer of computer products, foresees the need for additional computer capability. B becomes interested in replacing its "Prime" operating system with an "Ultrix" system, but wants to continue using certain business-applications software for accounting and inventory tracking needs. This software is not compatible with the Ultrix system, so B acquires software from A called "uniVerse " that A claims in advertising and in statements to B will allow B to run its accounting and inventory software on the Ultrix system. At the time of the transfer of the uniVerse software, A knows of a defect in uniVerse that causes severe problems with its use on an Ultrix system. In fact, B encountered difficulties using uniVerse almost immediately so that B could not run its accounting and inventory software on the Ultrix system and was not able to fix the problems. A has breached an express warranty and has misrepresented the capabilities of its product. A also has breached the implied warranty of no material hidden defects.

3. Same facts as Illustration 2, except that A has disclaimed all warranties and has transferred the software to B "as is." A has breached the implied warranty of no material hidden defects.

4. Company A markets software for preparing construction bids. In a negotiated exchange in which A disclaims all warranties, Company B acquires the software and uses it to submit a bid. B loses a business opportunity because the software is defective and causes an inaccurate bid. An internal memo of A, written prior to the transfer, notes that a material bug exists in the software. A knew of the bug and failed to disclose it. A has breached the implied warranty of no material hidden defects. If A's only knowledge of the bug was internal documentation describing a minor bug, A has not breached the warranty even if the bug is material.

5. Company A licenses software for modeling automobile aerodynamics. Company B is an automobile manufacturer. A and B, at arms-length and each assisted by counsel, negotiate a custom agreement including a clause

stating that A will disclose material defects on a secure website, accessible only by B. At the time of the sale, A knows of several minor defects in the software that hinder performance, but do not prevent the software from substantially performing its purpose. A does not post these defects on its website. A has not breached the implied warranty of no material hidden defects because the defects are not material.

6. Same facts as Illustration 5, except that, in addition to the minor defects, A knows of a major defect that prevents the software from properly modeling airflow around cars. A discloses this defect on its website pursuant to its agreement with B. A has not breached the implied warranty of no material hidden defects because A properly disclosed the defect because the parties bargained at arms length and made a custom agreement that included the method of disclosure used by A.

7. Same facts as Illustration 6, except that A is unaware of the material defect in the software and so posts nothing on its website. A has not breached the implied warranty of no material hidden defects because A was not aware of the material defect at the time of the transfer.

8. Same facts as Illustration 6, except that A has found the material defect, but mistakenly believes the defect to be minor and so posts nothing on its website. A has not breached the implied warranty of no material hidden defects because A was not aware of the materiality of the defect at the time of the transfer.

REPORTERS' NOTES

Comment a. Course of dealing and usage of trade. U.C.C. § 2-314(3), Comment 12, states in part that course of dealing and trade custom "can create warranties . . . that . . . are implied rather than express warranties and thus subject to exclusion or modification under Section 2-316."

Comment b. Hidden defects. Under the common law, a contracting party must disclose material facts if they are under the party's control and the other party cannot reasonably be expected to learn the facts. Failure to disclose in such circumstances may amount to a representation that the fact does not exist and may be fraudulent. See, e.g., *Hill v. Jones, 725 P.2d 1115, 1118-1119 (Ariz. Ct. App. 1986)* ("[U]nder certain circumstances there may be a 'duty to speak.'. . . [N]ondisclosure of a fact known to one party may be equivalent to the assertion that the fact does not exist . . . . Thus, nondisclosure may be equated with and given the same legal effect as fraud and misrepresentation."). The Restatement Second of Contracts § 161(b) supports the *Hill* dictum: "A person's non-disclosure of a fact known to him is equivalent to an assertion that the fact does not exist . . . where he knows that disclosure of the fact would correct a mistake of the other party as to a basic assumption on which that party is making the contract and if non-disclosure of the fact amounts to a failure to act in good faith and in accordance with reasonable standards of fair dealing." Section 161, Comment *d*, of the Restatement Second adds: "In many situations, if one party knows that the other is mistaken as to a basic assumption, he is expected to disclose the fact that would correct the mistake. A seller of real or personal property is, for example, ordinarily expected to disclose a known latent defect of quality or title that is of such a character as would probably prevent the buyer from buying at the contract price."

The duty to disclose arises in a multitude of contract settings. See, e.g., *Janel World Trade, Ltd. v. World Logistics Servs., Inc., 2009 WL 735072*, at *10 (S.D.N.Y. 2009) ("A duty to disclose between negotiating parties arises . . . where 'one party has superior knowledge of certain information, that information is not readily available to the other party, and the first party knows that the second party is acting on the basis of mistaken knowledge.'"); *Suzlon Wind Energy Corp. v. Shippers Stevedoring Co., 2009 WL 197739*, at *15 (S.D. Tex. 2009) ("A party fraudulently induced to consent to a contract is not bound by the contract's terms and may rescind the entire contract. . . . Fraud can be by either misrepresentation or passive silence."); *Holman v. Howard Wilson Chrysler Jeep, Inc., 972 So. 2d 564, 568 (Miss. 2008)* ("The duty to disclose is based upon a theory of fraud that recognizes that the failure of a party to a business transaction to speak may amount to a suppression of a material fact which should have been disclosed and is,

in effect, fraud."); *Hess v. Chase Manhattan Bank, USA, 220 S.W.3d 758, 765 (Mo. 2007)* ("A duty to speak arises where one party has superior knowledge or information that is not reasonably available to the other."); *Bear Hollow, L.L.C. v. Moberk, L.L.C., 2006 WL 1642126 (W.D.N.C. 2006)* ("[A] party negotiating at arm's length has a duty to disclose . . . where one party has knowledge of a latent defect in the subject matter of the negotiations of which the other party is ignorant and which it is unable to discover through reasonable diligence."); *Kaloti Enters., Inc. v. Kellogg Sales Co., 699 N.W.2d 205, 213 (Wis. 2005)* ("We conclude that a party to a business transaction has a duty to disclose a fact where: (1) the fact is material to the transaction; (2) the party with knowledge of that fact knows that the other party is about to enter into the transaction under a mistake as to the fact; (3) the fact is peculiarly and exclusively within the knowledge of one party, and the mistaken party could not reasonably be expected to discover it; and (4) on account of the objective circumstances, the mistaken party would reasonably expect disclosure of the fact."); *Cirillo v. Slomin's Inc., 768 N.Y.S.2d 759, 765 (Sup. Ct. 2003)* ("Upon the facts alleged in this case, the Court can infer that Slomin's had superior knowledge regarding the capabilities of its own alarm system, which knowledge was unavailable to plaintiffs through ordinary inspection, and which was material to the plaintiffs' decision to enter into the Contracts with Slomin's or to forego alternatives that might have provided more effective or complete protection. This superior knowledge gives rise to a duty to disclose which, in turn, supports a cause of action for fraud in the event of its breach, either by non-disclosure or by misrepresentation."); *Everts v. Parkinson, 555 S.E.2d 667, 672 (N.C. Ct. App. 2001)* ("[W]here a material defect is known to the seller, and he knows that the buyer is unaware of the defect and that it is not discoverable in the exercise of the buyer's diligent attention or observation, the seller has a duty to disclose the existence of the defect to the buyer.") (quoting *Carver v. Roberts, 337 S.E.2d 126, 128 (N.C. Ct. App. 1985)); Shapiro v. Sutherland, 76 Cal. Rptr. 2d 101, 107 (Cal. Ct. App. 1998)* ("Generally, where one party to a transaction has sole knowledge or access to material facts and knows that such facts are not known or reasonably discoverable by the other party, then a duty to disclose exists."); *Johnson v. Davis, 480 So. 2d 625, 629 (Fla. 1985)* ("[W]here the seller of a home knows of facts materially affecting the value of the property which are not readily observable and are not known to the buyer, the seller is under a duty to disclose them to the buyer.").

For a discussion of the concept of materiality in the context of material breach, see Restatement Second, Contracts § 241.

In *Vmark Software Inc. v. EMC Corporation, 642 N.E.2d 587, 596-597 (Mass. App. 1994)* (citations omitted), the transferee counterclaimed due to defective software. The court stated:

> Delivery of a defective product without revealing the defects, to the extent they are known and material, is surely market disruptive to the same extent whether the promisor is genuinely hopeful of eventually fulfilling his contract . . . or is deliberately deceptive and entirely disdainful of his commitments. . . . Nonetheless, the fault of the former-which smacks more (the trial judge's off-hand conclusion notwithstanding) of gross negligence than of intentional fraud . . . is markedly less damnable than that of the latter.

(The court refused to give double or treble damages, believing that Vmark's conduct was not "entirely disdainful of [its] commitments." *Id. at 597).*

In *M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305 (Wash. 2000),* an internal memo of Timberline suggested that a bug found in the software "does not appear to be a major problem." *Id. at 309.* The case sheds light on how a court could determine whether a transferor knew of a defect and whether it was material.

The Restatement Second of Contracts § 161 applies the law of fraudulent concealment. *Gibb v. Citicorp Mortgage, Inc., 518 N.W.2d 910, 916 (Neb. 1994)* sets forth the elements of fraudulent concealment:

In order to maintain an action based on fraudulent concealment, the plaintiff must allege and prove the following elements: (1) that the defendant concealed or suppressed a material fact; (2) that the defendant had knowledge of this material fact; (3) that this material fact was not within the reasonably diligent attention, observation, and judgment of the plaintiff; (4) that the defendant suppressed or concealed this fact with the intention that the plaintiff be misled as to the true condition of the property; (5) that the plaintiff was reasonably so misled; and
(6) that the plaintiff suffered damage as a result.

Concealment includes "silence in the face of a duty to speak. Thus, one is equally culpable of fraud who by omission fails to reveal that which it is his duty to disclose . . . ." *Stephenson v. Capano Dev., Inc., 462 A.2d 1069, 1074 (Del. 1983).*

Disclaimers and "as is" clauses often do not preclude claims of fraud. See, e.g., *Limoge v. People's Trust Co., 719 A.2d 888, 891 (Vt. 1998); Gibb, supra.*

See generally Cem Kaner, Why You Should Oppose UCITA, 17 Computer Law. 20, 23 (2000). According to Kaner, "[i]n mass-market software, a large proportion of defects (often the vast majority of them) that reach customers are discovered and intentionally left unfixed by the publisher before the product is released." Id. at 23. But § 3.05(b) applies only if the unfixed defect is material.

Illustration 1 is based on *Gindy Mfg. Corp. v. Cardinale Trucking Corp., 268 A.2d 345 (N.J. Super. Ct. Law Div. 1970).*

Illustrations 2 and 3 are based on *Vmark Software, Inc. v. EMC Corp., 642 N.E.2d 587 (Mass. App. 1994)* ("Delivery of a defective product without revealing the defects, to the extent they are known and material, is surely market disruptive . . . .").

Illustration 4 is based on *M.A. Mortenson, supra* (internal memo of software publisher notes that a "bug has been found").

§ 3.06 Disclaimer of Express and Implied Quality Warranties

(a) A statement intending to exclude or modify an express quality warranty is unenforceable if a reasonable transferee would not expect the exclusion or modification.

(b) Unless the circumstances suggest otherwise, all implied quality warranties other than the warranty of no material hidden defects (§ 3.05(b)) are excluded by language in a record communicated to the transferee such as "as is," "with all faults," or other language that a reasonable transferee would believe excludes all implied quality warranties.

(c) The implied warranty of merchantability is excluded if the exclusion is in a record communicated to the transferee, is conspicuous, and mentions "merchantability."

(d) The implied warranty of fitness for a particular purpose is excluded if the exclusion is in a record communicated to the transferee, is conspicuous, and mentions "fitness for a particular purpose."

(e) If before entering an agreement a transferee has tested the software as fully as desired or unreasonably has refused to test it, there are no implied quality warranties with regard to defects that a test should have or would have revealed.

(f) An implied quality warranty other than the warranty of no material hidden defects (§ 3.05(b)) may be excluded or modified by course of performance, course of dealing, or usage of trade.

(g) Remedies for breach of quality warranties may be limited in accordance with § 4.01 of these Principles.

Comment:

a. Disclaiming express warranties. Section 3.06(a) clarifies the approach of U.C.C. § 2-316(1), which governs the exclusion or modification of express warranties in the sale-of-goods context. Section 2-316(1) directs courts to attempt to construe language creating and nullifying express warranties consistently. Failing that, courts must find the seller responsible for any inconsistencies between words or conduct creating and negating warranties. This approach causes confusion: How can language or conduct of warranty ever be "consistent" with language of disclaimer? The approach of § 2-316(1) is better understood by reading the explanation in § 2-316, Comment 1: Section 2-316(1) is meant to "protect a buyer from unexpected and unbargained language of disclaimer . . . ." Section 3.06(a) follows this comment, but omits the superfluous "unbargained" language.

The relative clarity, distinctiveness, and conspicuousness of language or acts of warranty and language of disclaimer help determine whether a disclaimer should be unexpected. For example, a disclaimer may be unexpected notwithstanding its conspicuousness if the warranty is clear and definitive. If a contract states definitively that software is "compatible with Windows Vista," but also disclaims all express and implied warranties, a reasonable transferee would not expect the disclaimer to apply to the statement and the disclaimer falls out of the contract. Similarly, if the transferor clearly describes the software as "word-processing software," a reasonable transferee would not expect a disclaimer to absolve the transferor of responsibility if the software consists of a low-level word game. On the other hand, if the transferor made statements during negotiations that would otherwise constitute express warranties, but the transferor takes pains to explain to the transferee that the transferor has decided not to make warranties and includes terms in the contract to that effect, a reasonable transferee would believe the transferor has disclaimed any express warranties.

Additional factors in determining whether a disclaimer is reasonably unexpected include whether the transferee drafted or helped draft the contract, and whether the transferee had actual knowledge of the disclaimer. As to the latter, if the transferor points out the disclaimer and the transferee therefore has actual knowledge of it before committing to the transfer, a reasonable transferee standing in the shoes of the transferee would not be surprised by the disclaimer.

Section 3.06(a) renders disclaimers of express warranties unenforceable if reasonably unexpected, but first there must be an express warranty. Thus, as with sales law, these Principles require a determination of what a reasonable transferee would believe about the sum total of words and conduct of the transferor of software to see whether an express warranty has arisen. See § 3.02. Further, as with U.C.C. § 2-316(1), evidence of an express warranty must be admissible under the parol-evidence rule. Suppose, for example, the transferee alleges that the transferor made a "free of all bugs" warranty orally before the parties signed a contract that disclaims all warranties express or implied. The parol-evidence rule may bar the admissibility of the express oral warranty. On the other hand, a transferor should not be able to use the parol-evidence rule as part of a strategy to confuse or surprise a transferee. See § 3.08 of these Principles.

Illustrations:

1. B, a consumer, acquires WordHappy, a packaged word-processing program provided by A. The back of the box states that the software "Contains lots of amazing fonts for fun and creative work!" The electronic standard form states: "A DISCLAIMS ALL EXPRESS WARRANTIES OTHERWISE CREATED ON THE PACKAGING OF THIS PROGRAM." B uses the program for a month, and then brings an action for breach of express warranty, arguing that WordHappy included only 25 fonts, while its competitors each had at least 50 fonts. The explicit and plain-English disclaimer excludes any express warranty that potentially arose from the box's vague and casual representation.

2. After testing, B, a large manufacturer of hot-dog buns, negotiates with A, a leading software manufacturer, for the transfer of 1000 copies of A's RecipeMaker program. Subsequently, over several months, a team of lawyers from each company draft a contract that includes the following provision: "TRANSFEROR DISCLAIMS ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY REGARDING THE COMPATIBILITY OF RECIPEMAKER WITH THE ULTRA95 OPERATING SYSTEM." Subsequently, B brings an action for breach of express warranty, arguing that the "test" copy of RecipeMaker ran on B's Ultra95 system, whereas the final program does not. B argues that RecipeMaker is therefore unsuitable for use in its operation. B's claim should fail because B is a sophisticated business with significant bargaining power and B negotiated the terms of the contract. The disclaimer should not be unexpected and is therefore enforceable.

b. Disclaiming implied warranties. Sections 3.06(b) through 3.06(f) clarify the approach of U.C.C. § 2-316(2) and (3). The U.C.C. sections set forth various methods of disclaiming implied warranties. According to § 2-316(2), to disclaim the implied warranty of merchantability, the seller must mention the term "merchantability" by name, and, if in a writing, the disclaimer must be conspicuous. The seller's disclaimer of the implied warranty of fitness for a particular purpose under § 2-316(2) must be in a conspicuous writing, but the seller does not have to use the words "fitness for a particular purpose." But U.C.C. § 2-316(3) offers additional avenues of disclaimer, less detailed than subsection (2): A seller can disclaim all implied warranties by including language such as "as is," "with all faults," or the like. The seller does not have to mention merchantability or disclaim conspicuously after all. Confusion about modes of disclaimer may arise primarily because of the order of presentation of disclaimers in the U.C.C. Instructions are particular in subsection (2), suggesting that these are the sole strategies of disclaimer, and general in subsection (3). For clarity, § 3.06 reverses the order, first setting forth general modes of disclaimer and then proceeding to the specific safe harbors.

Section 3.06(b) follows the principle that a transferee should not receive implied-warranty protection if the transferee should have known from the language of a disclaimer that the contract affords no such protection. In addition, some courts have enforced implied-warranty disclaimers in sale-of-goods cases, even if inconspicuous or vague, if the purchaser had actual knowledge of the transferor's intent to disclaim. Such a result is possible under the "unless the circumstances suggest otherwise" preamble of § 3.06(b). The preamble also means that in some situations "as is" or similar language is not sufficient to exclude implied warranties, such as where the contract contains language that contradicts the disclaimer of implied warranties.

Section 3.06(c) sets forth a safe harbor for transferors, so long as the merchantability disclaimer is in a record, mentions "merchantability," and is conspicuous. Section 3.06(d) also is a safe harbor. Unlike U.C.C. § 2-316(2), however, the disclaimer must mention "fitness for a particular purpose." The "conspicuous" requirement is well-rehearsed in the jurisprudence of Article 2 and no elaboration is necessary. For example, the U.C.C.'s definition of "conspicuous" suffices here: "A term or clause is conspicuous when it is so written that a reasonable person against whom it is to operate ought to have noticed it. A printed heading in capitals . . . is conspicuous. Language in the body of a form is 'conspicuous' if it is in larger or other contrasting type or color." U.C.C.§ 1-201(10). Section 1-201(b)(10) of Amended Article 1 elaborates, but the thrust is the same.

In a software transfer governed by an electronic contract, the transferor can bury a disclaimer of warranties several screens into the contract. In this instance, the location of the disclaimer weighs heavily in determining whether it is conspicuous. The test is nonetheless the same: Would the placement call the disclaimer to a reasonable transferee's attention? The likely answer is "no" if the disclaimer is not displayed on one of the first few screens.

Sections 2-316(3)(b) and 2-316(3)(c) of the U.C.C. set forth disclaimers based on the buyer's inspection of (or unreasonable refusal to inspect) the goods, and based on "course of dealing," "course of performance," or "usage of trade." Under § 2-316(3)(b), a seller must demand that the buyer inspect the goods; mere availability of the goods is insufficient. Further, the demand must put a reasonable buyer on notice that the buyer assumes the risk of defects the

inspection should reveal. In addition, the section accounts for the relative skill level of the buyer: "A professional buyer examining a product . . . will be held to have assumed the risk as to all defects which a professional in the field ought to observe, while a nonprofessional buyer will be held to have assumed the risk only for such defects as a layman might be expected to observe." U.C.C. § 2-316, Comment 8. Finally, the buyer's failure to inspect must be unreasonable. Section 3.06(e) of these Principles adopts all of these considerations in determining whether software implied warranties are excluded due to a test or failure to test the software. Further, if the transferee reasonably should have discovered defects under this Section, the defects are not hidden and the implied warranty of no hidden material defects, § 3.05(b), would not apply.

Under U.C.C. § 2-316(3)(c), if a seller and buyer repeatedly enter "as is" contracts prior to the transaction at issue that is silent on warranties, they may have established a course of dealing. If so, a court should interpret a new sale also "as is," unless the parties expressly draft otherwise. Section 3.06(f) of these Principles follows this approach as well. In addition, as pointed out in the Summary Overview to Topic 1 of this Chapter, the nature of open-source production and distribution means that transferees should not expect warranty coverage if the regular practice of open-source transferors "in a place, vocation or trade" is to transfer software "as is." See U.C.C. § 1-205(2). For example, a transferee who downloads open-source software from an Internet site that offers free downloads normally should expect "as is" software.

Illustrations:

3. B, a high-school math teacher, acquires packaged software manufactured by A. The written agreement contains an "as is" disclaimer and a disclaimer of the implied warranties of merchantability and fitness for a particular purpose. The disclaimers of the implied warranties are in the same font size, type, and color as the rest of the contract. These disclaimers are not conspicuous and thus ineffective under §§ 3.06(c) and 3.06(d), but the § 3.06(b) disclaimer may be effective. An "as is" disclaimer is not a safe harbor, however, because § 3.06(b) begins, "[u]nless the circumstances suggest otherwise." This preamble means that in some situations "as is" or similar language is not sufficient to exclude implied warranties, such as where the contract contains language that contradicts the disclaimer of implied warranties.

4. B, a carpenter, acquires packaged software manufactured by A. The written agreement contains the following instruction on the front of the contract in capital letters: "ADDITIONAL TERMS ON BACK." The back of the contract contains a disclaimer of implied warranties of merchantability and fitness in the eighth of sixteen paragraphs, with no heading, and in 7-point font, compared to 12-point font on the front and 5-point font on the rest of the back of the contract. The disclaimer of warranties is not conspicuous and thus ineffective under §§ 3.06(c) and 3.06(d).

5. B, a small software-engineering firm, downloads, without charge, open-source software from A, another software-engineering firm active in the open-source movement. Both A and B are aware that open-source software ordinarily is transferred "as is." The software contains bugs, but B is without implied-warranty protection.

c. Modification of software negates all warranties. UCITA § 407 provides that a "licensee that modifies a computer program . . . invalidate[s] any warranties, express or implied, regarding performance of the modified copy." These Principles do not include an equivalent rule in the black letter on the theory that such a rule is unnecessary. Unless the transferor warrants that the software will achieve the represented purposes even if modified, the transferor has not broken any express warranty when the copyholder modifies or reverse engineers the software and it does not work. Similarly, the merchantability warranty applies to software that the transferor delivers, not to modified software, unless the particular software's ordinary purpose includes modification. Finally, the fitness-for-a-particular-purpose warranty would not be broken if the copyholder alters the software so that it does not achieve its purpose.

Illustrations:

6. B, a major accounting firm, orders custom accounting software from A. After taking delivery of the source code,

B modifies the source code to add several new features and integrates them into the features of the accounting software. The modified software proves unreliable on B's computers. B's modification has invalidated all warranties from A.

7. B, a high-school math teacher, acquires packaged spreadsheet software manufactured by A. After using the software for several days, B creates a number of templates as described in the software documentation and alters a variety of the software's default preferences to make the software function more efficiently. The software stops working. B's modification of the default preferences does not constitute modification of the software and any applicable warranties continue to apply.

REPORTERS' NOTES

Comment a. Disclaiming express warranties. An early U.C.C. Article 2 draft denied enforcement to disclaimers of express warranties. See J. White & R. Summers, Uniform Commercial Code 425 (5th ed. 2000). White and Summers also remark that, under the current version of Article 2, "[i]f the factfinder determines that a seller's statement created an express warranty, words purportedly disclaiming that warranty will still be 'inoperative,' for the disclaiming language is inherently inconsistent." Id. at 425. Comment 1 to § 2-316 states that § 2-316(1) is supposed to "protect a buyer from unexpected and unbargained language of disclaimer by denying effect to such language when inconsistent with language of express warranty . . . ." Many cases follow the comment. See, e.g., *Manitowoc Marine Group, LLC v. Ameron Int'l Corp., 424 F. Supp. 2d 1119, 1132-1133 (E.D. Wis. 2006); Morningstar v. Hallett, 858 A.2d 125, 130 (Pa. Super. Ct. 2004); S. Energy Homes, Inc. v. Washington, 774 So. 2d 505, 512*-513 (Ala. 2000).

Case law generally favors express warranties over disclaimers. See, e.g., *Bell Sports, Inc. v. Yarusso, 759 A.2d 582, 593 (Del. 2000)* ("The restrictive provision of [§ 2-316(1)] renders Bell's effort to disclaim any express warranties in the manual's 'Five Year Limited Warranty' ineffective as a matter of law."); *James River Equip. Co. v. Beadle County Equip., Inc., 646 N.W.2d 265, 271 (S.D. 2002)* ("The UCC contemplates that only implied warranties can be disclaimed by use of 'as is' clauses . . . . The official comment to that section confirms its plain meaning, i.e., that '[o]nly implied-not express-warranties are excluded in "as is" transactions.'") (quoting *Tenwick v. Byrd, 659 S.W.2d 950, 952 (Ark. Ct. App. 1983)); Hercules Mach. Corp. v. McElwee Bros., 2002 WL 31015598*, at *6 (E.D. La.) ("[Section 2-316] expressly provides that negation or limitation of an express warranty is 'inoperative' if inconsistent with the seller's representation of an express warranty . . . . The Court finds it impossible to read Hercules' express warranty and Hercules' waiver of an express warranty as consistent with each other . . . . [T]his conflict renders Hercules' waiver of express warranties inoperative."); *Bushendorf v. Freightliner Corp., 13 F.3d 1024, 1027 (7th Cir. 1993)* ("[Section 2-316(1)] has been understood to forbid the complete negation of an express warranty . . . . [I]f the parties have negotiated an express warranty, a clause in the same contract disclaiming it . . . suggests some deep confusion which may warrant reparative efforts by the court."); *Providence & Worcester R.R. Co. v. Sargent & Greenleaf, Inc., 802 F. Supp. 680, 688 (D. R.I. 1992)* ("Generally a seller may not disclaim an express warranty."); *Duffin v. Idaho Crop Improvement Ass'n, 895 P.2d 1195, 1205 n.8 (Idaho 1995)* ("[E]xpress warranties are virtually impossible to disclaim under the Code."); *Hartman v. Jensen's, Inc., 289 S.E.2d 648, 649 (S.C. 1982)* ("[P]lacing alleged disclaimer under the bold heading of 'Terms of Warranty' created an ambiguity and was likely to fail to alert the consumer that an exclusion of the warranty was intended."); *Ritchie Enters. v. Honeywell Bull, Inc., 730 F. Supp. 1041 (D. Kan. 1990)* (express warranties hard to disclaim); *Consol. Data Terminals v. Applied Digital Data Sys., Inc., 708 F.2d 385 (9th Cir. 1983)* (specific express warranty prevails over general disclaimer); see also *Sierra Diesel Injection Serv., Inc. v. Burroughs Corp., 874 F.2d 653 (9th Cir. 1989).*

Notwithstanding this trend, sufficient confusion in the case law suggests the need for clarification in the black letter. For example, some courts seem not to understand the charge of § 2-316. See, e.g., *Kolle v. Mainship Corp., 2006 WL 1085067*, at *3 (E.D.N.Y.) ("UCC § 2-316, however, authorizes the exclusion of both express and implied warranties so long as the exclusion is specific, clear, and timely."); *Naftilos Painting, Inc. v. Cianbro Corp., 713 N.Y.S.2d 626, 627 (App. Div. 2000)* ("The court further erred in failing to dismiss the fourth and fifth causes of action,

predicated upon the breach of express and implied warranties of fitness of use for a particular purpose. Each of the invoices reflecting the sale of paint and paint thinner by defendant to plaintiff contained a conspicuous and thus effective disclaimer of all warranties . . . ."); *Travelers Ins. Cos. v. Howard E. Conrad, Inc., 649 N.Y.S.2d 586, 587 (App. Div. 1996)* ("The type size of the waiver provision is larger than that contained elsewhere on the back of the agreement, and it stands out in capital letters. In our view, a reasonable person would notice the provision 'when its type is juxtaposed against the rest of the agreement.' Thus, the provision waiving all warranties, express and implied, is conspicuous and therefore enforceable.") (quoting *Commercial Credit Corp. v. CYC Realty, 477 N.Y.S.2d 842, 844 (App. Div. 1984)); Ekizian v. Capurro, 444 N.Y.S.2d 361, 362 (Just. Ct. 1981)* (suggesting an "inconsistent" disclaimer would have trumped express warranty); *Bernstein v. Sherman, 497 N.Y.S.2d 298, 300-301 (Just. Ct. 1986)* (written disclaimer trumps express warranty).

For sales cases delineating the meaning of "expected" or "unexpected" disclaimers, see, e.g., *Bell Sports, Inc. v. Yarusso, 759 A.2d 582, 593 (Del. 2000)* ("While [seller's] manual contains disclaimers warning potential users that the helmet cannot prevent all injuries, other representations were made to assure a potential buyer that the helmet's liner was designed to reduce the harmful effects of a blow to the head. Those representations constituted essential elements of a valid express warranty that may not be effectively disclaimed as a matter of law."); *Betaco, Inc. v. Cessna Aircraft Co., 103 F.3d 1281, 1287*-1289 (7th Cir. 1996) (expected disclaimer was conspicuously "highlighted by capitalized lettering"; further purported warranties were "ambiguous" and "casual"); *Klickitat County Pub. Util. Dist. No. 1 v. Stewart & Stevenson Servs., Inc., 2006 WL 908042*, at *11 n.5 (E.D. Wash.) ("Given the sophistication of the parties and extensive negotiations which occurred, KPUD is not the sort of buyer [§ 2-316(1)] was meant to protect."); *Hayes v. Bering Sea Reindeer Prods., 983 P.2d 1280, 1286 (Alaska 1999)* ("A seller cannot negate express warranties through generalized disclaimers. But the clear, forceful, specific disclaimer in this contract defeats . . . any [claim of] enforceable express warranty. This is not a fine-print boilerplate disclaimer which NCI could not have negotiated or understood; it is a conspicuous, clearly written provision in a two-page contract between parties with equal bargaining power."); *Appalachian Ins. Co. v. McDonnell Douglas Corp., 262 Cal. Rptr. 716, 736 (Ct. App. 1989)* ("[I]t cannot be said the disclaimer language in the written contract with McDonnell Douglas was 'unexpected,' 'unbargained for' or a 'surprise' since Western Union negotiated the language contained in article 7 and itself drafted article 14 which waived claims against McDonnell Douglas's contractors and subcontractors, including claims against Morton Thiokol.").

Comment b. Disclaiming implied warranties. See generally U.C.C. §§ 2-316(2) and 2-316(3) and UCITA § 406, on which § 3.06 is based.

Software providers almost universally disclaim the implied warranty of merchantability. See, e.g., *Inter-Mark USA, Inc. v. Intuit, Inc., 2008 U.S. Dist. LEXIS 18834*, at *21-26 (N.D. Cal.); *Performance Chevrolet, Inc. v. Mkt. Scan Info. Sys., Inc., 402 F. Supp. 2d 1166 (D. Idaho 2005); M. Block & Sons, Inc. v. IBM, 2004 WL 1557631* (N.D. Ill.); *Lewis Tree Serv., Inc. v. Lucent Techs. Inc., 239 F. Supp. 2d 322 (S.D.N.Y. 2002); Telecom Int'l Am., Ltd. v. AT & T Corp., 280 F.3d 175 (2d Cir. 2001); Hou-Tex, Inc. v. Landmark Graphics, 26 S.W.3d 103 (Tex. App. 2000); Against Gravity Apparel, Inc. v. Quarterdeck Corp., 267 A.D.2d 44 (N.Y. App. Div. 1999).*

Some states preclude exclusion of implied warranties in consumer contracts. For example, Maryland's version of UCITA contains the following amendment: "Any oral or written language used in a consumer contract, which attempts to exclude or modify any implied warranties of merchantability of a computer program . . . or implied warranties of fitness for a particular purpose . . . or exclude or modify the consumer's remedies for a breach of those warranties, is unenforceable." Md. Code Ann., Com. Law § 22-406(i)(1) (2005).

As to what is conspicuous, Amended U.C.C. § 1-201(b)(10) offers some examples:

[A] heading in capitals equal to or greater in size than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same or lesser size; and language in the body of a record or display in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from surrounding text of the same size by symbols or other marks that call attention to the language.

Case law on what is conspicuous includes *Recursion Software, Inc. v. Interactive Intelligence, Inc., 425 F. Supp. 2d 756 (N.D. Tex. 2006); Sierra Diesel Injection Serv., Inc. v. Burroughs Corp., 874 F.2d 653 (9th Cir. 1989)* (disclaimer not conspicuous if on the back of the contract even though in capital letters, at least when the transferee is unsophisticated); *Myrtle Beach Pipeline Corp. v. Emerson Elec. Co., 843 F. Supp. 1027, 1038 (D. S.C. 1993)* (factors include: "(1) the color of print in which the purported disclaimer appears; (2) the style of print in which the disclaimer is written; (3) the size of the disclaiming language, particularly in relation to other print in the document; (4) the location of the disclaimer in the contract; (5) the appearance of the term 'merchantability' with respect to color, style, size, and type of print in the disclaimer clause; and (6) the status of the parties contesting the validity of the disclaimer, namely whether they be consumers or commercially sophisticated entities.").

For cases enforcing nonconspicuous disclaimers because of actual knowledge of the party asserting the warranty, see, e.g., *Twin Disc, Inc. v. Big Bud Tractor, Inc., 772 F.2d 1329, 1335 n.3 (7th Cir. 1985)* ("There is therefore no need to determine whether a disclaimer is conspicuous, such that the buyer's knowledge of disclaimer can be inferred, when the buyer has actual knowledge of the disclaimer."); *Fargo Mach. & Tool Co. v. Kearney & Trecker Corp., 428 F. Supp. 364, 372 (E.D. Mich. 1977)* ("sophisticated business buyer experienced in commercial dealings[]" who reviewed, understood, and apparently approved of a warranty paragraph containing a disclaimer clause cannot then argue its inconspicuousness even though the disclaimer sentence itself was in standard small print).

For cases construing the "unless the circumstances indicate otherwise" language of U.C.C. § 2-316(3)(a) to defeat otherwise effective disclaimers, see, e.g., *Murray v. D & J Motor Co., 958 P.2d 823, 829-830 (Okla. Civ. App. 1998)* ("Section 2-316(3) addresses the use of the terms 'as is' and 'with all faults'. . . . This Court holds that among the circumstances that could render a purported 'as is' or 'with all faults' disclaimer unreasonable and ineffective are fraudulent representations or misrepresentations concerning the condition, value, quality, characteristics or fitness of the goods sold that are relied upon by the Buyer to the Buyer's detriment."); *Alpert v. Thomas, 643 F. Supp. 1406, 1417 (D. Vt. 1986)* ("[C]lause 9(i) fails under § 2-316(3) to adequately disclaim plaintiffs' implied warranty that Raxx was merchantable as a breeder. First, subsection (3)(a) provides that implied warranties may be excluded by expressions like 'as is' or other expressions which would normally call the buyer's attention to the fact that the implied warranty is excluded, 'unless the circumstances indicate otherwise.' In this case, the circumstances indicate otherwise. The course of negotiations between Mallory and Thomas indicates that, despite the presence of clause 9(i) in the purchase and sale agreement, the parties intended that Raxx would be merchantable as a breeder, as is the custom in the Arabian horse trade when the seller knows that the buyer intends to use the horse for breeding purposes.").

For a discussion of the placement of disclaimers on web pages, see Stephen J. Davidson, Scott J. Bergs & Miki Kapsner, Open, Click, Download, Send . . . What Have you Agreed to? The Possibilities Seem Endless, 765 PLI/Pat 139 (2003) (conspicuousness on web pages depends in part on the number of clicks necessary to reach the disclaimer). For criticism of the use of the "conspicuousness" standard in software contracts, see Stephen E. Friedman, Text and Circumstances: Warranty Disclaimers in a World of Rolling Contracts, *46 Ariz. L. Rev. 677 (2004).*

Illustration 1 is based on *Betaco, Inc. v. Cessna Aircraft Co., 103 F.3d 1281 (7th Cir. 1996)* ("vague" and "casual" representations defeated by explicit and clear disclaimer).

Illustration 2 is based on *Hayes v. Bering Sea Reindeer Prods., 983 P.2d 1280 (Alaska 1999)* (negotiated disclaimer effective against sophisticated business with equal bargaining power) and *Appalachian Ins. Co. v. McDonnell Douglas Corp., 262 Cal. Rptr. 716 (Ct. App. 1989)* (party cannot claim "surprise" when it participated in drafting disclaimer).

Illustration 4 is based on *Sierra Diesel Injection Serv., Inc. v. Burroughs Corp., 890 F.2d 108 (9th Cir. 1989).*

§ 3.07 Third-Party Beneficiaries of Warranty

(a) A transferor's warranty extends to any person for whose benefit the transferor intends to supply the software if the person uses the software in a manner contemplated or that should have been contemplated by the transferor.

(b) A transferor's warranty to a consumer extends to the consumer's immediate family, household members, or guests if the transferor reasonably should expect such persons to use the software.

(c) Except as provided in (b), a contractual term that excludes or limits the third parties to which a warranty extends is enforceable.

(d) An exclusion or modification of a warranty that is effective against the transferee is also effective against third parties to which the warranty extends under this Section.

Comment:

a. Generally. Section 3.07(a) follows UCITA § 409 and the common-law development of third-party-beneficiary law. But § 3.07(b) expands the parties who can sue to include guests of the family or household if the transferor reasonably should expect such use. Nevertheless, § 3.07(d) enforces disclaimers against the third-party beneficiaries if they are effective against the transferee. Section 3.07 should be read in conjunction with the discussion of privity in § 3.03, Comment *c*.

Decisions involving sales of goods have not settled whether plaintiffs can sue as third-party beneficiaries if they claim only economic loss. Section 3.07 applies both to economic and personal injuries suffered by a third party. In the consumer context, personal injury from defective software should be less frequent.

b. Person for whose benefit the transferor intends to supply the software. This requirement roughly follows the Restatement Second of Contracts § 302. That Section provides that if (1) both contracting parties intend to recognize the beneficiary's right to performance and (2) the promisee "intends to give the beneficiary the benefit of the promised performance" then the beneficiary is an "intended beneficiary." Under the Restatement Second of Contracts § 304, only "intended beneficiaries" can sue. Section 3.07(a) of these Principles distills from the Restatement the requirement that the transferor must intend to benefit the third party. According to UCITA, "[t]his requires a conscious assumption of risk or responsibility for particular third parties." UCITA § 409, Comment 2. A transferor may clarify in the contract whether it intends for the warranty to extend to a third party or whether it specifically intends the opposite. See § 3.07(c).

Illustration:

1. For tax reasons, B, a medical practice, arranges for a hospital to acquire medical software and a computer system from A, a transferor. B supplies the funding for the software and system. The contract between A and the hospital expressly states that the turn-key system is for the benefit of B and that B will use the system exclusively. In case of a breach of warranty, B can sue A.

c. Third-party beneficiaries of consumer transferees. Under § 3.07(b) the transferor is liable to the transferee's immediate family, household, or guests only if the transferor reasonably should expect these parties to use the software. This approach follows UCITA § 409, Comment 4.

Illustration:

2. B, a consumer, downloads from A's website an "all-in-one" software package for creating audio, video, photo, and data projects. Among other things, the software allows picture editing, screen-saver designing, and movie

displaying. Members of B's household who lawfully use B's copy of the software can sue for breach of warranty as third-party beneficiaries.

d. Limitations. Under subsections (c) and (d), transferors can limit their exposure to third-party liability. Under subsection (c), a transferor can narrow the reach of subsection (a) by expressly delineating for whom the transferor intends to supply the software and for whom it does not. Subsection (d) makes clear that effective warranty disclaimers apply to third parties.

Illustration:

3. Same facts as Illustration 2, except that the contract between A and B includes an effective disclaimer of the warranty of merchantability. The disclaimer shields A from merchantability warranty liability to B's household members.

REPORTERS' NOTES

Comment a. Generally. On the importance of extending protection to guests of the household, see Jean Braucher, Uniform Computer Information Transactions Act (UCITA): Objections from the Consumer Perspective, 5 No. 6 Cyberspace Law. 2 (2000) ("[UCITA] [r]estricts responsibility to third party beneficiaries more narrowly than UCC Article 2: UCITA adopts an extremely narrow definition of third party beneficiaries of warranties. This definition excludes guests of the licensee even if they could have been reasonably expected to use the product . . . . Even the narrowest alternative in UCC 2-318 covers family, household members and guests if their use was reasonably expected. UCITA section 409 eliminates guests altogether.").

As with UCITA, § 3.07 applies to both personal and economic injury caused by the software. See Holly K. Towle, Mass Market Transactions in the Uniform Computer Information Transactions Act, *38 Duq. L. Rev. 371, 453 (2000)* ("Note that unlike UCC Alternatives A and B, there is no limitation in UCITA to personal injury damages."). Potential liability for personal injury may include "diet software, exercise control software, first aid software, recipe-creating software and the like . . . ." 2 Richard Raysman & Peter Brown, Computer Law: Drafting and Negotiating Forms, § 12.11A(4) (1984). For a comparison of approaches to interpreting "injury" under Alternative C of U.C.C. § 2-318, see, e.g., *Hyundai Motor Am., Inc. v. Goodin, 822 N.E.2d 947, 955-956 (Ind. 2005).*

Comment b. Person for whose benefit the transferor intends to supply the software. The Restatement Second of Contracts § 302 provides:

Intended and Incidental Beneficiaries

(1) Unless otherwise agreed between promisor and promisee, a beneficiary of a promise is an intended beneficiary if recognition of a right to performance in the beneficiary is appropriate to effectuate the intention of the parties and either

(a) the performance of the promise will satisfy an obligation of the promisee to pay money to the beneficiary; or

(b) the circumstances indicate that the promisee intends to give the beneficiary the benefit of the promised performance.

Section 3.07 overturns some cases in the software context that required privity. See, e.g., *Downriver Internists v. Harris Corp., 929 F.2d 1147 (6th Cir. 1991),* discussed in 2 L. J. Kutten, Computer Software Protection-Liability-Law-Forms, § 10.02(9). Kutten writes:

Before a "purchaser" can sue for breach of warranty, it may have to show that it has privity with the seller. This is not always easy since many times computer systems are leased through third parties. For example, in *Downriver Internists v. Harris Corporation, [929 F.2d 1147 (6th Cir. 1991)]* a medical practice used a hospital to purchase the system in order to obtain tax benefits. When the system did not work, and the medical practice sued, the Court ruled that it could not claim a third-party beneficiary status, since it was neither a party to the contact nor mentioned in it. The Court said:

In both cases, the negotiations prior to signing of the contracts did not involve Downriver. Although the contracts indicate that the equipment was to be shipped to Downriver, they clearly state that the equipment was sold to Lynn. Downriver's only apparent role in the contracts was as a provider of financing in order for Downriver to claim tax benefits. Downriver was not bound by the terms of the contracts, and was not a party to the performance obligations spelled out in the contracts. The district court properly found that privity of contract did not exist between Downriver and Harris or HRI [the sellers]. *[Id. at 1149-1150.]*

Conversely in *Spagnol Enters., Inc. v. Digital Equipment Corp., [568 A.2d 948 (Pa. Super. Ct. 1989)]* the Court held that a "lessor" of a computer system could sue the manufacturer even though there was no contractual relationship (privity) between them. There, the "lease" had been arranged through an authorized reseller and the seller attended meetings with both the lessor and lessee. The Court interpreted Pennsylvania's enactment of UCC § 2-318, to mean that privity is not required for any warranty claim where the buyer is the person who is reasonably and foreseeably injured by the defective goods.

Illustration 1 is based on *Downriver Internists v. Harris Corp., 929 F.2d 1147 (6th Cir. 1991).*

TOPIC 2

PAROL-EVIDENCE RULE AND INTERPRETATION

Summary Overview

Topic 2 deals with the admissibility of evidence to establish the meaning of a record (the parol-evidence rule) and the interpretation of words and conduct in light of the admissible evidence (interpretation). Section 3.08 contains the parol-evidence rule, § 3.09 sets forth general rules of interpretation, and § 3.10 governs whose meaning applies when the parties disagree as to the meaning of words.

The parol-evidence rule (subsections (e) and (f) of § 3.08) bars evidence that contradicts or varies an unambiguous record or particular unambiguous terms in the record that the parties intended to be a complete integration of their agreement or terms. Subsections (a) through (c) of § 3.08 provide guidance on how courts should determine whether a record or term is integrated. Section 3.08(d) deals with the process of determining whether a record is ambiguous. Section 3.08(g) sets forth exceptions to the parol-evidence rule.

In theory, the parol-evidence rule helps assure that courts enforce parties' actual agreements, principally by barring fraudulent assertions of agreement inconsistent with a record. In fact, in some contexts, the rule may subvert parties' intentions. For example, a transferor may expressly warrant the quality of software on its website, in brochures, or through a salesperson's representations, knowing that the consumer-transferee will not read the standard-form record, which disclaims all warranties. The parol-evidence rule should not bar admission of evidence supporting the express warranties (and the issue should be whether a reasonable transferee would expect the disclaimer (see § 3.06(a) of these Principles)). In fact, because of the potential harshness of the parol-evidence rule, courts often find exceptions to the rule when they believe that barring parol evidence would conflict with enforcing the parties' real agreement. These Principles establish a parol-evidence rule that seeks a middle ground between rigid enforcement and abrogation of the rule.

Several emerging issues in the context of the interpretation of software contracts highlight this area of the law. Technology continues to advance, rapidly changing the nature of software products. In fact, contract terms do not always keep up with the parties' understanding of precisely what software is being transferred because providers continue to improve the functionality and features of software, distribute many different versions, and provide plug-ins and updates. n39 Further, an agreement may fail to delineate clearly authorized uses of software because technology has created new uses during the contracting or performance periods. In addition, parties do not always clearly describe the meaning of terms involving, for example, functionality and quality because of software's complexity, tendency to contain bugs, and, in some instances, uniqueness. In fact, the case law is expanding rapidly on all of these fronts, making the clear formulation of rules of interpretation particularly relevant in the software realm. n40

In addition, courts must interpret terms against the backdrop of federal intellectual property law. For example, in copyright-infringement cases, courts should interpret the meaning of a software license in light of the scope and purposes of federal copyright law. n41

Sections 3.08 through 3.10 are based in part on the Restatement Second of Contracts and in part on Article 2 of the U.C.C., but the Sections have been written with the goal of achieving greater clarity and emphasizing the issues raised by software exchanges.

§ 3.08 Integration, Ambiguity, and Parol Evidence

(a) A full integration constitutes a record or records intended by the parties as a complete and exclusive statement of the terms of an agreement. A partial integration constitutes a record or records intended by the parties as the complete and exclusive statement of one or more terms of an agreement.

(b) The court should determine whether a record is fully integrated, partially integrated, or not integrated prior to applying subsections (e) and (f). In making this determination, the court should consider all credible and relevant extrinsic evidence, including evidence of agreements and negotiations prior to or contemporaneous with the adoption of the record.

(c) If the transfer is a standard-form transfer of generally available software, a term in a record indicating that the record is fully integrated or partially integrated should be probative but not conclusive on the issue.

(d) The court should determine whether a term in a record is ambiguous prior to applying subsections (e) and (f). In making this determination, the court should consider all credible and relevant extrinsic evidence, including evidence of agreements and negotiations prior to or contemporaneous with the adoption of the record. If a term or terms is ambiguous, extrinsic evidence is admissible to prove the meaning of the term or terms.

(e) Unambiguous terms set forth in a fully integrated record may not be contradicted by evidence of any prior agreement or of a contemporaneous oral agreement, but may be explained by evidence of a course of performance, course of dealing, or usage of trade.

(f) Unambiguous terms set forth in a partially integrated record may not be contradicted by evidence of prior or contemporaneous oral conflicting terms, but may be explained by evidence of course of performance, course of dealing, usage of trade, or consistent additional terms.

(g) Notwithstanding subsections (e) and (f),

(1) evidence is admissible to prove

(A) illegality, fraud, duress, mistake, or other invalidating causes; and

(B) independent agreements; and

(2) evidence of course of performance, course of dealing, and usage of trade is admissible to supplement a record.

Comment:

a. Generally. Section 3.08 seeks a middle ground between rigid enforcement of the parol- evidence rule and its abrogation. The approach is not novel, but is based on the common law, the Restatement Second of Contracts, and U.C.C. § 2-202. Each of these sources indicates factors that courts should consider or processes that courts should employ in determining whether to admit evidence. Based on these sources, these Principles bar evidence only if (1) the parties intended a full integration or (2) the parties intended a partial integration and the evidence is of conflicting terms. Evidence is nonetheless admissible if the record is ambiguous or the evidence consists of course of dealing, course of performance, or usage of trade. Evidence is also admissible if the evidence shows fraud or another invalidating cause or if the evidence is of an independent agreement. Further, courts should admit all probative evidence to determine integration or ambiguity before applying the parol-evidence rule. All of these points are amplified in Comments *b* through *e*.

b. Integration. Subsections (b) and (c) deal with the issue of whether a record is fully or partially integrated. The parol-evidence rule operates only when the parties intended their record to be a complete and exclusive statement of their entire agreement (full integration), or a complete and exclusive statement of particular terms included in the record (partial integration). A court may find that the parties intended neither, and hence the parol-evidence rule would not operate. Courts and commentators heretofore have disagreed on how to determine integration. The traditional approach requires the judge to decide simply by reading the contract. But a more reasoned view, which takes into account the challenges of accurately and completely reducing an agreement to a record and which Corbin and others adopted, is that judges should weigh the offered evidence preliminarily as part of the process of determining integration. Subsection (b) adopts this approach, which is also found in the Restatement Second of Contracts § 214(a). The issue is a matter of law for the judge.

Of course, credible evidence of agreements that contradicts a record tends to show that the parties did not intend to integrate their agreement. This is particularly relevant in the context of retail-like transfers of software if a transferor makes express warranties about the quality of software on its website, in brochures, or via a salesperson's representations, only to disclaim all warranties in the standard form. Assuming the evidence is credible, the court should consider the evidence in determining whether the standard form is integrated. If the court concludes that the evidence tends to show that the record is not integrated, the evidence should be submitted to the trier of fact.

Courts also disagree on the weight to be given to a "full integration clause." The better approach, at least in the context of standard-form transfers of generally available software (see §§ 1.01(l) and 2.02), is that such boilerplate, typically ignored, is probative but not definitive on the issue of integration, and these Principles adopt that position in subsection (c). The Principles leave for case-by-case analysis whether a "full integration clause" should control in other contexts.

Illustrations:

1. A, a software transferor, transfers to B, an automotive dealer, a computer system consisting of hardware and software. A orally promises that the system is particularly suitable for auto dealerships and only requires minimal maintenance. The record covers all pertinent terms, including a disclaimer of all warranties, and appears complete on its face, but it does not contain an integration clause. The software fails to satisfy the needs of B's dealership and requires frequent maintenance. At trial, B seeks to testify concerning A's oral promise. The court should consider B's testimony preliminarily on the question of whether the parties intended a full integration. If credible and relevant, the court should admit the evidence.

2. B is shopping for recreational software. She acquires *Number Cruncher*, manufactured by A, a software developer, who is marketing the software to the general public. Before the transfer, A tells B that *Number Cruncher* is a "fun and exciting numbers game for grownups and kids." Upon downloading the software, B agrees to A's clickwrap standard form that disclaims all warranties and contains a full integration clause. *Number Cruncher* turns out to be a spreadsheet program for accountants. Section 3.08(c) applies. In the context of a standard-form transfer of generally available software, the full-integration clause should not conclusively determine whether the agreement is fully integrated.

c. Ambiguity. An agreement or term is ambiguous if the language is reasonably susceptible to more than one meaning. Courts and commentators disagree on how courts should determine ambiguity. As with the issue of integration, the traditional view is that the judge should determine ambiguity simply by reading the contract. But in light of the inherent imprecision of language, the better view and the one adopted by these Principles in subsection (d) is that courts should consider probative extrinsic evidence preliminarily to determine whether a record is reasonably susceptible to more than one meaning. The question is one of law for the judge. Courts routinely admit evidence of course of dealing, course of performance, and usage of trade in this regard because they are reliable indicators of the meaning of the language. See § 3.09. If the language is ambiguous, the parol-evidence rule does not apply.

Illustrations:

3. A, a software developer, licenses B, another software developer, "to use AMP software that decodes mp3 files for 'WINAMP,'" a stand-alone, digital-content player that plays music on personal computers. The licensing agreement defines WINAMP as a "suite of programs" and contains a full integration clause. B uses AMP software in conjunction with a modified version of WINAMP called Media Player 6.0. A asserts that this use exceeds the scope of the licensing agreement. B offers evidence that its use does not exceed the scope of the agreement because Media Player incorporates WINAMP, thus AMP is still used in conjunction with WINAMP. Courts should consider this evidence preliminarily on the question of the meaning of the term "WINAMP." If WINAMP is reasonably susceptible to more than one meaning, the parol-evidence rule should not apply.

4. A, a software developer, transfers a software suite that generates invoicing, reporting, and sales documents, to B, a manufacturer of faucet and showering devices. The agreement contains a full-integration clause and promises that the software suite will function "correctly." As a preliminary matter, courts should consider evidence of whether the term "correctly" as used in the agreement is ambiguous. If so, evidence of communications and negotiations predating the parties' written agreement is admissible to determine its meaning.

d. The parol-evidence rule. Subsections (e) and (f) constitute the Principles' parol-evidence rule. In part, the rule follows U.C.C. § 2-202 and the Restatement Second of Contracts §§ 209, 213, and 214. Under the rule set forth here, a court first must determine whether the parties intended the record or the terms at issue to be complete and exclusive and whether the record or terms are ambiguous. Even if the rule applies, evidence of a course of performance, course of dealing, or trade usage is admissible to explain or supplement the record. For a discussion of these sources of evidence, see § 3.09, Comment *c*, and the Reporters' Notes to that Section. Evidence of consistent additional terms is also admissible if subsection (f) applies.

Illustrations:

5. A, a software developer, contracts with B, a trucking company, to develop B's in-house software for commercial sale. B transfers the software to A. The agreement calls for B to receive a 32 percent royalty on all software sales based on the wholesale price of the software. The agreement is unambiguous and contains a full-integration clause. The agreement breaks down and B offers evidence at trial that A promised to base royalty payments on the retail price of the

software. Section 3.08(e) applies and B's evidence is not admissible.

6. Same facts as Illustration 5, except that before breakdown of the agreement A distributes the software to customers and, over a three-month period, makes three royalty payments to B based on the retail price. B, who is aware that the payments are based on the retail price, accepts the payments without comment. Section 3.08(e) applies. Although the agreement is unambiguous and fully integrated, the course of performance explains the record and is admissible.

e. Other admissible evidence. Most courts admit evidence of fraud, illegality, duress, misrepresentation, mistake, and other evidence probative of the quality of assent because the evidence, if proven, establishes the absence of an enforceable agreement so that the parol-evidence rule should not operate at all. These Principles adopt a similar approach in subsection (g)(1)(A).

Under the independent-agreement exception of subsection (g)(1)(B), even if the parties intended the record to be a full or partial integration, the parol-evidence rule does not bar evidence of independent agreements that the parties would not have ordinarily included in the record at issue. For example, if software contracts rarely include a provision dealing with repairs to hardware, a court should admit evidence that a transferor of software agreed to repair a computer even if the parties' record says nothing about repairs and is fully integrated. On the other hand, transferor representations regarding the software's functionality ordinarily would be part of a record and would not be admissible as an independent agreement.

Distinguishing between independent agreements and agreements that parties would ordinarily include in their record is difficult. In the above example, a transferor could argue with some justification that if hardware repair was one of the inducements for the transferee to enter the agreement, then the court should expect that the transferee would have insisted that the parties include the term in the record. Its absence tends to show that the parties made no such agreement. On the other hand, if the transferee was a consumer with little bargaining power and little inclination to read the record, the likelihood is low that the transferee would insist that record include the repair term.

Subsection (g)(2) acknowledges that evidence of course of performance, course of dealing, and trade usage is admissible not only to explain terms, see subsections (e) and (f), but also to supplement a record. U.C.C. § 2-202 authorizes courts to admit such evidence to "explain or supplement" a writing without delineating the difference between explaining and supplementing. The terms are not interchangeable as used here. This evidence explains terms because it has "become an element of the meaning of the words used." U.C.C. § 2-202, Comment 2. The evidence supplements a record if the evidence proves the existence of terms that fill gaps in the agreement.

Illustration:

7. A, a software transferor, transfers invoice software to B, a single-proprietor, auto-body repair shop. The software is accompanied by a shrinkwrap license that is unambiguous and contains a full-integration clause. In a separate agreement made at the same time, A agrees to help B install and maintain word-processing software for B's home. The independent- agreement exception in § 3.08(g)(1)(B) applies. Evidence of the maintenance agreement is not barred by the parol-evidence rule because it is a separate, independent agreement that the parties would not normally have included in the shrinkwrap license.

REPORTERS' NOTES

Comment a. Generally. See Restatement Second, Contracts §§ 209, 213-214; U.C.C. § 2-202; Jeremy Adamson, The Parol Evidence Rule and the Principles (2007) (unpublished seminar paper, on file with the Reporters at Cornell Law School) (proposing a rule that combines the best of the Restatement Second of Contracts and U.C.C. § 2-202).

Comment b. Integration. The Restatement Second of Contracts § 209 provides in part:

(1) An integrated agreement is a writing or writings constituting a final expression of one or more terms of an agreement.

(2) Whether there is an integrated agreement is to be determined by the court as a question preliminary to determination of a question of interpretation or to application of the parol evidence rule.

The Restatement Second of Contracts § 214 provides in part:

Agreements and negotiations prior to or contemporaneous with the adoption of a writing are admissible in evidence to establish

(a) that the writing is or is not an integrated agreement;

(b) that the integrated agreement, if any, is completely or partially integrated;

(c) the meaning of the writing, whether or not integrated.

For software cases dealing with the issue of integration, see generally *Pure Bioscience v. Ross Sys., Inc., 2008 U.S. Dist. LEXIS 28454*, at *15-16 (S.D. Cal.) (parol evidence of defendant's salesmen's promises are barred because a merger clause makes the software licensing agreement the "final and exclusive statement of the agreement's terms"); *Piper Jaffray & Co. v. SunGard Sys. Int'l, Inc., 2005 U.S. Dist. LEXIS 7497*, at *17 (D. Minn.) ("The parol evidence rule . . . provides that written contractual terms may not be contradicted by evidence of any prior agreement or of a contemporaneous oral agreement. This section permits oral evidence of consistent additional terms to explain or supplement a contract, but only where the written terms were not intended as a complete and exclusive statement of the contract."); *SER Solutions, Inc. v. Masco Corp., 103 F. App'x 483, 487 (4th Cir. 2004)* ("The parol evidence rule provides that an integrated agreement 'may not be contradicted by evidence of any prior agreement or of a contemporaneous oral agreement[. . . .]'") (quoting Va. Code Ann., § 8.2-202 (2001 & Supp. 2008)); *Sagent Tech., Inc. v. Micros Sys., Inc., 276 F. Supp. 2d 464, 467 (D. Md. 2003)* ("[P]arol evidence is not admissible to contradict or supplement a writing intended by the parties to be a complete and exclusive expression of their agreement. However, parol evidence is admissible to prove consistent, additional terms if the writing is a final, but not complete, expression of the parties' agreement."); *Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., 85 F. Supp. 2d 519, 530 (W.D. Pa. 2000)* (integration clause prohibits contradictory parol evidence); *Accolade, Inc. v. Distinctive Software, Inc., 1990 U.S. Dist. LEXIS 14305*, at *8-9 (N.D. Cal.) ("Where a contract contains . . . an integration clause, the parol evidence rule operates to exclude consideration of any extrinsic evidence offered to vary or contradict the terms of the written agreement."); *Aplications, Inc. v. Hewlett-Packard, Co., 501 F. Supp. 129, 132-133 (S.D.N.Y. 1980)* ("When the parties agree to a written contract as a 'complete and final embodiment of the terms of the agreement,' the writing is an integration of the agreement, and parol evidence may not be used to vary its terms. Similarly, when only part of the agreement is integrated, parol evidence may not vary that part.") (quoting *Masterson v. Sine, 436 P.2d 561, 563 (Cal. 1968)).*

Courts have not been consistent on the process for determining integration. See generally *Jaskey Fin. & Leasing v. Display Data Corp., 564 F. Supp. 160, 163-165 (E.D. Pa. 1983)* (court strikes evidence of seller's oral representations of compatibility of software and hardware); *Dave Markley Ford, Inc. v. Lair, 565 P.2d 671, 673 (Okla. 1977)* (parol evidence not admissible if the contract itself shows that the parties intended it to be complete); *Redfern Meats, Inc. v. Hertz Corp., 215 S.E.2d 10, 18 (Ga. Ct. App. 1975)* (integration clause conclusive); *Huntsville Hosp. v. Mortara Instrument, 57 F.3d 1043, 1046 (11th Cir. 1995)* (salesperson's oral representations admitted as consistent additional terms that explain the record); *Sierra Diesel Injection Serv., Inc. v. Burroughs Corp., 890 F.2d 108, 112-113 (9th Cir. 1989)* (court held that parties' intentions are paramount and thus admitted extrinsic evidence despite an integration clause in the agreement); *O'Neil v. Int'l Harvester Co., 575 P.2d 862, 864-865 (Colo. App. 1978)* ("[B]uyer alleges the existence of oral warranties prior to execution of the written contract . . . . [T]here is a material issue of fact for resolution. That issue is whether the parties intended the written contract to be a final expression of their agreement, and

if not, what the terms actually agreed upon by the parties consisted of. Further, we hold that . . . evidence of . . . oral warranties . . . is admissible . . . .").

For a discussion of why the court should decide the issue of integration *without* the aid of extrinsic evidence, see 11 Samuel Williston, A Treatise on the Law of Contracts § 33:16 (Richard A. Lord, ed., 4th ed. 1999) ("'If we may go outside of the instrument to prove that there was a stipulation not contained in it, and so that only part of the contract was put in writing, and then, because of that fact, enforce the oral stipulation, there will be little of value left in the rule itself.'") (quoting *Eighmie v. Taylor, 98 N.Y. 288, 294 (1885)).* See also id. ("Even if the oral agreement were repugnant to the writing, what was orally agreed would be of equal importance with what was written, since its existence would prove that there was no complete integration of the contract in regard to the matter to which it related . . . . It is generally held that the contract must appear on its face to be incomplete in order to permit parol evidence of additional terms."); *Harrison v. Fred S. James, P.A., Inc., 558 F. Supp. 438, 442 (E.D. Pa. 1983)* ("[W]hen a writing contains an integration clause which expressly provides that the written instrument contains the entire agreement of the parties, it is conclusively presumed to do so . . . ."). But see 3 Arthur Linton Corbin, Corbin on Contracts 442 (rev. ed. 1960) ("[T]he 'parol evidence rule' does not itself purport to establish the fact of 'integration'; and until that fact is established the 'rule' does not purport to have any legal operation."); E. Allan Farnsworth, Contracts 424 n.37 (4th ed. 2004) (citing cases treating integration clauses as evidence, but not conclusive); *Marinelli v. Unisa Holdings, Inc., 655 N.Y.S.2d 495, 496 (App. Div. 1997)* ("[T]he standard for the introduction of an oral promise was satisfied here. The . . . agreements are collateral, they do not conflict with the [written] agreement and they would not reasonably be expected to be found there."); *Mitchill v. Lath, 160 N.E. 646 (N.Y. 1928).*

Comment c. Ambiguity. The ambiguity exception to the parol-evidence rule applies when the language of an agreement is reasonably susceptible to more than one meaning. For software cases applying the exception, see, e.g., *Tingley Sys., Inc. v. Healthlink, Inc., 509 F. Supp. 2d 1209 (M.D. Fla. 2007)* (meaning of "users" ambiguous); *Meridian Project Sys., Inc. v. Hardin Constr. Co., 426 F. Supp. 2d 1101, 1109 (E.D. Cal. 2006)* ("'[W]hen two equally plausible interpretations of the language of a contract may be made parol evidence is admissible to aid in interpreting the agreement.' Further, a party may present extrinsic evidence to show that a facially unambiguous contract is susceptible of another interpretation.") (quoting *Centigram Arg., S.A. v. Centigram, Inc., 60 F. Supp. 2d 1003, 1007 (N.D. Cal. 1999)); SER Solutions, Inc. v. Masco Corp., 103 F. App'x 483, 488 (4th Cir. 2004)* ("'The rule excluding parol evidence has no application where the writing on its face is ambiguous, vague, or indefinite. In such a case, the proper construction of the contract is an issue for the trier of fact, and the court should receive extrinsic evidence to ascertain the intention of the parties and to establish the real contract between them.'") (quoting *Cascades N. Venture, Ltd. v. PRC, Inc., 457 S.E.2d 370, 373 (Va. 1995)); Gilleland v. Schanhals, 55 F. App'x 257, 261 (6th Cir. 2003)* ("[T]he parol evidence rule does not preclude the consideration of a document that 'indicates the actual intent of the parties where an actual ambiguity exists.'") (quoting *Wonderland Shopping Ctr. Venture L.P. v. CDC Mortgage Capital, Inc., 274 F.3d 1085, 1095 (6th Cir. 2001); Playmedia Sys., Inc. v. Am. Online, Inc., 171 F. Supp. 2d 1094, 1100-1101 (C.D. Cal. 2001)* (finding that the term WINAMP is ambiguous, thus allowing extrinsic evidence); *NIKA Corp. v. City of Kansas City, Mo., 582 F. Supp. 343 (W.D. Mo. 1983).*

Courts disagree on how to determine ambiguity. See, e.g., *Tingley Sys., Inc. v. Healthlink, Inc., 509 F. Supp. 2d 1209, 1215 (M.D. Fla. 2007)* ("[P]arol evidence may only be considered if the terms are 'reasonably susceptible to more than one construction.'") (quoting *Strama v. Union Fid. Life Ins., 793 So. 2d 1129, 1132 (Fla. Dist. Ct. App. 2001)); AMC Tech., LLC v. SAP AG, 2005 WL 3008894* (E.D. Pa.) (court can look to circumstances only if the words are ambiguous on their face); *Vision Info. Servs., LLC v. Comm'r, 419 F.3d 554, 559 (6th Cir. 2005)* ("'[A] court, however, may not use extrinsic evidence to create an ambiguity; the ambiguity must be apparent on the face of the contract.'") (quoting *United States v. Donovan, 348 F.3d 509, 512 (6th Cir. 2003)); Computrol, Inc. v. Newtrend, L.P., 203 F.3d 1064, 1070 (8th Cir. 2000)* ("Illinois uses a 'four corners' rule in the interpretation of contracts, holding that 'if the language of a contract appears to admit only one interpretation, the case is indeed over.' Contracts 'must be construed to give effect to the intention of the parties which, when there is no ambiguity in the terms of the [contract], must be determined from the language of the [contract] alone.'") (quoting *Flora Bank & Trust v. Czyzewski, 583 N.E.2d 720,*

725 (Ill. App. Ct. 1991)).

But see *Meridian Project Sys., Inc. v. Hardin Constr. Co., 426 F. Supp. 2d 1101, 1109 (E.D. Cal. 2006)* ("[A] party may present extrinsic evidence to show that a facially unambiguous contract is susceptible of another interpretation."); *Altera Corp. v. Clear Logic, Inc., 424 F.3d 1079, 1090-1091 (9th Cir. 2005)* (court must decide preliminarily whether evidence is relevant to prove a meaning of which the instrument is reasonably susceptible); *Mid-America Real Estate Co. v. Iowa Realty Co., 406 F.3d 969, 972 (8th Cir. 2005)* ("'Any determination of meaning or ambiguity must be made in light of all of the circumstances, including the relations of the parties, subject matter of the transaction, preliminary negotiations, usages of trade, and the course of dealing.' Extrinsic evidence may not be used, however, to alter the terms of the agreement.") (quoting *Hofmeyer v. Iowa Dist. Ct., 640 N.W.2d 225, 228 (Iowa 2001)); Adobe Sys., Inc. v. One Stop Micro, Inc., 84 F. Supp. 2d 1086, 1090 (N.D. Cal. 2000)* ("'[E]xtrinsic evidence is admissible to demonstrate that there is an ambiguity in an instrument and for the purpose of construing this ambiguity.'") (quoting *LaCount v. Hensel Phelps Constr. Co., 145 Cal. Rptr. 244, 253 (Ct. App. 1978)).*

See generally *Pac. Gas & Elec. Co. v. G.W. Thomas Drayage & Rigging Co., 442 P.2d 641 (Cal. 1968)* (all credible evidence admitted to determine ambiguity). Justice Traynor, who wrote *Pacific Gas*, stated:

A rule that would limit the determination of the meaning of a written instrument to its four[#8209]corners merely because it seems to the court to be clear and unambiguous, would either deny the relevance of the intention of the parties or presuppose a degree of verbal precision and stability our language has not attained.

. . . .

. . . A court must ascertain and give effect to [the intention of the parties] by determining what the parties meant by the words they used. Accordingly, the exclusion of relevant, extrinsic evidence to explain the meaning of a written instrument could be justified only if it were feasible to determine the meaning the parties gave to the words from the instrument alone.

If words had absolute and constant referents, it might be possible to discover contractual intention in the words themselves and in the manner in which they were arranged. Words, however, do not have absolute and constant referents. 'A word is a symbol of thought but has no arbitrary and fixed meaning like a symbol of algebra or chemistry * * *.' The meaning of particular words or groups of words varies with the '* * * verbal context and surrounding circumstances and purposes in view of the linguistic education and experience of their users and their hearers or readers (not excluding judges).
* * * A word has no meaning apart from these factors; much less does it have an objective meaning, one true meaning.' Accordingly, the meaning of a writing '* * * can only be found by interpretation in the light of all the circumstances that reveal the sense in which the writer used the words. The exclusion of parol evidence regarding such circumstances merely because the words do not appear ambiguous to the reader can easily lead to the attribution to a written instrument of a meaning that was never intended.'

Although extrinsic evidence is not admissible to add to, detract from, or vary the terms of a written contract, these terms must first be determined before it can be decided whether or not extrinsic evidence is being offered for a prohibited purpose.

Id. at 644-645 (citations and footnotes omitted).

Not everyone agreed with Justice Traynor's reasoning: "*Pacific Gas* casts a long shadow of uncertainty over all transactions . . . . It also chips away at the foundation of our legal system. By giving credence to the idea that words are inadequate to express concepts, *Pacific Gas* undermines the basic principle that language provides a meaningful constraint on public and private conduct." *Trident Ctr. v. Conn. Gen. Life Ins., 847 F.2d 564, 569 (9th Cir. 1988).*

Comment d. The parol-evidence rule. See, e.g., *ETC Int'l, Inc. v. Curriculum Advantage, Inc., 2008 U.S. App.*

LEXIS 7113, at *7 (3d Cir.) (evidence of letters referring to an exclusive agreement would be inadmissible under the parol-evidence rule to contradict a term in a subsequent contract that refers to a "nonexclusive agreement"); *Tingley Sys., Inc. v. Healthlink, Inc., 509 F. Supp. 2d 1209 (M.D. Fla. 2007)* (evidence of course of dealing, usage of trade, and consistent additional terms admissible even if the contract is unambiguous).

Comment e. Other admissible evidence. On the admissibility of evidence of fraud and the like in software cases, see, e.g., *De Mexico S.A. v. Ariba, Inc., 2004 U.S. Dist. LEXIS 22473,* at *12 n.2 (N.D. Cal.) ("well-settled" that evidence of fraud in inducement is admissible notwithstanding a full-integration clause); *Sagent Tech., Inc. v. Micros Sys., Inc., 276 F. Supp. 2d 464, 467 (D. Md. 2003)* ("Parol evidence is also generally admissible to prove fraud."); *Inter-Americas Ins. Corp. v. Xycor Sys., Inc., 757 F. Supp. 1213, 1222 (D. Kan. 1991)* ("'A well-recognized exception to the parol evidence rule permits the use of evidence of fraudulent representations made during the course of negotiations where a contract is procured or induced by the fraudulent representations of one of the parties which were relied upon by the other.'") (quoting *Hawthorn-Mellody, Inc. v. Driessen, 518 P.2d 446, 448 (Kan. 1974)); Aplications, Inc. v. Hewlett-Packard, Co., 501 F. Supp. 129, 132-133 (S.D.N.Y. 1980)* ("In both California and New York, it is clear that a properly maintained action for fraud may overcome the policies behind the parol evidence rule, even with respect to contracts that disclaim reliance on representations not contained in the written instrument."). But see *Redprairie Corp. v. Jerome's Furniture Warehouse, 2007 U.S. Dist. LEXIS 87549,* at *3, *8 (E.D. Wis.) (an integration clause stating that "there are no representations . . . relied upon by customer that are not contained herein" disclaims plaintiff's "ability to rely upon any and all alleged fraudulent misrepresentations, whether in the inducement or thereafter"); *Tibco Software, Inc. v. Gordon Food Serv., Inc., 2003 U.S. Dist. LEXIS 12020,* at *16 (W.D. Mich.) ("[F]raud that relates solely to an oral agreement that was nullified by a valid merger clause would have no effect on the validity of the contract. Thus, when a contract contains a valid merger clause, the only fraud that could vitiate the contract is fraud that would invalidate the merger clause itself, i.e., fraud relating to the merger clause or fraud that invalidates the entire contract.") (quoting *UAW-GM Human Res. Ctr. v. KSL Recreation Corp., 579 N.W.2d 411, 419 (Mich. Ct. App. 1998); Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., 85 F. Supp. 2d 519 (W.D. Pa. 2000).*

See also *Hynansky v. Vietri, 2003 WL 21976031,* at *2 (Del. Ch.) ("'[P]arol evidence may be available to show []that the agreement was rendered invalid, void, or voidable by such causes as fraud, illegality, duress, mutual mistake, lack or failure of consideration, and incapacity.[]'") (quoting *Rodgers v. Erickson Air-Crane Co., 2000 WL 1211157,* at *4 (Del. Super. Ct.)); *Krossa v. All Alaskan Seafoods, Inc., 37 P.3d 411, 417 n.14 (Alaska 2001)* ("The parol evidence rule does not apply 'where a contract has been formed as a result of misrepresentation or mutual mistake.'") (quoting *Philbin v. Matanuska-Susitna Borough, 991 P.2d 1263, 1270 (Alaska 1999)); Culbreth v. Simone, 511 F. Supp. 906, 915 (E.D. Pa. 1981)* ("Exceptions to the parol evidence rule exist to explain essential written terms in instances of fraud . . . .").

Illustration 1 is loosely based on *Jaskey Fin. & Leasing v. Display Data Corp., 564 F. Supp. 160 (E.D. Pa. 1983).*

Illustration 3 is based on *Playmedia Sys., Inc. v. Am. Online, Inc., 171 F. Supp. 2d 1094 (C.D. Cal. 2001).*

Illustration 4 is loosely based on *SER Solutions, Inc. v. Masco Corp., 103 F. App'x 483 (4th Cir. 2004).*

Illustrations 5 and 6 are loosely based on *Regscan, Inc. v. Con-Way Transp. Servs., Inc., 875 A.2d 332 (Pa. Super. Ct. 2005).*

§ 3.09 General Principles of Interpretation

(a) Words or conduct should be interpreted in accordance with the meaning intended by both parties. Subject to § 3.10, if the parties disagree over that meaning, words or conduct should be interpreted reasonably in light of all of the circumstances.

(b) In determining a reasonable interpretation of the words or conduct,

significant factors include:

(1) each party's purpose or purposes in making the contract;

(2) any course of performance, course of dealing, or usage of trade; and

(3) the language of the entire agreement.

Comment:

a. Generally. This Section sets forth general principles of interpretation and applies after a court has decided questions of admissibility of evidence under the parol-evidence rule of § 3.08. Subsection (a) asks courts to enforce the meaning of words or conduct that both parties intended even if that meaning is inconsistent with an objective interpretation of the words or conduct. This subsection follows the Restatement Second of Contracts § 201(1), and is also consistent with freedom of contract because it enforces the parties' actual intentions. Of course, courts rarely entertain cases in which the parties' mutual, but unusual interpretation of language should prevail. In the usual case, the parties are each trying to prove that their different interpretation of the language is the reasonable one.

In the usual case, the second sentence of subsection (a) applies, which states that the meaning of the parties' words or conduct should be interpreted reasonably based on all of the circumstances. Subject to the exceptions set forth in § 3.10, the test is objective: What would a reasonable person with knowledge of the circumstances believe the words or conduct mean, not what either of the parties actually thought the language meant. So, for example, if a contract calls for software to perform "correctly" and the parties disagree over the meaning of this performance standard, the court should consider all of the circumstances in interpreting the language. Evidence of circumstances includes writings, records, oral communications, conduct, and negotiations. Especially important, and highlighted in subsection (b), is evidence of the parties' purpose or purposes in making the contract; any applicable course of dealing, course of performance, or trade usage; and the language of the agreement taken as a whole.

Illustrations:

1. A, a software developer, transfers invoicing software to B, a manufacturer of faucet and showering devices, which generates invoices and other sales documents. The contract includes a term barring claims one year after an action has "occurred." The parties agree that this is a typographical error and that "occurred" means "accrued." The first sentence of § 3.09(a) applies. A court should interpret the words of the written record in accordance with the meaning intended by both parties. Same result if both parties shared an unusual understanding of the meaning of "occurred."

2. A, a software developer, transfers to B, a video-editing systems manufacturer, software to run B's video-editing hardware. The record authorizes B to modify the software and integrate it with its "hardware." At the time of the agreement, B's commercially marketed hardware consisted exclusively of Macintosh computers. After the software transfer, B modifies the software to run on Windows-based hardware and begins marketing Windows-based hardware with the modified software. A objects, claiming that the written agreement meant B's Macintosh hardware only. The

second sentence of § 3.09(a) applies. A court should consider all of the circumstances to discern the meaning of "hardware" in the agreement.

b. Purposive interpretation. Evidence of the parties' purpose or purposes in making a contract is highly probative of a reasonable interpretation of words or conduct. See subsection (b)(1). Software agreements are no exception. For example, if the parties use the words "purchase," "own," and "licensing agreement" interchangeably, a court may face the issue of whether the parties intended to sell or license the software. An agreement for a developer to develop one copy of high-priced, custom software for a single payment may suggest that the parties intended a sale of the software. To cite another example, evidence of the parties' purpose or purposes may clarify the agreed performance standards of software if an agreement is obscure on the issue.

Illustrations:

3. A, a large software developer, transfers photo-editing software to B, a software distributor. B claims that it has full ownership of the software and therefore is not bound by the licensing agreement because the agreement contains language of a sales agreement, including "purchase" and "ownership." However, the agreement also contains language and restrictions indicating a license, including denying the right to copy the software. The president of A testifies that it was A's purpose in drafting the agreement to create a license and not to transfer ownership in the software in order to protect the innovative software code in the product. Expert testimony and trade-usage evidence also suggest that software transferors typically use sales terminology in a software license. Section 3.09(b) applies. The trier of fact should afford considerable weight to A's testimony of its purpose in making the agreement.

4. A, a software developer, licenses software to B, an insurance company. Although the contract is silent on the issue, B asserts that the purpose of the contract was for B to acquire software capable of handling all of its accounting and billing functions, but the software only handles accounting activities. B offers evidence of the efficiency of software that performs both functions and of the high price of B's software relative to software that can perform only one or the other function. If B's evidence is accurate, the evidence creates an inference that A agreed to develop software that could handle both functions.

c. Course of performance, course of dealing, and usage of trade. The Principles do not define these sources of evidence but, instead, rely on the definitions in U.C.C. Article 1 and their interpretations in the case law. In brief, usage of trade constitutes evidence of what similarly situated people intend when they use particular language. Course of dealing and course of performance constitute evidence of the parties' prior conduct to show the meaning of their present language. These sources of evidence constitute objective evidence of the meaning of words and conduct because they do not rely on the parties' testimony concerning their intentions. These sources better ascertain the parties' intentions than the dictionary meaning of their language alone because people likely attach the meaning used in their environment or act according to their understanding of the terms of their agreements.

The parties can avoid courts' use of course-of-performance, course-of-dealing, and trade- usage evidence. For example, the parties can agree to exclude evidence of trade usage or course of dealing. A party can avoid the implication of a course of performance by objecting to the performance and reserving legal rights.

The U.C.C. and the Restatement Second of Contracts establish a hierarchy for resolving evidentiary matters when course of performance, course of dealing, and usage of trade conflict: Course of performance trumps course of dealing and trade usage, and course of dealing prevails over trade usage. This hierarchy is based on the likelihood of each type of evidence proving the parties' actual intentions.

Illustrations:

5. A, a software developer, contracts with B, a trucking company, to develop for commercial sale B's in-house software. B transfers the software to A. The agreement calls for B to receive a 32 percent royalty on all software sales based on the wholesale price of the software. The agreement is unambiguous and contains a full-integration clause. Later, B tells A that the royalty should be based on the retail price of the software. A distributes the software to customers and, over a three-month period, makes three royalty payments to B based on the retail price. B accepts the royalty payments without comment. Section 3.09(b) applies. The evidence of course of performance reveals the parties' intentions.

6. A, a software transferor, transfers to B, a small plumbing company, bookkeeping and accounting software to satisfy B's record-keeping needs. The record includes a software service plan in which A agrees to transfer any subsequent versions of the software to B for a two-year period. After one year, a virus infects the program and deletes all of B's records. B claims A was obligated to transfer a software update that A developed that would have protected B from the virus. A claims that antiviral software does not constitute a new version of the software transferred to B. The trade custom is that antiviral-software updates do constitute "new" versions of the software for purposes of service plans such as the one between A and B. Section 3.09(b)(2) applies. The court should afford this trade-usage evidence substantial weight in determining whether the service agreement obligated A to transfer its antiviral software.

d. The language of the entire agreement. Subsection (b)(3) is not controversial. Courts should peruse the entire agreement, which often sheds light on the language in dispute. For example, if one term in a license limits the number of users, but another term refers to "unlimited" use, a court should determine whether other parts of the license help resolve the conflict.

e. Other rules of interpretation. Courts often set forth rules for interpreting contracts that in many cases may be no more than after-the-fact rationalizations of interpretation decisions reached on other grounds. These rules include the following: parties are presumed to incorporate the common meaning of language; specific language is preferred over general language; and an interpretation that upholds a contract should trump one that defeats it. Because of the nature of these rules, § 3.09 takes no position on their use.

REPORTERS' NOTES

Comment a. Generally. See Restatement Second, Contracts § 201(1) ("Where the parties have attached the same meaning to a promise or agreement or a term thereof, it is interpreted in accordance with that meaning."); *Berke Moore Co. v. Phoenix Bridge Co., 98 A.2d 150, 156 (N.H. 1953)* ("[W]hen it appears that the understanding of one is the understanding of both, no violation of the rule results from determination of the mutual understanding according to that of one alone."). For a software case, see *SER Solutions, Inc. v. Masco Corp., 103 F. App'x 483, 486 n.1 (4th Cir. 2004)* ("The contract actually provides 'more than one year after such action *occurred*.' The parties agree, however, that 'occurred' is a typographical error and that the word should be 'accrued.'").

For a software case interpreting what the term "correctly" means, see *id. at 488* ("What 'correctly' means . . . is indefinite and ambiguous . . . .").

For software cases looking to enforce the parties' intentions, see *Rent Info. Tech., Inc. v. Home Depot U.S.A., Inc., 2008 U.S. App. LEXIS 4675,* at *2-3 (9th Cir.) ("'If we find a contract to be ambiguous, we ordinarily are hesitant to grant summary judgment because differing views of the intent of parties will raise genuine issues of material fact.'") (quoting *San Diego Gas & Elec. Co. v. Canadian Hunter Mktg. Ltd., 132 F.3d 1303, 1307 (9th Cir. 1997)); Netbula, LLC v. Bindview Dev. Corp., 516 F. Supp. 2d 1137, 1148 (N.D. Cal. 2007)* (although federal copyright law governs the assignability of licenses, "the question of whether a license has in fact been assigned depends on contract interpretation and, accordingly, is a matter controlled by state law"); *Bus. Sys. Eng'g, Inc. v. IBM, 520 F. Supp. 2d 1012, 1019 (N.D. Ill. 2007)* ("'In order to overcome [the presumption that parties only intend the terms of the contract to apply to them],

the implication that the contract applies to third parties must be so strong as to be practically an express declaration.'") (quoting *Ball Corp. v. Bohlin Bldg. Corp., 543 N.E.2d 106, 107 (Ill. App. Ct. 1989)); Con-Way Transp. Servs., Inc. v. Regscan, Inc., 242 F. App'x 823 (3d Cir. 2007)* (holding that, under a licensing agreement to develop a software "Product" marketable in the trucking industry, a jury could reasonably interpret the contract to find that one software program developed falls under the licensing agreement while one other did not); *Altera Corp. v. Clear Logic, Inc., 424 F.3d 1079, 1091 (9th Cir. 2005)* ("The intent of the parties is the governing notion of contract law. Altera's intent is clear from the language of its license agreement: Altera sought to prevent competitors from benefitting from its software."); *Mid-America Real Estate Co. v. Iowa Realty Co., 406 F.3d 969, 972 (8th Cir. 2005)* ("The parties' intentions at the time that they executed the contract are the touchstone for determining its meaning."); *Vision Info. Servs., LLC v. Comm'r, 419 F.3d 554, 558 (6th Cir. 2005)* ("'[T]he cardinal rule in the interpretation of contracts is to ascertain the mutual intention of the parties and then, so far as it is possible so to do consistently with legal principles, give effect to that intention.'") (quoting *Pickren v. United States, 378 F.2d 595, 599 (5th Cir. 1967)); Gilleland v. Schanhals, 55 F. App'x 257, 260 (6th Cir. 2003)* ("'[T]he essence of the inquiry here is to effectuate the intent of the parties.'") (quoting Melville B. Nimmer, *Nimmer on Copyright § 10.03*(A)(2) (MB 2000)); *Aplications Inc. v. Hewlett-Packard Co., 501 F. Supp. 129, 132 (S.D.N.Y. 1980)* ("Under California law, as elsewhere, the contract must be interpreted to give effect to the intentions of the parties."); see also *Cardonet, Inc. v. IBM Corp., 2007 WL 3256204* (N.D. Calif.) (dispute over the meaning of the unit measure of software usage).

For software cases stressing the importance of considering the entire record in determining its meaning, see, e.g., *Teragram Corp. v. Marketwatch.com, Inc., 444 F.3d 1, 10 (1st Cir. 2006)* (finding that courts must evaluate the entire agreement); *Postlewaite v. McGraw-Hill, Inc., 411 F.3d 63, 69 (2d Cir. 2005)* ("Contracts should be viewed in the light in which they were made."); *Computrol, Inc. v. Newtrend, L.P, 203 F.3d 1064, 1070 (8th Cir. 2000)* (ruling that courts must consider a contract as a whole to determine the intentions of the parties).

On the use of the "reasonable person" test, see generally, *Zell v. Am. Seating Co., 138 F.2d 641, 647* (2d Cir. l943) (Frank, J.), rev'd, *322 U.S. 709* (l944) (per curiam) ("We ask judges or juries to discover that 'objective viewpoint'-through their own subjective processes."); *Hotchkiss v. Nat'l City Bank of New York, 200 F. 287, 293* (S.D.N.Y. l911), aff'd sub nom. *Ernst v. Mechanics & Metals Nat'l Bank, 201 F. 664 (2d Cir. 1912),* aff'd, *231 U.S. 50 (1913);* see also Robert A. Hillman, Contract Lore, *27 J. Corp. L. 505, 510-512 (2002).* As Judge Learned Hand famously stated:

A contract has, strictly speaking, nothing to do with the personal, or individual, intent of the parties . . . . If . . . it were proved by twenty bishops that either party, when he used the words, intended something else than the usual meaning which the law imposes on them, he would still be held, unless there were some mutual mistake, or something else of the sort.

Hotchkiss, 200 F. at 293.

The relevant circumstances to explore in interpreting language or conduct include "all writings, oral statements, and other conduct by which the parties manifested their assent, together with any prior negotiations between them and any applicable course of dealing, course of performance, or usage." E. Allan Farnsworth, Contracts 453 (4th ed. 2004).

Comment b. Purposive interpretation. On the importance of purposive interpretation, see Farnsworth, at 454-455; Restatement Second, Contracts § 202(1); see also *Rockland Trust Co. v. Computer Assocs. Int'l, Inc., 2007 WL 2746804* (D. Mass.); *Sutter Ins. Co. v. Applied Sys., 393 F.3d 722 (7th Cir. 2004); Adobe Sys., Inc. v. One Stop Micro, Inc., 84 F. Supp. 2d 1086 (N.D. Cal. 2000).*

Comment c. Course of performance, course of dealing, and usage of trade. According to the U.C.C., "[a] 'usage of trade' is any practice or method of dealing having such regularity of observance in a place, vocation, or trade as to justify an expectation that it will be observed with respect to the transaction in question." U.C.C. § 1-303(c); see also Restatement Second, Contracts § 222. Thus, a party can be bound to a usage of trade even if not a member of the trade,

if the party should reasonably expect the trade meaning to apply because it is regularly observed in the *place* the party is doing business. *Nanakuli Paving & Rock Co. v. Shell Oil Co., 664 F.2d 772, 791 (9th Cir. 1981)* ("[A] usage need not necessarily be one practiced by members of the party's own trade or vocation to be binding *if* it is so commonly practiced in a locality that a party should be aware of it.") (emphasis added). Further, a usage of trade does not have to be "ancient or immemorial," or practiced without exception in the trade, but only "regularly observed" over a reasonable period of time by "the great majority of decent dealers." Id. at 52-53 (quoting U.C.C. § 1-303, cmt. 4).

Under the U.C.C., a course of dealing is a "sequence of previous conduct between the parties to a particular transaction which is fairly to be regarded as establishing a common basis of understanding for interpreting their expressions and other conduct." U.C.C. § 1-205(1); see also Restatement Second, Contracts § 223.

A course of performance involves "repeated occasions for performance by a party" where the other party has "knowledge of the nature of the performance and opportunity for objection to it . . . ." U.C.C. § 1-303(a). If the other party does not object to the performance, it is "relevant to determine the meaning of the agreement." U.C.C. § 2-208(1); see also Restatement Second, Contracts § 202(4). For a case dealing with objection to a course of performance, see *Schulze & Burch Biscuit Co. v. Tree Top, Inc., 831 F.2d 709, 715 (7th Cir. 1987)* ("To prevent the clause from becoming part of the contract, [plaintiff] needed only to give notice of objection within a reasonable time.").

For software cases involving course-of-dealing, course-of-performance, or usage-of-trade evidence, see, e.g., *RealPage, Inc. v. EPS, Inc., 560 F. Supp. 2d 539 (E.D. Tex. 2007)* (course of dealing); *Regscan, Inc. v. Con-Way Transp. Servs., Inc., 875 A.2d 332 (Pa. Super. Ct. 2005); Abram & Tracy, Inc. v. Smith, 623 N.E.2d 704 (Ohio Ct. App. 1993).*

As to the hierarchy of sources of evidence, see Restatement Second, Contracts § 203(b) ("[E]xpress terms are given greater weight than course of performance, course of dealing, and usage of trade, course of performance is given greater weight than course of dealing or usage of trade, and course of dealing is given greater weight than usage of trade."); see also U.C.C. §§ 2-208(2), 1-303(e).

Comment d. The language of the entire agreement. See, e.g., *Health Care Logistics, Inc. v. Adonix Transcomm, Inc., 2007 U.S. Dist. LEXIS 48294,* at *10 (S.D. Ohio) ("In view of the extent of detail as to the [arbitration] procedure, the Court cannot conclude that the parties intended, by the use of the word "should" . . . , to make [arbitration] permissive."); *Tingley Sys., Inc. v. Healthlink, Inc., 509 F. Supp. 2d 1209, 1216 (M.D. Fla. 2007)* ("contract is interpreted as a whole" where license refers to "unlimited" use and "32 user license").

Comment e. Other rules of interpretation. For software cases see, e.g., *Teragram Corp. v. Marketwatch.com, Inc., 444 F.3d 1, 10 (1st Cir. 2006)* ("'The presumption in commercial contracts is that the parties were trying to accomplish something rational.'") (quoting *Fishman v. LaSalle Nat'l Bank, 247 F.3d 300, 302 (1st Cir. 2001)); Sutter Ins. Co. v. Applied Sys., 393 F.3d 722 (7th Cir. 2004)* (interpret language to create an equitable exchange); *PlayMedia Sys., Inc. v. Am. Online, Inc., 171 F. Supp. 2d 1094, 1099 (C.D. Cal. 2001)* ("A copyright license must be interpreted narrowly. Copyright licenses are presumed to prohibit any use not authorized."); *S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1088 (9th Cir. 1989)* ("The district court applied the California rule that the contract should be interpreted against the drafter . . . ."). But see *Beckman Instruments, Inc. v. Sys. Mgmt. Specialists, Inc., 2000 U.S. App. LEXIS 18166,* at *5 (9th Cir.) ("We have rejected the argument that license agreements permit that which they do not prohibit.").

See generally *Southgate Recreation & Park Dist. v. Cal. Ass'n for Park & Recreation Ins., 130 Cal. Rptr. 2d 728, 730 (Ct. App. 2003)* ("The basic rule of contract interpretation is to effectuate the parties' intent as expressed in the contract's terms, which are given their common meaning."); *State ex rel. Dept. of Transp. v. Delta Inn, Inc., 3 P.3d 180, 186 (Or. Ct. App. 2000)* ("In resolving . . . ambiguity, we resort, necessarily, to the 'construe against the drafter' principle."); see also Restatement Second, Contracts § 202(3)(a); *Robert W. Carlstrom Co. v. German Evangelical Lutheran St. Paul's Congregation of Unaltered Augsburg Confession at Jordan, 662 N.W.2d 168, 173 (Minn. Ct. App.*

2003) ("Phrases found in the contract should not be interpreted out of context, but rather given meaning in accordance with the obvious purpose of the contract as a whole."); *Genunzio v. Genunzio, 598 So. 2d 129, 132 (Fla. Dist. Ct. App. 1992)* ("[G]eneral language of a contract must yield to specific language which deals with the matter at issue . . . ."); *Beck Park Apartments v. U.S. Dept. of Hous. & Urban Dev., 695 F.2d 366, 370 (9th Cir. 1982)* ("Where, as here, a public interest is involved, 'an interpretation is preferred which favors the public.'") (quoting Restatement of Contracts § 236(f)); *Torncello v. United States, 681 F.2d 756, 761 (Ct. Cl. 1982)* ("[A]ny choice of alternative interpretations, with one interpretation saving the contract and the other voiding it, should be resolved in favor of the interpretation that saves the contract.").

Illustration 1 is based on *SER Solutions, Inc. v. Masco Corp., 103 F. App'x 483 (4th Cir. 2004).*

Illustration 2 is loosely based on *McRoberts Software, Inc. v. Media 100, Inc., 329 F.3d 557 (7th Cir. 2003).*

Illustration 3 is loosely based on *Adobe Sys., Inc. v. One Stop Micro, Inc., 84 F. Supp. 2d 1086 (N.D. Cal. 2000).*

Illustration 4 is loosely based on *Sutter Ins. Co. v. Applied Sys., 393 F.3d 722 (7th Cir. 2004).*

Illustration 5 is loosely based on *Regscan, Inc. v. Con-Way Transp. Servs., Inc., 875 A.2d 332 (Pa. Super. Ct. 2005).*

Illustration 6 is loosely based on *Abram & Tracy, Inc. v. Smith, 623 N.E.2d 704 (Ohio Ct. App. 1993).*

§ 3.10 Whose Meaning Prevails

(a) If the parties disagree over the meaning of words or conduct, the meaning intended by one of them should be enforced if at the time the parties made the agreement that party did not know or have reason to know any different meaning intended by the other party, and the other party knew or had reason to know the meaning intended by the first party.

(b) The parties have not made an enforceable agreement if

(1) the parties disagree over the meaning of a fundamental term or terms;

(2) the term or terms are ambiguous; and

(3) neither party knew or should have known of the other's meaning.

(c) In all other cases of disagreement as to the meaning of a term or terms, § 3.09 applies.

Comment:

a. Generally. Section 3.10 constitutes two exceptions to § 3.09(a)'s objective interpretation if the parties disagree over the meaning of language. Section 3.10(a) applies if the parties have assigned different meanings to language or conduct and one party knew or had reason to know of the other's intended meaning while that other party did not know or have reason to know the meaning intended by the first party. Section 3.10(b) applies if the parties disagree over the meaning of a fundamental term or terms, the words or conduct is reasonably susceptible to more than one meaning even after the trier of fact considers all relevant extrinsic evidence, and neither party knew or should have known of the other's meaning. Section 3.10 is based on the Restatement Second of Contracts § 201.

Illustrations:

1. A, a software developer, licenses B, an Internet service provider, "to use AMP, software to decode mp3 files, in conjunction with 'WINAMP,'" a stand-alone, digital-content player owned by B that plays music on personal computers. The licensing agreement defines WINAMP as a "suite of programs." At the time of contracting, B tells A that B intends to integrate AMP into a modified version of WINAMP, called Media Player 6.0. A does not respond. B uses AMP in conjunction with Media Player 6.0. A argues this use exceeds the scope of the licensing agreement. B asserts that its use does not exceed the scope of the agreement because Media Player incorporates WINAMP; thus, AMP is still used in conjunction with WINAMP. Although WINAMP is reasonably susceptible to more than one meaning, A knew the meaning attached by B, and B did not know or have reason to know the meaning attached by A. Therefore, § 3.10(a) applies and the meaning attached by B governs.

2. B, a video-editing systems manufacturer, contracts with A, a software developer, to acquire software to run B's video-editing hardware. A term in the record authorizes B to modify the software and integrate it with its hardware. Prior to the agreement, A had developed software solely for Macintosh hardware. However, also prior to the agreement, B sent two letters to A revealing that B owned both Macintosh and Windows-based hardware. B modifies the software to run on its Windows-based hardware and markets Windows-based hardware with the modified software. Although "hardware" is reasonably susceptible to more than one meaning, A had reason to know the meaning attached by B, and B did not know or have reason to know the meaning attached by A. Section 3.10(a) applies and the meaning attached by B applies.

b. Misunderstanding. Subsection (b) sets forth the common-law and Restatement Second of Contracts's misunderstanding doctrine. See Restatement Second, Contracts § 201(3). The doctrine holds that if the parties' understanding of a term or terms differs at the time of contracting, neither party knew or had reason to know the other's interpretation, and the misunderstanding is over a fundamental term, then the parties have not made an enforceable contract. A misunderstanding over a fundamental term is one in which neither party would receive substantially what it bargained for if the other party's understanding applied. As such, courts can receive some guidance from courts' treatment of the concept of materiality under the doctrine of material breach. See § 3.11 of these Principles. If the parties misunderstanding is over a term that is not fundamental, the court can strike the term and enforce the rest of the contract.

The problem of misunderstanding may be particularly relevant to software contracts because software developers continuously improve the functionality and features of software, distribute multiple versions, and provide plug-ins and updates. In such an environment, the parties reasonably may have different interpretations of the nature of the software the developer is transferring. In cases in which the parties have partially performed an unenforceable agreement, principles of the law of restitution would govern the remedies available to the parties.

Illustrations:

3. Same facts as Illustration 2, except that B did not write letters to A explaining the nature of B's hardware and neither party knew or had reason to know the hardware contemplated by the other. The meaning of hardware is likely fundamental so that

§ 3.10(b) applies. If so, the parties have not made an enforceable agreement. Principles of the common law of restitution govern the remedies available to the parties.

4. A, a software developer, licenses software to B, a finance company. The license calls for A to "customize/modify" the software for B. A installs the software on B's computers. B thought that A would modify the software to calculate interest using Federal Regulation Z rate tables, but this would be costly, and A thought the parties agreed that A would make basic modifications only. The agreement is ambiguous as to the scope of customizations/modifications, and if neither party knew or had reason to know of the meaning attached by the other and

the misunderstanding is fundamental, § 3.10(b) applies. The parties have not made an enforceable agreement.

REPORTERS' NOTES

Comment a. Generally. See *Joyner v. Adams, 361 S.E.2d 902, 905 (N.C. Ct. App. 1987)* ("[W]here one party knows or has reason to know what the other party means by certain language and the other party does not know or have reason to know of the meaning attached to the disputed language by the first party, the court will enforce the contract in accordance with the innocent party's meaning.").

Comment b. Misunderstanding. Subsection (b) is based in part on the Restatement Second of Contracts § 201(3), which follows the famous English case of *Raffles v. Wichelhaus, (1864) 159 Eng. Rep. 375* (KB). In *Raffles*, the contract required the seller to sell cotton scheduled to arrive on a ship called the "Peerless." The buyers refused to accept the cotton, even though it arrived on a ship called the Peerless, because the ship sailed from Bombay in December and the buyers intended to buy cotton arriving on a different ship also called the Peerless that sailed from Bombay in October. The seller demurred, so that the issue before the court was the sufficiency of the buyers' defense. The court upheld the defense, finding that the existence of two ships named Peerless created latent ambiguity. See also *First United Leasing Corp. v. Campagnie Nationale Air Fr., 1995 WL 560918*, at *5 (N.D. Ill.) ("When parties attach different meanings to a contract term, a situation best understood as a 'misunderstanding' or a 'mistake,' there is . . . technically no meeting of the minds and, consequently, no contract.").

For software cases involving alleged or real misunderstandings, see *McRoberts Software, Inc. v. Media 100, Inc., 329 F.3d 557 (7th Cir. 2003)* (ambiguity with respect to whether type of hardware meant existing hardware only); *Evolution, Inc. v. Ins. Fin. Corp., 2003 WL 22227461* (Kan. Ct. App.) (term regarding customizing software ambiguous, therefore "no meeting of the minds"); *PlayMedia Sys., Inc. v. Am. Online, Inc., 171 F. Supp. 2d 1094, 1100 (C.D. Cal. 2001)* ("[T]here are many different versions of WINAMP in existence, and . . . the Licensing Agreement does not restrict the licensee to using any particular version . . . .").

Illustration 1 is based on *Playmedia Sys., Inc. v. Am. Online, Inc., 171 F. Supp. 2d 1094 (C.D. Cal. 2001).*

Illustrations 2 and 3 are loosely based on *McRoberts Software, Inc. v. Media 100, Inc., 329 F.3d 557 (7th Cir. 2003).*

Illustration 4 is based on *Evolution, Inc. v. Insurance Fin. Corp., 2003 WL 22227641* (Kan. Ct. App.).

TOPIC 3

BREACH

Summary Overview

Topic 3 addresses issues primarily relevant to determining when a party is entitled to a remedy under Chapter 4 of the Principles. The Principles here, as elsewhere, do not replicate otherwise applicable law. For example, the Principles do not contain provisions restating such accepted doctrines as waiver, anticipatory repudiation, adequate assurance of performance, or other performance-related topics such as inspection. They focus instead on what constitutes breach so as to entitle an aggrieved party to a remedy. In particular, the emphasis here is on providing guidance as to what constitutes a material breach. Under the remedial scheme set forth in Chapter 4, only a material breach permits the aggrieved party to employ the remedy of cancellation, which ends rights of access to and/or use of the software.

Likewise critical to the remedial scheme of Chapter 4 is the notion of cure, particularly in the context of material breach.

§ 3.11 Breach and Material Breach

(a) A breach occurs if a party without legal excuse fails to perform an obligation as required by the agreement.

(b) An uncured breach, whether or not material, entitles the aggrieved party to remedies.

(c) In determining whether a breach is material, significant factors include:

(1) the terms of the agreement;

(2) usage of trade, course of dealing, and course of performance;

(3) the extent to which the aggrieved party will be deprived of the benefit reasonably expected;

(4) the extent to which the aggrieved party can be adequately compensated for the part of the benefit deprived;

(5) the degree of harm or likely harm to the aggrieved party; and

(6) the extent to which the behavior of the party failing to perform or to offer to perform departs from standards of good faith and fair dealing.

(d) Notwithstanding subsection (c) or any provision to the contrary in the agreement, a material breach occurs if:

(1) the transferor breaches the warranty of § 3.05(b);

(2) an exclusive or limited remedy fails of its essential purpose under

§ 4.01; or

(3) the transferor breaches the agreement by failing to comply with

§ 4.03.

(e) The cumulative effect of nonmaterial breaches may be material. Comment:

a. Scope. This Section is based on both the Restatement Second of Contracts § 241 and UCITA § 701. The concept of breach is a familiar one and less difficult to define than a "material breach." A breach occurs when a party fails to perform under the requirements of the agreement (including any terms of the agreement that a court may imply or incorporate from adoption of these Principles or outside law). Failing to perform in a timely manner, repudiating the agreement, and exceeding terms of use are examples of common breaches.

b. Remedies generally. Subsection (b) follows the commonly accepted reasoning that an uncured breach (§ 3.12) entitles a party to remedies. This Section generally also adopts the distinction between material and nonmaterial breaches. Thus, it must be read in conjunction with Chapter 4, which limits certain remedies (i.e., cancellation) to material breaches.

Intellectual property law determines whether a breach is also an infringement or misappropriation. For example, exceeding the permissible terms of use may constitute a contract breach and a copyright infringement, the latter

determined by federal law. In many cases, a helpful guideline is that if the conduct that breaches the agreement would infringe the relevant intellectual property right in the absence of an agreement, the conduct likely constitutes both a breach of contract and infringement. Courts in copyright cases often analyze whether a breach is also an infringement by determining whether the breach constitutes a failure of a promissory condition defining the scope of a license and implicating intellectual property rights or breach of a "covenant" (a mere promise). In making the distinction between a promissory condition and a covenant, courts look to state contract law. In using general interpretive principles under state law, a court may look, for example, to the parties' intent as revealed by their language and the placement of the term within the agreement.

Whether an aggrieved party can sue for both infringement and breach of contract depends on whether the breach-of-contract action is preempted. See § 1.09 of these Principles. In appropriate cases, an aggrieved party may have damages under both the Principles and intellectual property law so long as there is no duplication of recovery.

Illustrations:

1. Company A transfers software to Company B under terms in which B promises to use A's software to develop and market new programs only if they are compatible with A's software. B uses A's software to develop and distribute programs that are not compatible with A's software. In determining whether the compatibility requirement is a condition or a covenant, a court may look to the language of the license grant (whether the grant was expressly conditioned on meeting the compatibility requirement) and other provisions, such as the remedial scheme. If the license grant does not use language conditioning the grant on compatibility and the remedial scheme would be frustrated if A can sue for copyright infringement, the breach is most likely that of a covenant.

2. Company A transfers software to Company B under terms that permit B "to distribute versions of modified software when integrated with B's Media 100 hardware, and such versions shall be licensed only for use on such hardware." The requirement that the software be distributed only if integrated with the specified hardware should be interpreted as an express condition of the license because of the restrictive nature of the language. Thus, B's distribution of the software on other hardware would constitute an infringement.

c. Material breach. Defining material breach is difficult and courts often do not rigorously analyze the issue in particular cases, instead simply concluding that a breach is material or not. A bright-line definition is difficult because terms and manners of breach vary widely. Thus, the Restatement and UCITA both adopt a flexible approach, providing factors for a court to consider in determining whether a breach is material. The Principles generally adopt this approach, but also identify certain breaches as "per se" material in subsection (d). See Comment *d*.

The parties may define material breach in their agreement. However, particularly in the standard-form transfer of generally available software, such a definition should not be determinative. Also, any definition of material breach is subject to limiting doctrines such as unconscionability and public policy. Usage of trade, course of dealing, and course of performance may serve as independent sources of guidance to a court on what constitutes a material breach. Other relevant factors include the extent to which the aggrieved party will be deprived of the benefit of its bargain and the good faith or lack thereof of the breaching party.

Unlike the Restatement but consistent with UCITA, the Principles do not include "the likelihood that the party failing to perform or to offer to perform will cure his failure" as a factor for determining a material breach. This avoids confusing the issues of defining material breach and of when the aggrieved party has a right to cure.

Illustrations:

3. Company A transfers software to Company B under terms that permit B to distribute the software. B is obligated to pay A 40 percent of the revenue it receives when it distributes the software and to provide periodic reports

documenting its payments. B is also obligated to permit A to audit B's books for compliance with its payment obligations. A asserts that B has failed to pay royalties under the terms of the agreement, conducts an audit, and discovers a number of problems with B's payments. If the breach is material, A may cancel under § 4.04, in which case B's rights under the agreement terminate. Should B thereafter continue to use the software, it may be liable for infringement.

4. Company A transfers software to Company B under terms that require B to pay $100,000 annually over three years, with payments due 30 days after A's initial delivery and on the anniversaries of that date. B fails to make the first payment on time. This may constitute a material breach of the agreement if it so provides. In the absence of an express term, a court would consider the other factors listed under subsection (c). The longer the delay in payment in the absence of a countervailing usage of trade, course of dealing, or course of performance that would accord B more time to pay, the more likely B is in material breach of the agreement.

5. Company A transfers software to Company B under an agreement in which B agrees to "use best efforts to aggressively market and promote" the software. B never undertakes substantial marketing efforts, lacking the resources to do so. B is likely in material breach of the agreement. A contracted for B's "best efforts" and would not have contemplated that B would fail to engage in any meaningful effort. A has been "deprived of the benefit reasonably expected." Section 3.11(c)(3).

6. See Illustrations 1 and 2 to § 4.01. The exclusive remedy's failure of essential purpose is a material breach of the agreement.

7. Company A transfers software to Company B under terms permitting B to use the software within the publishing industry. The agreement does not define material breach. B agrees to an initial payment followed by periodic royalty payments. B also agrees to use a particular piece of code that functions as a hyperlink that identifies A's role in providing content and serves as advertising for A. B also agrees to make periodic reports available to A in hard-copy form and online so that A can determine if B is complying with its royalty obligations. B uses its own name in the hyperlink, which directs business to B rather than A. B continues to make royalty payments, but denies A access to online reports while providing the same reports in hard-copy form. B's failure to use the code to identify and promote A, while promoting itself and diverting business its way, is likely a material breach because it has caused A to lose business opportunities and has deprived A of a meaningful part of its bargain. B's failure to provide online royalty reports likely is not a material breach because A can still verify the appropriateness of the royalty payments using the reports in hard-copy form.

8. Company A provides Company B, a health-care provider, with a software system for use at B's call centers. The system uses algorithms to help B's operators ask the right questions so that they can advise callers on how to address their health issues. Under the agreement, each party designates two employees (one primary and one secondary) as points of contact in administering the agreement. Also, A must provide quarterly electronic updates to the software. The agreement provides that updates more than 30 days late would constitute a material breach. A party's failure to provide a secondary contact is likely not a material breach because the failure will not deprive the other party substantially of its bargain, particularly if the breaching party named a primary contact. The failure to provide timely updates is a material breach under the terms of the agreement.

9. See Illustration 1 in § 3.01. If A fails to indemnify B, A materially breaches the agreement for failing to comply with its implied indemnification obligation.

d. Per se material breaches. Subsection (d) sets forth certain breaches that are so fundamental the Principles deem them material without the need to employ the flexible test of subsection (c). Breach of the implied warranty of no material hidden defects, as well as an exclusive or limited remedy's failure of its essential purpose, go directly to the

aggrieved party's reasonable expectations regarding its bargain and do not require further inquiry before being deemed material. Breach of the restrictions on automated disablement frustrate the public policy reflected in those restrictions and thus are likewise deemed material without further analysis.

Illustration:

10. See Illustration 2 in § 3.05. The breach of the implied warranty of no hidden defects is material under § 3.11(d). The breach of express warranty is likely material under § 3.11(c).

*e. Cumulative effect of nonmaterial breach*es. Consistent with common law, the U.C.C., and UCITA, the Principles provide that the cumulative effect of nonmaterial breaches may constitute a material breach.

REPORTERS' NOTES

Comment a. Scope. See UCITA § 701(a) (2002) ("Whether a party is in breach of contract is determined by the agreement and this [Act]. A breach occurs if a party without legal excuse fails to perform an obligation in a timely manner, repudiates a contract, or exceeds a contractual use term, or otherwise is not in compliance with an obligation placed on it by this [Act] or the agreement."); see also, e.g., *Tracfone Wireless, Inc. v. Bitcell Corp., 2008 U.S. Dist. LEXIS 41955,* at *6-7 (S.D. Fla.) (tampering or altering cell-phone software in violation of Terms and Conditions constitutes a breach of contract and grounds for relief).

Comment b. Remedies generally. For a discussion of the relationship between breach and infringement, see Raymond T. Nimmer & Jeff C. Dodd, Modern Licensing Law §§ 11:24-11:27, 11:54 (2008):

Stated simply . . . in a license relationship both infringement and breach may result in cases when the defendant's conduct fails to perform a contractual obligation and infringes the exclusive rights of the rights owner. . . . If the conduct breaches an agreed obligation or limitation but not an intellectual property right, there is a contract breach but not infringement. If the conduct does not violate the agreement but infringes an intellectual property right without authorization, there is an infringement claim. . . . [C]ourts recognize a distinction between conduct that merely breaches the contract (or a covenant within the contract), and conduct that exceeds the license scope resulting also in a claim for infringement. The distinction rests on contract interpretation under state contract law principles unless an overriding federal intellectual property law policy dictates otherwise. . . . A breach of a mere covenant entitles the licensor to damages perhaps, but does not support an infringement claim so long as the licensee continues to perform within the license scope. On the other hand, breach of a scope provision entitles the licensor to both a contract remedy and an infringement claim, providing of course that there can be no double recovery.

See *Jacobsen v. Katzer, 535 F.3d 1373 (Fed. Cir. 2008)* (setting forth the distinction between conditions, which may limit the scope of a license and support an action in copyright remedies, and covenants, which are addressed by contract law, and citing authorities); *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1316 (Fed. Cir. 2005)* (reviewing authorities and concluding that "'uses' that violate a license agreement constitute copyright infringement only when those uses would infringe in the absence of any license agreement at all"); *Sun Microsys., Inc. v. Microsoft Corp., 188 F.3d 1115 (9th Cir. 1999)* (remanding to district court to determine if compatibility requirements were limitations on the scope of the license or independent contractual covenants); *Graham v. James, 144 F.3d 229 (2d Cir. 1998)* (where licensee breached by failing to pay royalties and removing licensor's copyright notice, obligations breached were covenants rather than conditions of the license and the appropriate cause of action was in breach of contract not infringement).

For cases addressing the issue of double recovery, see, e.g., *Kepner-Tregoe, Inc. v. Vroom, 186 F.3d 283, 288-289 (2d Cir. 1999)* (no double recovery where statutory damages compensated for willful copyright infringement and

consequential damages for breach of contract where licensee was required to litigate to enforce its copyrights infringed as a result of the breach); *Valve Corp. v. Sierra Entm't Inc., 431 F. Supp. 2d 1091, 1098-1102 (W.D. Wash. 2004)* (stating that the plaintiff could recover "general damages" under the contract and copyright damages for infringement); *Bieg v. Hovnanian Enters., Inc., 1999 WL 1018578,* at *6 (E.D. Pa.) ("A plaintiff . . . may consistently recover damages for breach of a licensing agreement to pay for each use of a protected work and for copyright infringement based on any use which exceeds the scope of the license. . . . It is not absolutely clear at this juncture that plaintiff can prove no set of facts which could entitle him to recover additional damages for copyright infringement beyond those for breach of the payment obligation in the license agreement.").

For the question whether intellectual property law preempts a breach-of-contract action, see § 1.09.

Comment c. Material breach. See Restatement Second, Contracts § 241:

In determining whether a failure to render or to offer performance is material, the following circumstances are significant: (a) the extent to which the injured party will be deprived of the benefit which he reasonably expected; (b) the extent to which the injured party can be adequately compensated for the part of that benefit of which he will be deprived; (c) the extent to which the party failing to perform or to offer to perform will suffer forfeiture; (d) the likelihood that the party failing to perform or to offer to perform will cure his failure, taking account of all the circumstances including any reasonable assurances; (e) the extent to which the behavior of the party failing to perform or to offer to perform comports with standards of good faith and fair dealing.

UCITA § 701(c) (2002) states:

A breach of contract is material if: (1) the contract so provides; (2) the breach is a substantial failure to perform a term that is an essential element of the agreement; or (3) the circumstances, including the language of the agreement, the reasonable expectations of the parties, the standards and practices of the business, trade, or industry, and the character of the breach, indicate that:
(A) the breach caused or is likely to cause substantial harm to the aggrieved party; or (B) the breach substantially deprived or is likely substantially to deprive the aggrieved party of a significant benefit it reasonably expected under the contract.

See also Restatement Second, Contracts § 241 and Reporter's Note to Comment *a* ("Courts frequently use 'material breach' in a conclusory fashion without indicating how or why they reached the conclusion"); *Bauhaus Software, Inc. v. TVPaint Developpement, 2007 U.S. Dist. LEXIS 59477,* at *6-19 (W.D. Tex.) (finding that a refusal to supply updates for a software product, as required by a written contract, would constitute a material breach allowing the other party to cease royalty payments).

Comment d. Per se material breaches. See §§ 3.05(b), 4.01, and 4.03 and their accompanying Comments for a discussion of the rules and their rationale.

Comment e. Cumulative effect of nonmaterial breaches. See, e.g., UCITA § 701(d) (2002).

Illustration 1 is based on *Sun Microsys., Inc. v. Microsoft Corp., 81 F. Supp. 2d 1026 (N.D. Cal. 2000).*

Illustration 2 is based on *McRoberts Software, Inc. v. Media 100, Inc., 2001 WL 1224727* (S.D. Ind.).

Illustration 3 is based on *Atlantis Info. Tech., GmbH v. CA, Inc., 485 F. Supp. 2d 224 (E.D.N.Y. 2007).* Note that under New York law the payment of royalties is assumed to be a covenant. *Id. at 233.*

Illustration 4 is based on *Teragram Corp. v. Marketwatch.com, Inc., 444 F.3d 1, 12 (1st Cir. 2006)* ("[The

defendant] admitted that it *never* made any payment to Teragram at any time during the course of their contractual relationship. [This] failure to pay, the only obligation . . . under the contract, constitutes a material breach.") (emphasis in original).

Illustration 5 is based on *In re Amica, Inc., 17 U.C.C. Rep. Serv. 2d 11 (Bankr. N.D. Ill. 1992).*

Illustration 7 is based on *Valeo Intellectual Prop., Inc. v. Data Depth Corp., 368 F. Supp. 2d 1121, 1126-1127 (W.D. Wash. 2003).*

Illustration 8 is loosely based on *McKesson Health Solutions, LLC v. Oxford Health Plans, Inc., 2006 WL 1680064* (Conn. Super. Ct.).

§ 3.12 Cure of Breach

(a) Unless otherwise agreed, a party in breach of contract may, on seasonable notice to the aggrieved party and at its own expense, cure the breach by making a conforming performance if:

(1) the time for performance has not yet expired and the conforming performance occurs within the time for performance; or

(2) the breaching party had reasonable grounds to believe the nonconforming performance would be acceptable with or without money allowance and provides a conforming performance within a further reasonable time after performance was due; or

(3) the breaching party seasonably notifies the aggrieved party of its intent to cure and promptly provides a conforming performance before the aggrieved party cancels under § 4.04.

(b) If a breaching party fails to cure a material breach, the aggrieved party's obligation to perform any remaining duties is suspended except with respect to restrictions on the use of the software. The aggrieved party also may cancel under
§ 4.04.

(c) A party may not cancel or refuse to perform because of a breach that has been seasonably cured under subsection (a).

(d) The cumulative effect of repeated attempts to cure may be a material breach.

Comment:

a. Scope. This Section is based on both U.C.C. Article 2 and UCITA. It provides a breaching party with a right to cure under certain circumstances. Certainly, the agreement itself can prohibit cure or otherwise limit it. Indeed, many, if not most, software agreements address a breaching party's right to cure in the agreement. For example, the effect of common exclusive- or limited-remedy provisions is to provide the breaching party with an ability to cure defective software by repair or replacement. More complex agreements often contain detailed provisions regarding whether and under what circumstances a breaching party is permitted to cure. Thus, an agreement may specify such matters as for what defects the breaching party may cure and the time within which it must do so. Additionally, as UCITA notes, there are some contexts, such as a breach by disclosing a trade secret, in which a breach simply cannot be cured because the damages cannot be reversed.

Illustrations:

1. Company A and Company B enter an agreement under which A agrees to install a software system at B's place of business. The agreement gives B the right to test the system for 60 days from the date of installation and to refuse it if the system contains material defects, provided that B notify A within the 60 days of the defects. The agreement also gives A the right to fix defects within 30 days after receiving a complying notice from B that identifies the defect(s) for which it was refusing to accept the system. If B finds defects and appropriately notifies A, A has 30 days from the date it receives the notice to fix the defects. If it does so, B must accept the system as repaired.

2. Same facts as Illustration 1, except that A installs the system 90 days earlier than the date required by contract. B finds a defect and notifies A 30 days after installation. A argues that it should have 60 days to fix the defects from the date it received B's notice rather than the 30 days specified in the agreement because 60 days remain before A became obligated to install the system. A must cure within 30 days. The agreement controls (unless unconscionable) rather than § 3.12(a).

Section 3.12(a)(1) follows the U.C.C. and UCITA by allowing a breaching party to cure (unless otherwise agreed) if the time for performance has not yet expired. In such cases, the aggrieved party is protected because it will still receive what it expected under the agreement.

Illustration:

3. Same facts as Illustration 2, except there is no cure provision in the contract. A may cure in the time remaining before the agreed-on date for installation.

Section 3.12(a)(2) also follows the U.C.C. and UCITA by allowing a breaching party to cure (unless otherwise agreed) if that party has reasonable grounds to believe the nonconforming performance would be acceptable with or without money allowance. A breaching party would have such grounds, for example, if the transferor provides different but "better" software than called for in the agreement or if the breaching party is a retailer passing on an already packaged product that it would have no reason to test. Of course, under § 3.12 the right to cure arises after the occurrence of a breach. The rules of interpretation set forth in §§ 3.09-3.10 define the terms of the agreement and thus what constitutes a conforming performance. If the performance conforms, there is no breach and the question of cure does not arise.

Section 3.12(a)(3) follows UCITA. The aggrieved party has a right to insist on performance and thus, under subsection (a)(3), cure must occur before it cancels the contract. The aggrieved party is not required to withhold cancellation merely because of a notice of an intent to cure. The breaching party must both notify of its intent and cure before cancellation occurs.

b. Suspension of aggrieved party's duty to perform. Subsection (b) is based on UCITA

§ 601(b), § 237 of the Restatement Second, Contracts, and common law. It is less detailed than UCITA because the principle stated in subsection (b) is well established. As the Restatement provides, the duty of one party to perform depends on the absence of an uncured material breach by the other. However, the aggrieved party may not ignore restrictions on use, including restrictions on disclosure of information under trade-secret law.

Illustration:

4. A transfers software to B under an agreement that allows B to use but not copy the software. Under the agreement, A promises to fix bugs in the software in a timely manner, but no later than three weeks after receiving notice from B. B finds a major bug, but A has not fixed the bug more than five weeks after receiving the notice. This likely constitutes a material breach and B may suspend its performance under the agreement. However, B may not copy the software.

c. Obligation to accept cure. Subsection (c) is based on UCITA § 703(c). Once the breaching party has cured (in the case of subsection (a)(3), prior to cancellation), the aggrieved party is obligated to accept the cure. The aggrieved party may still have a claim for damages for the original breach.

d. Limit on cure. A party does not have an unlimited right to cure. Repeated attempts to cure may constitute a material breach.

REPORTERS' NOTES

Comment a. Scope. For the proposition that agreements often address cure, see Raymond T. Nimmer & Jeff C. Dodd, Modern Licensing Law § 11:7 (2008) ("License agreements frequently provide for a contractual period during which the breaching party is entitled to cure defects, at least with respect to specified types of breach. 'Cure' clauses typically are explicit about the consequences of a failure to cure: remedies for breach may be enforced or, as to cancellation of the license, may occur automatically."). For examples of when cure is not applicable, see UCITA § 703 cmt. 5 (2002) ("Some contract breaches cannot be cured. This is true, for example, if a party breaches a contract by publicly disclosing licensed trade secret information. In such cases, the damage done cannot be reversed and cure is inapplicable. A similar condition may arise where the agreement demands performance on a specific date or hour, but the party materially fails to meet the deadline. Cure is an opportunity to avoid ending a contract relationship by bringing the performance into line with the other party's rightful expectations. It does not allow a breaching party to avoid the consequences of breaches that have significant irreversible effects.").

Cases addressing cure include *Computrol, Inc. v. Newtrend, L.P., 203 F.3d 1064, 1068 (8th Cir. 2000)* ("The Agreement allowed a party to terminate only in the event of material or repeated breach and after the nonbreaching party provided the breaching party a detailed notice of deficiencies and a ninety[#8209]day cure period for defaults other than payment"); *Omaha World-Herald Co. v. Neasi-Weber Int'l., 2000 WL 84430 (8th Cir. 2000)* (contract provided 60-day cure period for system provider); *Stenograph Corp. v. Microcat Corp., 1990 WL 146754* (N.D. Ill.) (10-day cure period); see also *Teragram Corp. v. Marketwatch.com, Inc., 444 F.3d 1 (1st Cir. 2006)* (exclusive remedy called for correction of any material failure reported during warranty period); *AMC Tech., L.L.C. v. SAP AG, 2005 WL 3008894 at 13* (E.D. Pa.) (noting that SAP's standard End User License Agreement permits SAP to "cure negligence or breach by bringing 'the performance of the Software into substantial compliance with the functional specifications'").

For non-software cases involving (i) the seller providing a different but "better" good than contracted for, see, e.g., *Bartus v. Riccardi, 284 N.Y.S.2d 222 (1967)* (newer model of hearing aid provided rather than one ordered); and (ii) the seller's passing on an already-boxed product that it would have no reason to test, see, e.g., *Wilson v. Scampoli, 228 A.2d 848 (D.C. Ct. App. 1967)* (TV sold by retail dealer as crated by the factory).

Comment b. Suspension of aggrieved party's duty to perform. See Restatement Second, Contracts § 237 ("[I]t is a condition of each party's remaining duties to render performances to be exchanged under an exchange of promises that there be no uncured material failure by the other party to render any such performance due at an earlier time."); UCITA § 601(b) (2002) ("If an uncured material breach of contract by one party precedes the aggrieved party's performance, the aggrieved party need not perform except with respect to restrictions in contractual use terms.").

Comment c. Obligation to accept cure. See UCITA § 703 (2002); Restatement Second, Contracts § 242, Comment *a*. ("Ordinarily there is some period of time between suspension and discharge, and during this period a party may cure his failure. Even then, since any breach gives rise to a claim, a party who has cured a material breach has still committed a breach, by his delay, for which he is liable in damages.").

Illustration 1 uses a variation of the contractual terms in *Omaha World-Herald Co., supra.*

Return to Text

n1 1 Douglas E. Phillips, When Software Fails: Emerging Standards of Vendor Liability Under the Uniform Commercial Code, *50 Bus. Law. 151, 151-155 (1994);* see also Diane W. Savage, Performance Warranties in Computer Contracts, 8 No. 12 Computer Law. 32, 32 (1991), available at http://library.findlaw.com/1997/Nov/1/128553.html (last visited Aug. 19, 2009) ("computer litigation is on the increase").

The *Wall Street Journal* reports that a Malaysia Airlines jetliner "suddenly took on a mind of its own, and zoomed 3000 feet upward." It took the crew 45 seconds to regain control of the plane. The cause was defective software that provided the wrong data about the plane's speed. Daniel Michaels & Andy Pasztor, Incidents Prompt New Scrutiny of Airplane Software Glitches, Wall St. J., May 30, 2006, at A1.

n2 2 See, e.g., Lorin Brennan, Why Article 2 Cannot Apply to Software Transactions, *38 Duq. L. Rev. 459, 506-508 (2000);* see also *VMark Software, Inc. v. EMC Corp., 642 N.E.2d 587, 596 (Mass. App. Ct. 1994)* (a "seasoned user of computer systems" should know that customized technology requires some "debugging."); *Lovely v. Burroughs Corp., 527 P.2d 557, 560 (Mont. 1974)* (malfunction after "debugging").

n3 3 *Phillips, supra* note 1, at 151.

n4 4 Nim Razook, The Politics and Promise of UCITA, *36 Creighton L. Rev. 643, 655 (2003).*

n5 5 Cem Kaner, Why You Should Oppose UCITA, 17 No. 5 Computer Law. 20, 23 (2000), available at http://www.kaner.com/pdfs/ComputerLawyer.pdf (last visited Aug. 19, 2009). ("It is impossible to test software products exhaustively or to prove by testing that a product is defect free."); see also Paul S. Hoffman, Software Warranties and the Uniform Commercial Code, 6 No. 4 J. Proprietary Rts. 7, 11 (1994) (discussing software's uniqueness and complexity). But Kaner also asserts that defect-free software is not so pie-in-the-sky. Kaner, supra at 24.

n6 6 See Barkley Clark & Christopher Smith, The Law of Product Warranties § 2:23 (Database update Nov. 2008); Savage, supra note 1.

n7 7 See, e.g., Robert W. Gomulkiewicz, The Implied Warranty of Merchantability in Software Contracts: A Warranty No One Dares to Give and How to Change That, 16 J. Marshall J. Computer & Info. L. 393, 398 (1997) ("In the software contract warranty cases that have arisen, the courts have made no attempt to tailor their construction of the warranty to the unique nature of software or software transactions."). But see *Carl Beasley Ford, Inc. v. Burroughs Corp., 361 F. Supp. 325, 330-331 (E.D. Pa. 1973),* aff'd, *493 F.2d 1400 (3d Cir. 1974)* (while software often requires debugging, 8 months of attempts to make the software work are enough).

n8 8 UCITA creates two implied warranties for software: the warranty of noninfringement, and the warranty of quiet enjoyment. Uniform Computer Information Transactions Act, § 401 (2002).

n9 9 Clark & Smith, supra note 6. Transferees generally win warranty cases only when the transferor has neglected to include disclaimers or has failed to follow accurately the roadmap for disclaiming in Article 2. For a recent case narrowing the warranty to substantial conformance to the documentation within 30 days of delivery of the software, see *Teragram Corp. v. Marketwatch.com, Inc., 444 F.3d 1 (1st Cir. 2006).*

n10 10 Kaner, supra note 5, at 27-28.

n11 11 U.C.C. Article 2A, governing leases, follows a similar strategy.

n12 12 Hoffman, supra note 5, at 11 ("Software of any sophistication is rarely bug-free even after years of use.").

n13 13 See these Principles, supra Chapter 2, Summary Overview to Topic 2 and § 2.02.

n14 14 See, e.g., *AMF, Inc. v. Computer Automation, Inc., 573 F. Supp. 924, 929 (S.D. Ohio 1983)* (enforcing disclaimers because of the "commercial sophistication" of the businesses).

n15 15 See infra § 3.02(b)(1).

n16 16 See infra § 3.02, Comment *b*.

n17 17 U.C.C. § 2-316(1) ("Words or conduct relevant to the creation of an express warranty and words or conduct tending to negate or limit warranty shall be construed wherever reasonable as consistent with each other . . . negation or limitation is inoperative to the extent that such construction is unreasonable."); see also Ajay Ayyappan, UCITA: Uniformity at the Price of Fairness?, *69 Fordham L. Rev. 2471, 2478-2485 (2001).*

n18 18 See infra § 3.06, Comment *a*, of these Principles, and the corresponding Reporters' Note.

n19 19 See infra § 3.06. See also Hoffman, supra note 5, at 16 ("[C]ustomized software involves some modification to standard software, custom software implies the creation of a new program or set of programs from scratch.").

n20 20 H. Ward Classen, A Practical Guide to Software Licensing for Licensees and Licensors: Analyses and Model Forms 71-74 (ABA 2005).

n21 21 See, e.g., Omri Ben-Shahar & James J. White, Boilerplate and Economic Power in Auto Manufacturing Contracts, *104 Mich. L. Rev. 953, 962 (2006)* (auto industry defers to software suppliers).

n22 22 Razook, supra note 4, at 663; see also Matthew D. Stein, Rethinking UCITA: Lessons From the Open Source Movement, *58 Me. L. Rev. 157, 179 (2006).*

n23 23 Ayyappan, supra note 17, at 2488-2489; Edward G. Durney, The Warranty of Merchantability and Computer Software Contracts: A Square Peg Won't Fit in a Round Hole, *59 Wash. L. Rev. 511, 521-523 (1984);* Hoffman, supra note 5, at 7.

n24 24 *Phillips, supra* note 1, at 155-156 (reliability means "'the probability of failure-free operation of a computer program for a specified time' in a given environment," and software "'failure'" occurs when software "'has not met user requirements in some way.'") (quoting Victor R. Basili & John D. Musa, The Future Engineering of Software: A Management Perspective, in Software Management 9, 10 (Donald J. Reifer ed., 4th ed. 1993); John D. Musa et al., Software Reliability: Measurement, Prediction, Application at 5, 15 (Prof. ed. 1990)); see also Savage, supra note 1 ("A standard software . . . warranty provides . . . that the software 'performs substantially in accordance' with an identifiable set of functional specifications.").

n25 25 Hoffman, supra note 5, at 9 ("Sometimes errors are graded in severity from Class 1 (unable to use the software productively) through Class 2 (significant interference with operation of the software) to Class 3 (interferes with but does not prevent productive use of the software).").

n26 26 See, e.g., Gomulkiewicz, supra note 7, at 399 ("[C]omputer programs are essentially diverse collections of ideas that cannot reasonably be compared to one another.").

n27 *27 Id. at 400* ("[M]ost mass-market software products are neither experimental nor custom-made.").

n28 28 Free Software Foundation, Why We Must Fight UCITA, http://www.gnu.org/philosophy/ucita.html

(last visited Aug. 19, 2009).

n29 29 See Chapter 2, Topic 2, on disclosure.

n30 30 Section 3.04(a). The Section follows U.C.C. § 2-315 and UCITA § 405(a) (2002).

n31 31 U.C.C. § 2-315.

n32 32 See § 3.05(b); Kaner, supra note 5, at 23-24. ("[L]et the new law reduce publisher risk for losses caused by previously undiscovered defects or defects that were disclosed to the customer, but reduce the customer's risk of losses caused by defects that were known and left hidden.") Jean Braucher states that "[b]ugginess of software is a choice of producers that externalizes huge costs." Memorandum of Jean Braucher, March 14, 2003.

n33 33 Cf. Kaner, supra note 5, at 23.

n34 *34 Id. at 28.* See Magnuson-Moss Warranty Act, *15 U.S.C. §§ 2301-2312* (West, Westlaw through 2009).

n35 35 *15 U.S.C. § 2308(a)(1)*.

n36 36 The Magnuson-Moss Act applies to sales of "consumer products," which are defined as "any *tangible* personal property which is distributed in commerce and which is normally used for personal, family or household purposes . . . ." *15 U.S.C. § 2301(1)* (emphasis added). Thus, "it seems clear that computer hardware and software which is sold through retail outlets . . . will constitute 'consumer products,' and, as such, will be subject to the warranty disclosure requirements of the Magnuson-Moss Act." Savage, supra note 1. Magnuson-Moss may not apply to software downloads, however.

n37 37 See Stein, supra note 22, at 199 ("Because of the collaborative nature of the open source development model, hundreds or even thousands of programmers contribute source code to open source projects. Liability for infringement and implied warranties of merchantability and fitness for a particular purpose are potentially substantial disincentives to contribution to open source projects.").

n38 38 See § 3.06(f).

n39 1 See, e.g., *Playmedia Sys., Inc. v. Am. Online, Inc., 171 F. Supp. 2d 1094 (C.D. Cal. 2001).*

n40 2 See § 3.08, Reporters' Notes.

n41 3 See, e.g., *S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081 (9th Cir. 1989);* Principles, §§ 1.09 and 1.10.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

How a License Becomes a Sale: Software Applications of the First Sale Doctrine

2008 Emerging Issues 2823

Claypoole on How a License Becomes a Sale: Software Applications of the First Sale Doctrine

By Ted Claypoole

September 8, 2008

SUMMARY: Even careful drafting of a software license can be stripped of its protections by a court. In some cases, United States courts have declared that standard software licenses must be interpreted as a sale of goods, granting the software users rights never intended by the software company. This commentary, written by software contracting attorney Ted Claypoole, examines a recent movement to apply the first sale doctrine to software licenses.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Even careful drafting of a software license can be stripped of its protections by a court. In some cases, United States courts have declared that standard software licenses must be interpreted as a sale of goods, granting the software users rights never intended by the software company.

Analysis

Many software companies deliver a licensed copy of their product to customers. These software licenses strictly define what the customer is allowed to do with the software, and most of them severely limit the customers right to sell or transfer the software to any other company or user.

Recently, several courts have held that some of these arrangements may not be licenses at all, but should be considered a sale of goods that would allow later purchasers of the software to use, sell or dispose of the software in any way they wish, ignoring restrictions in the original product license. Under these court rulings, software companies that do not use the right language restricting distribution of the products may lose the ability to enforce important license restrictions.

In short, if a software manufacturer allows its customers to keep a copy of licensed software, then the manufacturer runs a significant risk that the copy can be resold despite restrictions on resale built into the license. In a clear example of this trend, the Eastern District of Washington held in May, 2008 that a license of software can be considered a sale for purposes of the first sale doctrine. This ruling stopped a software company from enforcing restrictions in its license.

The *Vernor* Case Applies the First Sale Doctrine to a Software License

The court in *Vernor v. Autodesk, Inc., No. 07-1189, 2008 U.S. Dist. LEXIS 43693* (W.D. Wash. 5/20/2008), held

that Autodesk, an established manufacturer of commercial design software, sold its products for the purposes of the Copyright Acts first sale doctrine, ignoring transfer restrictions from those products. The court interpreted the Autodesk license in a way that removed many of the restrictions on resale contained in the original contract.

The first sale doctrine states that a copyright holder loses the right to enforce a copyright over a copy of a product that has already been sold in commerce. For example, this doctrine prohibits a book publisher from suing to restrict a the transfer of a book already legitimately sold to a store or a customer. The first sale doctrine is codified in U.S. law at *17 U.S. Code 109(a)*, which provides that

Notwithstanding the provisions of section 106(3), the owner of a particular copy . . . lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy . . . .

According to the Historical note to section *17 U.S.C. section 109*, the statute restates and confirms the principal that, where the copyright owner has transferred ownership of a particular copy . . . of a work, the person to whom the copy . . . is transferred is entitled to dispose of it by sale . . . or by any other means.

While the first sale of a copyrighted product exhausts the copyright holders right to restrict transfer of a copy of its work, a first sale does not exhaust other rights, such as the copyright holders right to prohibit duplication of the copy he sells. *See, United States v. Wise, 550 F.2d 1180, 1187 (9th Cir. 1977).* For example, the first sale doctrine permits a consumer who buys a lawfully made DVD copy of Gone With the Wind to resell the copy, but not to duplicate the copy. *Vernor*, at page 6.

A Second Purchase of a Software Copy May Avoid License Restrictions

The cases like *Vernor* that apply the first sale doctrine to software licenses, generally involve a software seller who did not buy from the original manufacturer. These cases are relevant to the practical business of creating a secondary market for certain expensive software products. The original license language of most commercial software products limits or forbids resale by the licensee, so that a secondary market for these products, on eBay or otherwise, is not possible in compliance with the licenses.

However, if the first sale doctrine applies to many software licenses, then consumers could more readily find and purchase used copies of the software at low prices, and not be forced to pay higher prices for new copies sold by the manufacturer. The legitimate market for used software could resemble the used car market, with thousands of models available to everyone.

Whoever Keeps the Copy May Have The Right to Dispose of the Copy

In the *Vernor* case, Mr. Vernor makes his living selling goods on eBay, where he tried to sell two packages of Autodesks copyrighted AutoCAD software. Mr. Vernor had purchased the authentic used AutoCAD software packages from an office sale at a Seattle architecture firm, and Autodesk objected to Mr. Vernors attempts to sell used copies of its software, claiming that such secondary sales violated Autodesks software license, and that Mr. Vernor must follow the license even though he did not purchase new copies of AutoCAD from Autodesk. In other words, Autodesk felt that it could impose the sales and transfer terms of its license upon Mr. Vernor, even though Autodesk was not in privity of contract with Mr. Vernor. n1

The court disagreed with Autodesk. It looked to the Ninth Circuits *Wise* decision as the primary authority (addressing film prints, rather than software), even though the *Vernor* court analyzed three more recent Ninth Circuit decisions that reached results contrary to *Wise*. n2 The Vernor court held, In comparing the transactions found to be sales in *Wise* with those that were not, the critical factor is whether the transferee kept the copy acquired from the copyright holder.

The Practitioner should note that where a copyright holder limits use of a copy of its product, but allows the first holder to keep the copy, then both *Wise* and *Vernor* hold that the transaction more resembles a sale with restrictions on use of the print then it resembles a traditional license. n3 The Court in *Vernor* concluded that Autodesks first transfer of AutoCAD packages was a sale with contractual restrictions on use and transfer of software, and that Mr. Vernors resale was not a copyright violation.

Other courts also found that where a copyright holder allows a user of its copyrighted material to keep a copy of that material, then the transaction is likely to be viewed as a sale for purposes of the first sale doctrine. The logic of *Vernor* regarding the first sale doctrine has been subsequently followed within the Ninth Circuit in *UMG Recordings, Inc. v. Augusto, 2008 U.S. Dist. LEXIS 48689* (C.D. Cal 6/10/2008), holding that the absence of a distributors intent to regain possession of a copyrighted product is strong evidence that the product was sold, not licensed, which would permit the sale or disposition of the product under copyright laws first sale doctrine. The *Augusto* court held found the following facts to be influential, and possibly dispositive, for determining whether copyrighted products were sold or licensed:

. The copyright holder gives copies of its materials and does not ask that those materials are returned.

. There are no consequences for the recipient should she lose or destroy the copyrighted materials.

. The copyright holder does not make affirmative efforts to recover the copies.

. The copyright holder does not keep permanent records identifying who received copies of the materials.

These facts and the nature of the copyright holders license led the Augusto court to find that the materials could be resold pursuant to the first sale doctrine, despite any license terms to the contrary.

In the Second Circuit, *Krause v. Titleserv, Inc., 402 F.3rd. 119 (2d Cir. 2005),* held that The right to perpetual possession is a critical incident of ownership. Addressing a different copyright question with regard to software (*17 U.S.C. Section 117(a)*), the Krause court made the distinction between the rights of the copyright owner versus the rights of an owner of a copy of the copyrighted material and it held that a persons degree of ownership of a copy as complete when he may lawfully use it and keep it forever, or if so disposed, throw it in the trash. *Id. At 123.*

After noting with favor cases that find software to be a good within the meaning of the Uniform Commercial Code, n4 the Federal District Court for the District of Utah held that the purchase of upgraded software by end-users from software distributors were sales of goods which gave rise to the first sales doctrine, so that the end-users were owners, not merely licensees, of software. Therefore, the court found that end-users did not infringe copyright by using or disposing of the software. *Novell, Inc. v. Network Trade Center, Inc., 25 F.Supp.2d 1218 (D. Utah 1997).*

The court stated that software transactions passing possession to end users under a shrinkwrap license do not merely constitute the sale of a license to use the software. The shrinkwrap license included with the software is therefore invalid as against such a purchase insofar as it purports to maintain title to the software in the copyright owner. *Id. at 1231.*

Practice Tip

Practitioners who draft software license agreements, or first licenses to use copies of intellectual property like films and music, should be aware that allowing a licensee to keep a copy of the software or other copyrighted material may render transfer restrictions in the license agreement unenforceable, particularly against future holders of the copy. Drafters who represent software producers should consider including in every agreement a demand for return of the software immediately upon termination of the license, and the software producer should build a procedure for collecting this software.

Opposing Viewpoint

Not all courts will apply the first sale doctrine to software licensors who allow their licensees to keep copies of the software. Several courts have ruled in the opposite direction. For example, in the case of *Microsoft Corporation v. Harmony Computers and Electronics, 846 F. Supp, 208 (E.D.N.Y. 1994),* the court simply held that entering into a software license agreement is not a sale for purposes of the first sale rule, and that the only authorized holders of Microsofts software were bound by the applicable Microsoft product license.

Similar holdings can be found in earlier California cases, *Adobe Systems, Inc. v. One Stop Micro, Inc., 84 Fed Supp.2d 1086 (N.D.Cal. 2000)* (The first sale doctrine applies only to actual sales; the copyright owner does not forfeit its right of distribution by entering into a license agreement.) and *Adobe Systems, Inc. v. Stargate Software Inc., 216 F.Supp2d 1951 (N.D.Cal. 2002)* (A software manufacturers distribution of copies of its software to licensed distributors did not constitute a sale of copies under the first sale doctrine, and would not preclude the manufacturer from asserting copyright claims against a purchaser engaging in unlicensed redistribution of copies.).

Rebuttal.

A later case, *Softman Prods. Co., LLC v. Adobe Sys., Inc., 171 F. Supp. 2d 1075 (C.D. Cal. 2001),* distinguished *Microsoft v. Harmony* and rejected *Adobe Systems, Inc. v. One Stop Micro, Inc.,* finding that a purchaser of Adobe software was entitled to the protections of the first sale doctrine. The Softman court found that a shrinkwrap license transaction was a sale of goods because, as in any sale of goods, the purchaser obtains a single copy of the software, with documentation, for a single price, which the purchaser pays at the time of the transaction, and which constitutes the entire payment for the license. The license runs for an indefinite term without provisions for renewal.

Conclusion.

Imposing unilateral and one-sided contracts upon their customers, software companies claim that their licenses and copyrights can control distributors and users of their software several steps down the transfer chain from the manufacturer or its original customer, well beyond those parties in actual privity of contract with the software manufacturer. American cases have applied the first sale doctrine to avoid this result. As stated in the classic treatise Nimmer on Copyrights, The vast bulk of popular software as of the time that the foregoing line of cases was decided accordingly falls under the first sale doctrine. *Nimmer section 8.12*.

Return to Text

n1 In rulings where the seller did not purchase directly from the manufacturer, the manufacturer may have lost its right to sue that party for transferring a copy of a software product, but the manufacturer may still have a claim against its original customer for transferring the software. [A] first sale buyers disregard of restriction on resale does not make buyer or subsequent buyer a [copyright] infringer; [a] copyright holders remedy is suit for breach of contract containing the restrictions. *Denbicare U.S.A. Inc. v. Toys R Us, Inc., 84 F.3d 1143, 1152 (9th Cir. 1996),* as cited by *Vernor,* page 6.

n2 The court analyzed the following cases and found them to be irreconcilably opposed to the findings in *Wise,* but found that Wise must be followed because it was the first decided case on the subject in the Ninth

Circuit. *MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993)* (addressing the first sale doctrine in a cursory footnote); *Triad Sys. Corp. v. Southeastern Express Co., 64 F.3d 1333 (9th Cir. 1995)* (implicitly concluding that a license could not be a sale); and *Wall Data Inc. v. Los Angeles County Sherriffs Department, 447 F.3d 769, 785* (9th cir. 2006) (holding that a license that did not contain restrictions on sale of the software still imposed those restrictions on the licensee).

n3 The *Wise* court held that the copyright laws protect the right of the copyright holder to sell its work, but that right is not absolute, but is subject to the first sale doctrine *Wise* at 1187. The courts opinion stated, While the proprietors other copyright rights (reprinting, copying, etc.) remain unimpaired, the exclusive right to vend the transferred copy rests with the vendee, who is not restricted by statute from further transfers of that copy, even though in breach of an agreement restricting its sale. *Id.*

n4 See, *Advent Sys. Ltd. V. Unisys Corp, 925 F.2d 670 (3rd Cir. 1991); Step-Saver Data Sys., Inc. v. Wyse Technology, 939 F.2d 91 (3rd Cir 1991); Downriver Internists v. Harris Corp., 929 F.2d. 1147 (6th Cir. 1991).*

RELATED LINKS: For a detailed analysis of the application of the first sale doctrine to software and entertainment licenses granting restricted use rights to a copy of the subject material, see:

- Computer Law, Chapter 4, Matthew Bender & Company, Inc. (2008).;
- Nimmer on Copyright, Chapter 8, Part III, Matthew Bender & Company, Inc. (2008).;
- Copyright Law, by Bruce Keller and Jeffrey P. Cunard, Chapter 4, Practicing Law Institute (2008).

ABOUT THE AUTHOR(S):

Ted Claypoole is a Member of Womble Carlyle Sandridge and Rice in its Technology Transaction Team, concentrating his practice on software contracting, supply chain management and outsourcing legal issues, as well as data management and protection. Claypoole has served as corporate counsel for CompuServe, Inc. and as assistant general counsel at Bank of America, concentrating on the banks technology, ecommerce, data security and intellectual property. A 1985 honors graduate of Duke University and 1988 graduate of the Ohio State University College of Law, he regularly writes and speaks on the intersection between the law and information technology, including recent presentations on Marketing in Online Social Networks, Offshore Business Process Agreements, and The Ethics of Pervasive Biometrics.

Bensen on Holding that Real Estate Agencys List of Renters Not a Trade Secret

2008 Emerging Issues 2004

Bensen on Holding that Real Estate Agencys List of Renters Not a Trade Secret

By Eric E. Bensen

March 6, 2008

SUMMARY: Use Title Below instead of Online Display Name for the ADF/Case Link:Eric E. Bensen on the South Carolina Supreme Courts Holding that a Real Estate Agencys List of Renters Did Not Constitute a Trade Secret: *Atwood Agency v. Black, 646 S.E.2d 882 (S.C. 2007).* In Atwood Agency, the South Carolina Supreme Court, over the thoughtful dissent of one justice, reversed the lower courts ruling that a real estate agencys list of vacation home renters was a trade secret because the defendant, a former property manager who left the agency to work for a competitor, was able to obtain some of the information on the list from other sources. The dissenting justice would have affirmed the lower courts holding that the list was a trade secret because the availability of some of the information on the list did not mean that the list as a whole was readily ascertainable from sources other than plaintiff. This expert commentary is written by Eric E. Bensen is a co-author of Milgrim on Licensing and Milgrim on Trade Secrets, the author of a number of articles on intellectual property issues, and an attorney with Paul, Hastings, Janofsky & Walker LLP in New York, where he focuses his practice on intellectual property litigation and licensing.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: In *Atwood Agency*, the South Carolina Supreme Court, over the thoughtful dissent of one justice, reversed the lower courts ruling that a real estate agencys list of vacation home renters was a trade secret because the defendant, a former property manager who left the agency to work for a competitor, was able to obtain some of the information on the list from other sources. The dissenting justice would have affirmed the lower courts holding that the list was a trade secret because the availability of some of the information on the list did not mean that the list as a whole was readily ascertainable from sources other than plaintiff.

Summary of the Case

The Atwood Agency (Atwood) was in the business of matching property owners on Edisto Island in South Carolina with renters seeking vacation accommodations. Defendant Elaine Shaw worked for Atwood for fifteen years as a property manager overseeing the rental of vacation homes in Edisto Beach. In that role, she had contact with both renters and property owners. In 2005, she left Atwood to work for a competitor, Edisto Sales and Rental Realty (Edisto Sales). Claiming that it subsequently lost more than fifty rentals to Edisto Sales, Atwood brought suit against Shaw and

others for, among other things, trade secret misappropriation under the South Carolina Trade Secrets Act (SCTSA).

At issue were two lists that Atwood used in its business: a Homeowners List of the property owners and a Renters List of vacationers who used Atwoods services. The identities of all homeowners in Edisto Beach and their contact information was a matter of public record available at the Edisto Beach Town Hall. While there was no corresponding source for renter information, Shaw testified that she was contacted directly by Atwood renters after Atwood announced her departure. There was also evidence that homeowners sometimes kept guest books containing renter contact information.

The lower court granted an *ex parte* temporary restraining order enjoining Shaw and the other defendants from contacting or contracting with vacation renters or homeowners of Atwoods. The court later granted a preliminary injunction based on a finding that both the Homeowners List and the Renters List were trade secrets. Atwood appealed.

Pertinent Legal Principles

Definition of Trade Secret. In all but a handful of states, the definition of a trade secret is provided by the Uniform Trade Secret Act (UTSA). South Carolina repealed its UTSA when it adopted SCTSA in 1997, but nonetheless kept the UTSAs trade secret definition, which provides that a trade secret is information that (i) derives independent economic value from not being generally known to, and not readily ascertainable by proper means by the public or any other person who can obtain economic value from its disclosure or use and (ii) is the subject of efforts reasonable under the circumstances to maintain its secrecy. S.C. Code Ann. § 39-8-20(5)(a); *cf.* USTA § 1.

The SCTSA, unlike the UTSA, however, additionally provides that a trade secret may consist of a simple fact, item, or procedure, or a series or sequence of items or procedures which, although individually could be perceived as relatively minor or simple, collectively can make a substantial difference in the efficiency of a process or the production of a product, or may be the basis of a marketing or commercial strategy. S.C. Code Ann. § 39-8-20(5)(b). The meaning of this additional language has not been the subject of much decisional law, but has been construed to expand rather than restrict the core trade secret definition that the SCTSA shares with the UTSA. *See BBA Nonwovens Simpsonville, Inc. v. Superior Nonwovens, LLC, 303 F.3d 1332, 1340, 64 U.S.P.Q.2d 1257 (Fed. Cir. 2002)* (use of permissive language (i.e., may consist of) in § 39-8-20(5)(b) demonstrates legislatures intent to expand trade secret protection).

For a discussion of the SCTSA as well as the UTSA as adopted by other states, see 1 Roger M. Milgrim & Eric E. Bensen, *Milgrim on Trade Secrets § 1.01*[3] (2008).

Customer Lists as Trade Secrets. It is very often the case that the most valuable asset of a business is its relationships with its customers. Not surprisingly, therefore, a common subject of trade secret litigation is the alleged misappropriation of information concerning customer relationships. The central issue in such litigations is typically whether the allegedly misappropriated information warrants trade secret protection.

Customers lists are, of course, information and information can be a trade secret if it derives independent economic value from not being readily ascertainable by proper means and is the subject of reasonable efforts under the circumstances to protect its secrecy. The question of whether a particular customer list is entitled to trade secret status, however, can be challenging. Simply put, a practioner cannot take it for granted that, *e.g.*, a clients customer list for his laundry business is a trade secret just because similar lists have been afforded trade secret protection in other jurisdictions.

The differing treatments that may be given to customer lists of a similar nature has less to do with different legal standards being applied under the UTSA than it does with the specific information being offered up as the trade secret. For instance, the identities of transmission repair shops on one list may be a list of prospects identified through a great deal of effort while the identity of such shops on another list may be readily available from a trade organization or even

the local phone book. The former will likely qualify as a trade secret while the latter probably will not. In the latter case, however, the list may nonetheless have trade secret status by virtue of customer-specific information such as the owners contacts at the customers, rates or discounts given to the customer, or expiration dates for the contracts with the customer. Even then, however, no trade secret status will obtain if such information is readily ascertainable by other means, such as by calling the customer.

Factors other than the nature of the information on the list may also be dispositive of the issue. For example, a party may be held liable for use of a former employers customer list because the use violated restrictive covenants in an employment agreement regardless of whether the list was entitled to trade secret protection. On the other hand, an otherwise protectable list may be denied trade secret status because of the owners failure to make efforts reasonable under the circumstances to protect the secrecy of the list.

Thus, in determining whether a particular customer list should qualify for trade secret protection, the practioner should focus less on whether lists of a similar nature have been afforded trade secret status in other litigations (although that can provide guidance), and more on the basics, *i.e.*, whether the information is readily ascertainable by other means, whether it was subject to efforts reasonable under the circumstances to keep it secret, and whether the accused party is subject to any restrictive covenants prohibiting his use of the list.

For a discussion of the treatment of customer lists under trade secret law, see *Milgrim on Trade Secrets § 1.09*[7].

The South Carolina Supreme Courts Holding

The central issue on appeal was whether the Homeowner List and the Rental List qualified as trade secrets. The court, overturning the lower courts decision, held that they did not because the information they contained was available from other sources. In so concluding, the court focused on the availability of homeowner information from public records, Shaws testimony to the effect that renters took the initiative to contact her and the fact that some homeowners kept information concerning their renters.

In separate opinion, Justice Plecones concurred with the portion of the majoritys opinion concerning the Homeowners List, but dissented from the portion of the opinion concerning the Renters List. In Justice Plecones view, a vacation rental agency derives independent economic value from protecting the identity of its renters because its renters list is not readily ascertainable by proper means, and therefore, Atwoods Rental List qualified as a trade secret. The fact that Shaw received the identity of some of Atwoods renters from the renters themselves or from homeowners was relevant to the question of whether Shaw received that information by proper means but, in the Justices view, it did not establish that the list was readily ascertainable.

Comment

That the Homeowners List did not qualify for trade secret protection should come as no surprise. While using that list may have been more convenient than a trip to the Town Hall to gather the same information, there was no serious question that the information on the list was readily ascertainable from legitimate sources so as to defeat trade secret protection.

As to the Renters List, however, Justice Plecones had the better of the argument. The majoritys holding that Shaws independent access to some renter information meant the *list* was readily ascertainable gave unfortunately light treatment to the issue. Certainly, had Shaw been reasonably able to get all of the information from the Renters List from other sources, the lists status as a trade secret would be open to serious question. However, in most cases arising from the alleged misappropriation of a customer list, some of the trade secret claimants customer information will be available by other means. That fact will not by itself defeat trade secret protection for the claimants list as a whole

because the list as a whole may nonetheless derive value from not being readily ascertainable by legitimate means. Shaws independent access to renter information was, as Justice Plecones pointed out, relevant to whether a misappropriation had occurred and would have also been relevant to the value of the Renter List as a trade secret, but the availability of some of the information on the list from other sources should not have been enough, by itself, to defeat trade secret status for the list.

ABOUT THE AUTHOR(S):

Eric E. Bensen is a co-author of Milgrim on Licensing and Milgrim on Trade Secrets, the author of a number of articles on intellectual property issues, and an attorney with Paul, Hastings, Janofsky & Walker LLP in New York, where he focuses his practice on intellectual property litigation and licensing.

12 of 18 DOCUMENTS

Ted Claypoole on Awarding Punitive Damages for an Inadvertent Privacy Breach

2008 Emerging Issues 1868

Ted Claypoole on Awarding Punitive Damages for an Inadvertent Privacy Breach

By Ted Claypoole

February 6, 2008

SUMMARY: Use Title Below instead of Online Display Name for the ADF/Case Link:Ted Claypoole on Awarding Punitive Damages for an Inadvertent Privacy Breach: *Randi A.J. v. Long Island Surgi-Center, 2007 NY Slip OP 6953; 46 A.D. 3d 74; 842 N.Y.S. 2d 558* (NY App. Div., Second Department, Sept. 25, 2007)Evolving personal privacy law creates a minefield of risk for businesses maintaining databases of their customers or patients personal information. Even an inadvertent error in handling this data can lead to costly compensatory and punitive damages. This commentary, written by data management attorney Ted Claypoole, highlights the dangers of lax data policies which can lead to a large punitive damage award arising from a mistaken release of information, as described in the New York Appellate Divisions Randi A.J. v. Long Island Surgi-Center decision. Ted Claypoole is a Member of Womble Carlyle Sandridge and Rice in its Technology Transaction Team, concentrating his practice on internet and data management legal issues. Claypoole has served as corporate counsel for CompuServe, Inc. and as assistant general counsel at Bank of America, concentrating on the banks technology, ecommerce, data security and intellectual property.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Evolving personal privacy law creates a minefield of risk for businesses maintaining databases of their customers or patients personal information. Even an inadvertent error in handling this data can lead to costly compensatory and punitive damages. This commentary, written by data management attorney Ted Claypoole, highlights the dangers of lax data policies which can lead to a large punitive damage award arising from a mistaken release of information, as described in the New York Appellate Divisions *Randi A.J. v. Long Island Surgi-Center* decision.

Analysis. Many U.S. jurisdictions allow vicarious punitive damages against a company where the wrongful actions of the companys agents lacked malice, but those cases are often limited to product liability or incidents resulting in death or grave bodily harm. An appellate court in New York has extended the imposition of such damages to a case where the defendant inadvertently released confidential personal information to a plaintiffs mother in violation of the plaintiffs request. Practitioners should advise business clients who handle sensitive information to create and follow reasonable procedures for protecting this information, or risk being swamped in the rising tide of legal punishment for sloppy data management.

The Case. In *Randi A.J. v. Long Island Surgi-Center, 2007 NY Slip OP 6953; 46 A.D. 3d 74; 842 N.Y.S. 2d 558* (NY App. Div., Second Department, Sept. 25, 2007), the plaintiff scheduled an abortion procedure at defendants clinic,

requesting that she not be contacted at her home number or address. Following the procedure, defendants agent called plaintiffs home with laboratory results and gave plaintiffs family enough information to deduce that plaintiff had received an abortion. The plaintiff sued, asserting that the defendant breached its legal duty to keep her information private, and the jury awarded compensatory damages of $65,000 for past and future emotional distress and $300,000 in punitive damages. The defendant appealed the punitive damage award.

The New York Appellate Court upheld the punitive damage award, even though the majority found that the record does not demonstrate a bad-faith, intentional violation of the plaintiffs rights or an act done maliciously with the purpose of causing injury. The majority held that New York law did not require bad faith or malicious motive as necessary elements of punitive damages, but instead, punitive damages could be awarded for the conscious disregard of the rights of others or for conduct so reckless as to amount to such disregard.

The majority of the *Randi A.J.* court found that the defendant was required to have a written plan to preserve patient privacy (N.Y. Public Health Law section 2803-c(5)), and that the defendant had none. In addition, the clinics policies regarding patient confidentiality requests were confusing, inconsistent and poorly executed, and the clinic failed to follow its own policies regarding testing and notification of patients. Note that a business failure of policy and procedure with regard to patient privacy was enough to support not only compensatory damages for the plaintiffs emotional distress, but also punitive damages.

Punitive Damages. In New York, conduct warranting an award of punitive damages need not be intentionally harmful but may consist of actions which constitute willful or wanton negligence or recklessness. *Home Insurance Company v. American Home Products Corporation, 75 NY2d 196, 204 (1990); Guariglia v. Price Chopper Operating Company, Inc., 830 N.Y.S.2d 871 (NY Appellate Division 2007).* Other states also allow punitive damages where a defendants unintentional conduct amounts to a conscious disregard of the rights of others, and do not require a showing of actual malice. *See e.g.* California: *Silberg v. California Life Insurance Company, 11 Cal. 3d 452 (1974);* Florida: Fla. Statutes Section 768.72(2) (2005); Illinois: *Cirrincione v. Johnson, 184 Ill.2d 109, 115*--116, *703 N.E.2d 67, 70 (1998);* Missouri: *Hoovers Dairy, Inc. v. Mid-America Dairyment, Inc./Special Products, Inc., 700 S.W.2d 426 at 435 (Mo. 1985);* Pennsylvania, *Feld v. Merriam, 506 Pa. 383 at 395, 485 A.2d 749 at 758 (Pa. Super. 1998);* Texas: Tex. Civ. Prac. & Rem. Code Ann. Section 41.003.

Emerging Data Management Obligations. The growing crime of identity theft has raised pressure on businesses to protect the personal data entrusted to them. (*See* United State Federal Trade Commissions Identity Theft Protection website: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html) Nearly every business that deals with individual consumers or that handles employee health benefits is legally required to safeguard that data and not to misuse it. United States federal law protects data relating to an individuals health care (Health Information Portability and Accountability Act of 1996, Pub. L. No. 104-191, *110 Stat. 1936* (Codified at *42 U.S.C. § 1320d* (2000)), personally identifiable financial data (Gramm-Leach-Bliley Act, *15 U.S.C. § 6801--6809*), and data identifying children (Childrens Online Privacy Protection Act, *15 U.S.C.A. § 6501 et seq.*). In addition, at this writing, at least 39 states have passed data management laws obligating businesses to treat consumer data in a certain manner and/or to notify consumers upon security breach affecting personal data. *See* LEXIS 50 State Comparative Legislation/Regulations: Non-Customer Personal Data Security, Breach & Notification (October 2007). While the defendant in the *Randi A.J.* case was bound by the New York health care regulations (specifically N.Y. Public Health Law section 2803-c[1], [3][f]) to protect its patients personal information, the personal data privacy rules that bind other businesses could also be used to justify imposition of large damage awards upon even an inadvertent lapse in data protection, just as the *Randi A.J.* court did.

When retailer TJX Corporation lost personally identifiable data for more than 46 million customers, it was subjected to a rain of litigation from consumers and financial companies based on TJXs contractual and statutory obligations to protect such data. *See* Financial industry lawsuits consolidated to *In re TJX Companies Retail Security*

Breach Litigation, D. Mass., No. 1:07-cv-10162-WGY, *class certification denied* 11/29/07. The specific obligations of data protection the Payment Card Industry Data Security Standards imposed on retailers by contract from their merchant banks have begun to be adopted into law (*See* Minn. Stat. 325E.64, effective August 1, 2008). Practitioners should be aware that the increasing number of laws and regulations requiring businesses to protect data can serve as the basis for compensatory or statutory damages, and in some cases punitive damages or administrative penalties (*See e.g.* various consent orders with United State Federal Trade Commission resulting from data security breaches with many types of companies, including retailers such as DSW Inc. and BJs Wholesale Club, data processors and aggregators like ChoicePoint and CardSystems Solutions, and others: http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html).

Also note that statutory violation is not always necessary to establish a breach of privacy case. In *Santiesteban v. Goodyear Tire & Rubber Company, 306 F.2d 9 (C.A. Fla. 1962),* the court recognized that, under Florida law, invasion of right of privacy is a distinct common law tort, that punitive damages are allowable in right of privacy actions, and malice is not a required element for the tort.

Conclusion. Attorneys representing data-holding business, from retailers to banks to medical providers, must note that failure to follow the basic information protection guidelines may subject the business to significant compensatory and punitive damages. This is true even if the breach of privacy at the basis of a consumer claim arises from accident or mistake. Businesses must demonstrate that they have taken their privacy obligations seriously by developing and following reasonable policies for dealing with protected data, limiting access to protected data, and appropriately training employees to handle the data. Otherwise the costs of a data breach may be enormous.

For a more detailed analysis of the elements needed to prove punitive damages, *see* John Kircher and Christine Wiseman, *Punitive Damages: Law and Practice, Second Edition*, Loose Leaf, West Group 2000 with updates; Morton D. Daller, *Tort Law Desk Reference: A Fifty State Compendium*, Aspen Publishers 2006.

For additional information on data management law, *see* 1 David Bender, Computer Law, Chapter 2A Data Protection (LexisNexis Matthew Bender); Andrew Serwin, Information Security and Privacy: A Practical Guide to Federal, State and International Law, (Thomson West 2006); John P. Hutchins and Anne P. Caiola, U.S. Data Breach Notification Law: State by State, American Bar Association, Section of Science and Technology Law 2007.

ABOUT THE AUTHOR(S):

Ted Claypoole is a Member of Womble Carlyle Sandridge and Rice in its Technology Transaction Team, concentrating his practice on internet and data management legal issues. Claypoole has served as corporate counsel for CompuServe, Inc. and as assistant general counsel at Bank of America, concentrating on the banks technology, ecommerce, data security and intellectual property. A 1985 honors graduate of Duke University and 1988 graduate of the Ohio State University College of Law, he regularly writes and speaks on the intersection between the law and information technology, including co-presenting The Ethics of Pervasive Biometrics at the 2007 RSA conference, and moderating a panel on Data Integrity at the 2007 ABA Business Law Spring Meeting. Claypoole has served on a U.S. Justice Department Computer Crimes Task Force and the Information Protection Committee for the Banking Industry Technology Secretariat.

13 of 18 DOCUMENTS

Bensen on BondPro Corp. v. Siemens Power Generation, Inc.

2008 Emerging Issues 1869

Bensen on BondPro Corp. v. Siemens Power Generation, Inc., 463 F.3d 702 (7th Cir. 2006)

By Eric E. Bensen

February 6, 2008

SUMMARY: Use Title Below instead of Online Display Name for the ADF/Case Link:Eric E. Bensen on the Seventh Circuits Holding that a Trade Secret Owner Failed to Prove Secrecy: *BondPro Corp. v. Siemens Power Generation, Inc., 463 F.3d 702 (7th Cir. 2006).*In BondPro Corp., the Seventh Circuit considered whether a defendant, which allegedly filed a patent application on the plaintiffs trade secret process after that process was disclosed to it in license negotiations with the plaintiff, was properly awarded summary judgment on the grounds that the plaintiff had failed to show that the trade secret was in fact secret. The court held that the grant of summary judgment was proper. Eric E. Bensen is a co-author of Milgrim on Licensing and Milgrim on Trade Secrets, the author of a number of articles on intellectual property issues, and an attorney with Paul, Hastings, Janofsky & Walker LLP in New York, where he focuses his practice on intellectual property litigation and licensing.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: In *BondPro Corp. v. Siemens Power Generation, Inc., 463 F.3d 702 (7th Cir. 2006)*, the Seventh Circuit considered whether a defendant, which allegedly filed a patent application on the plaintiffs trade secret process after that process was disclosed to it in license negotiations with the plaintiff, was properly awarded summary judgment on the grounds that the plaintiff had failed to show that the trade secret was in fact secret. The court held that the grant of summary judgment was proper.

Summary of the Case

In 2001, Scott Wang, founder of BondPro, a small company that manufactures products requiring the bonding of dissimilar materials, explained and demonstrated BondPros process for manufacturing slot cells for electrical generators to Siemens Power Generation (Siemens), a manufacturer of electrical generators. He hoped, of course, to lay the groundwork for a licensing arrangement with Siemens. Instead, he laid the groundwork for a litigation that would not end well for his company.

A slot cell is a U-shaped piece of insulation that forms the outer layer of copper coils inserted into the rotors of an electrical generator. Siemens manufactured its slot cells by placing insulation material into a U-shaped container (a

female mold) and then pressing a male mold on top of it and applying heat. The process resembled placing the material in a bowl and then pressing a slightly smaller bowl into the first bowl to compress the material. Siemens process, however, had a shortcoming, sometimes leaving wrinkles in the insulation material that were difficult to smooth out.

In BondPros process, which BondPro did not use commercially, the insulation material was placed over the male mold and compressed against the mold using air pressure and heat. Any wrinkles resulting from this process could be smoothed by hand.

The 2001 negotiations resulted in a confidentiality agreement, but not much else, at least not for BondPro. Rather than seeking a license from BondPro as BondPro had hoped, Siemens filed a patent application for a process similar to BondPros process. The application eventually published, but was rejected. Siemens later claimed that the bare bones version of BondPros process disclosed in the patent was no secret because it was described in advertising materials it received from Torr Technologies in 2000. (Whether Siemens failure to identify that advertising to the Patent & Trademark Office as prior art constituted inequitable conduct was apparently not an issue addressed in the litigation.)

BondPro sued Siemens for trade secret misappropriation and won a jury verdict on liability in the first part of a bifurcated trial. Before the damage phase of the proceeding commenced, however, court granted judgment to Siemens as a matter of law on the grounds that, in view of Torr Technologies advertising materials, no reasonable jury could conclude that the process was not generally known or reasonably ascertainable in the industry.

BondPro appealed to the Seventh Circuit.

Pertinent Legal Principles

The Secrecy Required for Trade Secret Protection. Needless to say, a trade secret must be secret to be entitled to protection, but there are a number of important considerations to keep in mind when evaluating the secrecy element of a trade secret claim. First, secrecy is an issue of fact. Thus, the issue of secrecy does not normally lend itself well to resolution by summary judgment, although summary judgment can be appropriate, for example, where the defendant presents evidence that the purported trade secret had been publicly disclosed and the plaintiff offers no evidence in rebuttal. Second, while reverse engineering to discover a trade secret is lawful, the mere fact that a trade secret is susceptible of being discovered through reverse engineering does not necessarily destroy secrecy. Third, even where public disclosure destroys a trade secret, it does not necessarily destroy a claim for trade secret misappropriation because a defendant cannot use its own disclosure of a trade secret as a defense to a claim for misappropriation.

For a discussion of the secrecy requirements for trade secret protection, see 1 Roger M. Milgrim & Eric E. Bensen, *Milgrim on Trade Secrets § 1.03* (2007).

Other Requirements for Trade Secret Protection. While secrecy is a requirement for trade secret status, it is not sufficient by itself to establish the existence of a protectable trade secret. To be a trade secret, the information must also afford its owner a competitive advantage from not being generally known and be subject to reasonable efforts to maintain its secrecy. These requirements are expressly provided for in the Uniform Trade Secret Act (the UTSA), now in force in 45 states, which defines a trade secret as information that (i) derives independent economic value from not being generally known to, and not readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use and (ii) is the subject of efforts reasonable under the circumstances to maintain its secrecy. UTSA § 1.

For a discussion of the UTSA, see 1 *Milgrim on Trade Secrets § 1.01*[3].

Trade Secrets & Patent Applications. Information eligible for trade secret protection may also be eligible for patent protection. There is, however, a fundamental trade-off between the two forms of protection. A trade secret exists

for so long as its owner exercises reasonable safeguards to protect its secrecy or until the subject matter becomes generally known, and thus, is potentially perpetual, but does not protect against independent discovery or reverse engineering. A patent, on the other hand, gives the patent holder the right to exclude others from practicing the patented invention, and thus, protects against even innocent infringement, but is in force for only limited time.

The choice as to which protection to pursue can be a complex one. A trade secret in commercial use for more than a year before a patent application is filed on it may be, by reason of such use, ineligible for patent protection. On the other hand, a trade secret fully disclosed in a published patent application or issued patent will, prospectively, be destroyed. In other words, where an invention potentially qualifies for either trade secret protection, because it meets the definition above, or patent protection, because it is also novel, has utility and is not obvious, its inventor has to choose one or the other form of protection. It and cannot have both, at least not for the same subject matter.

Historically, the inherent difficulty of this choice was somewhat eased because patent applications were kept confidential by the Patent and Trademark Office until the patent issued. That confidentiality protected the status of any trade secrets disclosed in the application, allowing the applicant to maintain those trade secrets in the event a patent did not issue. Under current U.S. law, however, patent applications are published 18 months from the applications filing. A concerned applicant can choose not to have its application published, and thereby maintain the traditional protection for trade secrets disclosed in its application, but would have to forgo using its application as a basis for foreign patent filings.

Were the proposed Patent Reform Act of 2007 enacted, the decision whether to apply for a patent would, in the patent/trade secret context, become yet more difficult. The Act would require that *all* patent applications be published after 18 months. Although an applicant could avoid publication by withdrawing the application before 18 months have passed, the applicant may not have a better sense at that time of the likelihood that a patent will issue than it did when it filed. Thus, by the time the applicant realizes the patent may not issue, the trade secret may already be lost under the automatic publication rule.

For a discussion of the relationship between patent and trade secret protection, *see* 1, 2 *Milgrim on Trade Secrets § 1.06* (effect of patents and patent applications on secrecy) and Chapter 8 (trade secrets as patentable matter).

The Seventh Circuits Decision

Addressing the issue of secrecy, the Seventh Circuit observed that the mere mention of a trade secret in a public document is not determinative of whether the trade secret has become public knowledge because trade secret status is an issue of fact and no one may have noticed the documents. Publication in a patent, however, was not in the courts view one of those circumstances because a patent is *intended* to be widely disclosed. Similarly, the disclosure of a trade secret in a published patent application will ordinarily destroy the secret, although the court stopped short of concluding that such would always be the case. The court recognized that a rejected patent application was less likely to contain information useful to other inventors and was thus less likely to result in destruction of the trade secret. However, it declined to rule that rejection necessarily saves the trade secret because patent examiners are not infallible and therefore, an application, though rejected, may contain information sought by others in the industry.

There was no need for the court to dwell on whether disclosure of BondPros process destroyed any secrecy, however, because BondPro conceded that it had. BondPros claim was based on the unlawful disclosure of the process by Siemens.

The question for the court was whether the process was, at the time of BondPros disclosures to Siemens, in fact a trade secret. To answer that question, the court examined the contours of BondPros claimed trade secret. If the purported secret were the manufacture of rotor coil insulation by applying heat and air pressure to insulation materials draped around a male mold, it was not secret at all because that much had been disclosed to Siemens in advertising

materials provided by Torr Technologies. If BondPro had a secret, the court reasoned, it would therefore have to be in the details of the process. BondPro, however, alleged no such details. Accordingly, the Seventh Circuit concluded that BondPro had failed to establish that it had a protectable secret and affirmed the lower courts decision.

Comment

Although not necessary to its holding, the court in *BondPro* offered a cogent rationale for the often stated, but rarely explained, requirement that the trade secret owners make efforts reasonable under the circumstances to protect the secrecy of their trade secrets. In the courts view, that requirement is justified by the three factors stated here.

1. The failure to take such steps is persuasive evidence that the trade secret has no value.

2. Courts are entitled to preserve their scarce resources by refusing to help trade secret owners who have failed to take steps to help themselves.

3. A trade secret owners efforts to protect secrecy put others on notice that the protected information may be a trade secret.

The *BondPro* decision contains a number of other statements of trade secret law, which, although largely *in dicta*, make it well worth the read.

ABOUT THE AUTHOR(S):

Eric E. Bensen is a co-author of Milgrim on Licensing and Milgrim on Trade Secrets, the author of a number of articles on intellectual property issues, and an attorney with Paul, Hastings, Janofsky & Walker LLP in New York, where he focuses his practice on intellectual property litigation and licensing.

14 of 18 DOCUMENTS

Bensen on Mortgage Specialists, Inc. v. Davey, 904 A.2d 652 (N.H. 2006).

2008 Emerging Issues 1759

Bensen on Mortgage Specialists, Inc. v. Davey, 904 A.2d 652 (N.H. 2006).

By Eric E. Bensen

January 8, 2008

SUMMARY: Use Title Below instead of Online Display Name for the ADF/Case Link:Eric E. Bensen on the New Hampshire Supreme Courts holding that the Uniform Trade Secret Act Preempts all Tort Claims Arising Solely from the Misappropriation of Information: *Mortgage Specialists, Inc. v. Davey, 904 A.2d 652 (N.H. 2006).*In Mortgage Specialists, addressing an issue that has divided courts, the New Hampshire Supreme Court held that claims arising solely from the misappropriation of information are preempted by the Uniform Trade Secret Act (the UTSA), even where the information does not qualify as a trade secret. Eric E. Bensen is a co-author of Milgrim on Licensing and Milgrim on Trade Secrets, the author of a number of articles on intellectual property issues, and an attorney with Paul, Hastings, Janofsky & Walker LLP in New York, where he focuses his practice on intellectual property litigation and licensing.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: In *Mortgage Specialists, Inc. v. Davey, 904 A.2d 652 (N.H. 2006)*, addressing an issue that has divided courts, the New Hampshire Supreme Court held that claims arising solely from the misappropriation of information are preempted by the Uniform Trade Secret Act (the UTSA), even where the information does not qualify as a trade secret.

Summary of the Case

When Joseph Davey and Steven Carbone left Mortgage Specialists, Inc., a mortgage broker and lending company, they took with them copies of information for individual customers that they used in their work, including, each customers current interest rates from which a competitor could learn whether refinancing would have appeal to the customer. Both Davey and Carbone then opened their own mortgage business closing loans for customers that they had worked with at Mortgage Specialists. Mortgage Specialists filed suit bringing claims for trade secret misappropriation, conversion, tortious interference with advantageous relations, violation of state consumer protection law and breach of fiduciary duty.

Defendants moved to dismiss all but the trade secret claim on the ground that the other claims were preempted by the New Hampshire UTSA, RSA 350-B:7. The trial court dismissed those claims on the grounds that because they were

not supported by facts other than the misappropriation of trade secrets, they were preempted by UTSA. In response to Mortgage Specialists argument that such a ruling was premature because it had not yet been determined whether the information at issue constituted trade secrets, the court ruled that the UTSA preemption provision displaces claims that rely on the misappropriation of trade secrets regardless of whether the claimant establishes that the subject information is entitled to trade secret status.

Mortgage Specialists appealed.

Pertinent Legal Issues

UTSA Definition of a Trade Secret. UTSA defines a trade secret as information that (i) derives independent economic value from not being generally known to, and not readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use and (ii) is the subject of efforts reasonable under the circumstances to maintain its secrecy. UTSA § 1.

Uniform Application of UTSA. UTSA provides that it shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this Act among states enacting it." Accordingly, decisions under UTSA by the courts of one state can generally be cited as authority in the courts of another. UTSA § 8.

For a discussion of UTSA, see Roger M. Milgrim & Eric E. Bensen, *Milgrim on Trade Secrets §§ 1.01*[2], [3] (2007).

UTSAs Preemption of Common Law Claims. The UTSA preemption provision, which provides that UTSA displaces conflicting tort, restitutionary, and other law of th[e] State pertaining to civil liability for misappropriation of a trade secret, UTSA § 7, may be the *least* uniformly applied provision of UTSA. To understand how the preemption provision has been treated by courts, it will be helpful to first divide the universe of tort claims that can give rise to a preemption question into three categories.

1. Those based solely on the misappropriation of information meeting the definition of a trade secret.

2. Those based solely on the misappropriation of information that does not meet the definition of a trade secret.

3. Those based on misappropriation of information (whether or not it meets the definition of a trade secret) *plus* other tort factors, such as breach of fiduciary duty or fraud.

As to the first category, there is little doubt that the UTSA was intended to supplant at least common law claims for trade secret misappropriation. While not as universally accepted, the weight of authority is that claims in the third category, that is, those concerning the misappropriation of information that requires a showing of facts beyond those required support a trade secret claim, such as fraud, breach of fiduciary duty and tortious interference, are not preempted.

It is the claims falling into the second category that provide the most difficulty. One could look at the plain language of the UTSA preemption provision, which expressly applies to trade secrets, and reasonably conclude that claims for misappropriation of non trade secret information are not preempted. However, that construction would appear to be at odds with the uniformity that UTSA was intended to provide.

On the other hand, one could look to the Commissioners Comment to UTSA Section 7, which states that UTSA applies to protect competitively significant information, and reasonably conclude that in the interests of uniformity, UTSA is intended to preempt claims for the misappropriation of information regardless of whether the information

warrants trade secret protection. However, given the infinite variety of circumstances in which the misappropriation of information can cause harm, such a broad reading of the preemption provision may lead to a denial of relief in circumstances where such denial would be plainly unjust. Perhaps it is no surprise that courts have struggled with this issue.

There is no indication yet that courts are moving towards a uniform approach to preemption where claims based solely on the misappropriation of non trade secret information are at issue. Thus, notwithstanding UTSAs intended uniformity, preemption remains an issue that has to be looked at on a jurisdiction by jurisdiction basis.

For a discussion of the UTSA preemption provision, see *Milgrim on Trade Secrets §§ 1.01*[3][a].

The New Hampshire Supreme Courts Decision

On appeal, Mortgage Specialists went to the heart of the matter arguing that UTSAs preemption provision is contingent on the misappropriated information qualifying as a trade secret and, alternatively, that its other claims should not have been dismissed because they were not based solely on the alleged misappropriation of confidential information. Defendants argued that UTSA preempts all remedies and theories of recovery where liability is based on the misappropriation of confidential information, including trade secrets.

UTSA Preempts Claims Based on the Misappropriation of Information. The court acknowledged that Mortgage Specialists narrow construction of the preemption provision in New Hampshires version of UTSA (NHUTSA) appeared to be supported by the text of the provision, which explicitly preempts remedies for misappropriation of trade secrets. However, because of NHUTSAs provision that it be construed in a manner consistent with that given to other states UTSAs, RSA 350- B:8, the court began its analysis with a review of the purpose of UTSA and the treatment the preemption provision has been given by other courts.

In examining the purpose of UTSA, the court found what it considered to be support for the proposition that UTSA was meant to create a uniform law concerning the misappropriation of not just bona fide trade secrets, but all commercially valuable information. Among other things, the court observed that prior to the enactment of UTSA, the Patent Section of the American Bar Association began considering the need for "enactment of a uniform state law to protect against the wrongful disclosure or wrongful appropriation of trade secrets, know-how or other information maintained in confidence by another." The court also cited to cases from Kentucky, Connecticut, Illinois, Michigan and, interestingly, from an appellate court decision from Wisconsin (although that states supreme court had reached the opposite conclusion), for the proposition that UTSA was intended to preempt common law causes of action for the misappropriation of information even where the information did not rise to the level of a trade secret.

The court considered the cases cited by Mortgage Specialists for the proposition that common law claims are not preempted where the information misappropriated does not meet the definition of a trade secret, but rejected that view on two grounds. First, in the courts judgment, the weight of authority was against that view. Second, the court concluded, that approach would undermine the uniformity that UTSA was intended to achieve.

The court concluded that at least with respect to common law claims, UTSA creates a system were information is either a protected trade secret or unprotected general knowledge. The court noted the apparent harshness of the rule, but observed that parties may continue to protect commercial information contractually regardless of whether such information meets the statutory definition of a trade secret.

For a discussion of the protection of confidential information by contract, see *Milgrim on Trade Secrets § 4.01* et seq. (2007).

UTSA Only Preempts Claims Based Solely on Misappropriation. The courts holding, however, did not resolve

the appeal. Again noting some conflict among the courts, the court addressed the issue of whether UTSA preempts all common law claims that concern trade secrets, or merely those based solely on the misappropriation of trade secrets. Following the majority view, the court held that UTSA does not preempt claims that require some allegation or factual showing in addition to those necessary to establish a trade secret claim. Accordingly, Mortgage Specialists conversion claim and breach of fiduciary duty claim, at least as alleged, which were both based solely upon the defendants misappropriation of trade secrets, were preempted. However, its tortious interference with advantageous relations, which was supported by allegations that defendants intentionally contacted Mortgage Specialists customers to get their business, and its state law unfair competition claim, which was supported by an allegation that defendants falsely informed Mortgage Specialists customers that Mortgage Specialists was not licensed in the state, were not preempted. With respect to those claims, the lower courts opinion was vacated.

Comments

Mortgage Specialists provides a good example of the broader approach taken by some courts to preemption under UTSA. For another analysis of the competing approaches to the preemption in which a court came to the *opposite* conclusion as that reached by the New Hampshire Supreme Court, see *Cenveo Corp. v. Slater, No. 06-CV-2632, 2007 U.S. Dist. LEXIS 9966, *12-13 (E.D. Pa. Feb. 12, 2007)* (concluding that the Pennsylvania UTSA did not preempt tort claims for theft of information that does not qualify as a trade secret and, accordingly, denying a motion to dismiss a claim for conversion of confidential pricing and quality control information on preemption grounds). For an example of the less common approach of preempting a claim supported by allegations that would support a claim for trade secret misappropriation even though claim requires allegations beyond those necessary for trade secret misappropriation, see *Atco Mfg. Co. v. Share Corp., No. 3:07-cv-028, 2007 U.S. Dist. LEXIS 37503, *7-8 (E.D. Tenn. May 22, 2007)* (claims for unfair competition and tortious interference with business relations based on the use of misappropriated trade secret information preempted by the Tennessee UTSA).

ABOUT THE AUTHOR(S):

Eric E. Bensen is a co-author of Milgrim on Licensing and Milgrim on Trade Secrets, the author of a number of articles on intellectual property issues, and an attorney with Paul, Hastings, Janofsky & Walker LLP in New York, where he focuses his practice on intellectual property litigation and licensing.

15 of 18 DOCUMENTS

Claypoole on Internet Jurisdiction: HighMaintenanceBitch v. Uptown Dog Club

2008 Emerging Issues 1569

Claypoole on Internet Jurisdiction: HighMaintenanceBitch v. Uptown Dog Club

By Ted Claypoole

December 17, 2007

SUMMARY: Use Title Below instead of Online Display Name for the ADF/Case Link:Ted Claypoole on the High Cost of Failing to Leash an Internet Store with Personal Jurisdiction: HighMaintenanceBitch, LLC v. Uptown Dog Club, Inc., slip op., *2007 U.S. Dist. LEXIS 82456 (W. Dist. Washington 2007).*Establishing personal jurisdiction over an out-of-state internet retailer can be complicated for plaintiffs counsel. The U.S. District Court in the Western District of Washington demonstrated that failure to understand these rules or to plead correctly can be costly. This commentary, written by internet specialist Ted Claypoole, analyzes the lessons of this District Courts HighMaintenceBitch, LLC decision on trying to establish jurisdiction over an opponent based on its broad internet presence.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Establishing personal jurisdiction over an out-of-state internet retailer can be complicated for plaintiffs counsel. The U.S. District Court in the Western District of Washington demonstrated that failure to understand these rules or to plead correctly can be costly. This commentary, written by internet specialist Ted Claypoole, analyzes the lessons of this District Courts HighMaintenceBitch, LLC decision on trying to establish jurisdiction over an opponent based on its broad internet presence.

Analysis. Over the past decade American courts instituted and then redefined the nature of establishing personal jurisdiction from an internet accessible presence. Practitioners must carefully apply these rules, remembering to plead properly, or risk not only dismissal of their claims, but also payment of the defendants costs and attorneys fees.

Summary of the Case. The Plaintiff, HighMaintenanceBitch, LLC. (HMB), holds three patents on certain types of accessory products for dogs, and claimed that Defendant Uptown Dog Club, Inc. (Uptown Dog Club) offered products in its online store that infringed on the HMB patents. HMB sued Uptown Dog Club in the Western District of Washington, claiming that the Texas-based defendant was subject to the courts jurisdiction because Uptown Dog Club sold products nationwide from its online store. This claim and the subsequently discovered sales figures were not enough to secure the Washington courts jurisdiction over Uptown Dog Club.

This case illustrates three important practical considerations when trying to establish jurisdiction over an internet retailer: 1) a defendants single sale or very limited sales in the district is unlikely to support jurisdiction; 2) alleging that the Defendants website allows purchasers to ship into the relevant district may not be enough to support even a request

for jurisdictional discovery, and 3) inadequate jurisdictional pleading can lead a court to rule your case frivolous and to award attorney fees to the Defendant.

Asserting Jurisdiction based on Internet Contacts. The party asserting jurisdiction has the burden of proving it. *WNS, Inc. v. Farrow, 884 F.2d 200, 203 (5th Cir. 1989).* That party succeeds if it proved that the defendant is bound by general jurisdiction or specific jurisdiction. General jurisdiction is satisfied if the defendant has maintained continuous and systematic contacts with the forum state even when the cause of action has no relation to those contacts. *HMB*, citing *LSI Industries v. Hubbell Lighting, Inc., 232 F.3d 1369, 1375 (Fed. Cir. 2000).* But the mere operation of a website alone does not satisfy this test, and the *HMB* court held that such a website plus a single provable sale within the state did not satisfy the test. *Citing GTE New Media Services, Inc. v. BellSouth Corp., 199 F.3d 1343, 1349*--1350 (D.C. Cir. 2000).

However, even if a partys general contacts with the state are too isolated or sporadic to support general jurisdiction, where the factual basis for the complaint arises out of or relates to the forum state and creates a substantial connection to the forum state, then the court may apply specific jurisdiction. *See, Asahi Metal Industrial Company v. Superior Court, 480 U.S. 102, 112*--13 (1987). The test for specific jurisdiction as defined in *HollyAnne Corporation v. TFT, Inc., 199 F.3d 1304, 1307*--08, is that a defendant must purposefully direct its activities at the residents of the forum state, that the claim arises out of those activities, and that the assertion of personal jurisdiction is reasonable and fair. The HMB court ruled that, when applying specific jurisdiction to a retailer, sales in the forum state must be more than isolated occurrences (*see Burger King v. Rudzewicz, 471 U.S. 462, 475*--76 (1986)), and a defendants interactive website accessible in the forum state is not enough to satisfy specific jurisdiction (*see Millennium Enterprises, Inc. v. Millennium Music, L.P., 33 F.Supp. 2d 907, 921 (D. Or. 1999)*). Because plaintiff HMB could show no more connection to the forum state than Uptown Dog Clubs widely accessible website and a single proven sale of an offending product in the forum state, the court refused to find specific jurisdiction.

Practitioners attempting to haul an opponent into court a thousand miles from its headquarters must carefully research, plead and support their jurisdictional assertions. For example, HMB never claimed precisely which products sold by Uptown Dog Club infringed the HMB patents, and HMB only asserted that one boa-feathered dog collar had shipped to the forum state. HMB was also coy when asked by Updown Dog Club to be more specific about its claims, implying that further specificity could limit HMBs damages or harm its negotiating position. The court noted those tactics and did not look favorably on them, finding the complaint to be frivolous.

Jurisdictional Discovery. Practitioners wishing to bring a national web retailer to trial in a distant jurisdiction should be prepared to prove the amount of the defendant retailers sales within the intended forum state. Proof of sales may not be available without jurisdictional discovery. Otherwise, a plaintiff does not have the legal mechanism to force a defendant to provide the sales figures needed in establishing jurisdiction.

The HMB court would not allow jurisdictional discovery based on unsupported allegations of the defendants potential contacts to the forum state. The court made clear that more research must be performed by the plaintiff to tie the defendant to a distant jurisdiction, and the court pointedly cited a case allowing jurisdictional discovery where affidavits showed compelling evidence of the defendants forum contacts, including customers, vendors and employee travel to the forum jurisdiction. A litigant basing jurisdiction on unsupported allegations that the defendant transacted business in the forum runs the significant risk of seeing its jurisdictional assertion labeled clearly frivolous (*see Massachusetts School of Law at Andover, Inc. v. American Bar Association, 107 F.3d 1026, 1042 (3rd Cir. 1997)*).

Conclusion: The High Cost of Poor Jurisdictional Pleading. The HMB case serves as a warning for litigators who are careless in pleading jurisdiction. Plaintiff HMBs assertions that defendants commercial website was accessible in the forum state, without further attempts to tie the defendants business either defendants internet sales or the underlying supplier and employee relationships to the forum, led to a ruling that the plaintiffs claim was frivolous, which kept the court from permitting jurisdictional discovery and led to an award of defendants attorney fees to be paid by plaintiff. To avoid this result, plaintiffs counsel should conduct significant research into defendants ties with the

forum, as well as filing a verified complaint with jurisdictional affidavits demonstrating the fullest discoverable extent of those ties. In the alternative, if plaintiffs counsel cannot find enough verifiable ties to support remote jurisdiction, then counsel should not overreach, opting instead to file the lawsuit in the defendants forum.

For a detailed analysis of current rules for asserting jurisdiction over company based on its internet presence, *see A Survey of Personal Jurisdiction based on Internet Activity: A Return to Tradition*, by TiTi Nguyen, *19 Berkeley Tech. L.J. 519 (2004); Caveat E-Emptor: Solutions to the Jurisdictional Problem of Internet Injury*, by John J. Schulz, Jr., *29 Am. J. Trial Advoc. 615*, (2005-2006); and *You Cant always Use the* Zippo *Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction*, by Dennis T. Yokoyama, *54 DePaul L. Rev. 1147* (2004-2005).

For discussion of various complexities affecting internet-based jurisdiction, *see* the several notes in Northwestern University Law Reviews Symposium on Personal Jurisdiction in the Internet Age, *98 Nw. U.L. Rev. 409-544* (2003-2004).

ABOUT THE AUTHOR(S):

Ted Claypoole is a Member of Womble Carlyle Sandridge and Rice in its Technology Transaction Team, concentrating his practice on internet and data management legal issues. Claypoole has served as corporate counsel for CompuServe, Inc. and as assistant general counsel at Bank of America, concentrating on the banks technology, ecommerce, data security and intellectual property. A 1985 honors graduate of Duke University and 1988 graduate of the Ohio State University College of Law, he regularly writes and speaks on the intersection between the law and information technology, including co-presenting The Ethics of Pervasive Biometrics at the 2007 RSA conference, and moderating a panel on Data Integrity at the 2007 ABA Business Law Spring Meeting. Claypoole has served on a U.S. Justice Department Computer Crimes Task Force and the Information Protection Committee for the Banking Industry Technology Secretariat.

16 of 18 DOCUMENTS

David Bender on the Conflict Between U.S. Discovery and EU Privacy

2008 Emerging Issues 1452

David Bender on the Conflict Between U.S. Discovery and EU Privacy

By David Bender

December 12, 2007

SUMMARY: This Emerging Issues Analysis, discusses the conflict between US discovery and EU Privacy and answers such important questions such as: What is the source of the various obligations? What are the different component parts of the problem? What is the crux of the conflict? What has been the result in other conflicts between EU privacy law and US law? What distinguishes this from those previous conflicts? What light is shed by precedents?

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: The extensive range of discovery in U.S. litigation and investigations has increasingly come into conflict with EU data protection laws designed to protect human rights. The U.S. laws are meant to give litigants a basis for proving their claims (or disproving their adversarys). The EU laws are meant to protect individuals from abuse of their personal data. Although several other areas of conflict between the EU data protection laws and U.S. law have been resolved, this conflict seems particularly difficult to settle, probably because in this conflict there is no governmental entity that is directly involved. Given that both types of laws include severe sanctions for non-compliance, companies subject to U.S. discovery demands for personal data located in the EU may find themselves in a difficult predicament. An increasing number of companies are finding themselves in such a position. Although several previous conflicts between the EU data protection laws and U.S. law have been resolved, no resolution of this problem appears to be on the horizon. It appears that there will be no resolution until some government intervention takes place.

Introduction. One of the areas where the EU data protection laws have come into conflict with U.S. law concerns the document discovery and retention requirements associated with litigation in U.S. federal or state courts, with federal and state agency investigations, and with audits that may be required by U.S. federal or state law. The scope of evidence that may be subject to discovery in U.S. litigation in particular is quite extensive more so than in any other country, and far more extensive than in most other countries. But if U.S. discovery law is the irresistible force, then EU data protection law, which imposes strict limitations on whether and how personal data may be processed, is the immovable object.

U.S. Discovery. [For information regarding U.S. discovery, see generally 4 D. Bender, Computer Law Chap. 9 (LexisNexis Matthew Bender)] *Rule 26(b)(1) of the Federal Rules of Civil Procedure* permits a litigant to request any information that is not privileged and is relevant to the claim or defense of any party. Relevant evidence includes evidence that is admissible, or is reasonably calculated to lead to the discovery of admissible evidence. In this regard,

U.S. law imposes two types of requirements. First, with regard (generally) to ongoing litigation the Federal Rules of Civil Procedure, and the state counterparts of those rules, impose on litigants and third parties broad obligations to produce evidence in the form of documents or electronically stored information, n1 testimony, n2 and written answers to written questions. n3 As a practical matter, it has generally been in connection with document production, governed by *Rule 34, Fed. R. Civ. Pro.* and its state analogues, that U.S. law has come into conflict with the EU data protection laws. In addition to the obligation to produce evidence, U.S. law imposes an obligation to preserve evidence that is relevant to ongoing litigation, or is relevant to litigation that does not yet exist but whose existence is reasonably foreseeable. [For a discussion of this obligation, see 4 D. Bender, Computer Law § 9.05[1] (LexisNexis Matthew Bender)] Failure to adhere to these obligations of production or preservation can lead to sanctions, including adverse jury instructions, preclusion of issues from trial, dismissal of claims, tort claims, contempt citations, fines, and imprisonment. Nor are these sanctions limited to litigants, as third parties may also be sanctioned.

Who is Subject to Discovery? The obligation to produce documents applies to documents that are within the possession, custody or control n4 of the party from whom the documents are sought. So long as that test is met, the location of the documents is irrelevant. With multinationals increasingly linking their offices through computer networks, documents used by one office may well be located in a server resident in another office (and another country). Discovery may be sought from any person, natural or legal, that is subject to the jurisdiction of the court where the action is pending or (in the case of a third party) from which the subpoena issued. A company that is doing business in the venue will generally be subject to the jurisdiction of the court, and often a somewhat lower standard will suffice for jurisdiction to attach. Thus, a company incorporated in and based in the U.S. may be required under U.S. law to produce its documents located in the EU. And a company incorporated in and based in the EU that does business in the U.S. or is otherwise subject to jurisdiction in the U.S., may be required under U.S. law to produce its documents located in the EU. Often the discovery can be thought of as comprising three phases. First, the discovering party wishes to collect (and perhaps analyze) the documents in the EU, and may wish also to disclose them to others in the EU. It also wishes to transfer the documents to the U.S. And finally, it wishes to study those documents in the U.S., perhaps disclose them to others in the U.S., and perhaps use them in depositions or at trial in the U.S.

EU Data Protection Law. The actual data protection law that will apply to a particular situation will be the national data protection law, which differs from member state to member state, sometimes quite significantly. Aside from differences among the statutes, there are even larger differences among the interpretations and attitudes of the 27 data protection authorities. (DPAs) created for the purpose of implementing and enforcing the data protection laws. In order to introduce an element of commonality, the discussion that follows is based on the EU Data Protection Directive (the Directive), n5 rather than any national law enacted in implementation of the Directive.

The Restrictions. The Directive places severe restrictions on the processing of personal data within its scope. [For an extensive discussion of the restrictions imposed by the Directive, see 1 D. Bender, Computer Law §§ 2A.02, 2A.03 (LexisNexis Matthew Bender)] The Directives scope extends to processing wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. The Directive defines processing quite broadly. n6 In particular, the collection of documents within the Directives scope in the EU will constitute processing, as would analysis or disclosure to others in the EU. And so will the transfer of those documents to the U.S. (which generally would be effected electronically). And likewise, with regard to any consultation or disclosure in the U.S. or use in a hearing or trial. Thus, for documents within the scope, compliance with EU law will require a basis under EU law for (1) the collection, (2) disclosure and (3) analysis in the EU, a basis for (4) the transfer to the U.S., and a basis for (5) the analysis, (6) disclosure, and (7) use in the U.S. n7 Thus, the matter of discovering documents located in the EU is by no means solely a transfer problem. In fact, finding a basis for the transfer may be the least difficult of the seven tasks.

Permissible Bases for Processing. The initial task for which a basis in law must be found is that of collecting the documents. As specified in Article 7 of the Directive, that basis may be unambiguous consent n8 or may be one of

several necessities. n9 The problem with using any of the necessities is the narrow view of necessity that many DPAs have taken. In the case of discovery, the first necessity (performance of a contract with the data subject) is unlikely to apply. The second necessity (necessary for compliance with a legal obligation to which the controller is subject) is also unlikely to be deemed applicable unless the documents have been requested through a procedure established under a treaty, for the EU view is that legal obligation means one imposed by EU, member state, or international law. Accordingly, an obligation under U.S. law does not suffice. n10 The third necessity (necessary to protect the vital interests of the data subject) is unlikely to apply; in fact, discovery of the documents sometimes would be antithetical to those interests. The fourth necessity (necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed) runs into the problem that official authority is interpreted not to include U.S. official authority. The discovery situation may well qualify under the first segment of the fifth necessity (necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)), but the EU view of fundamental rights and freedoms is so expansive that the controllers or the third partys rights will likely be deemed overridden.

And as if the requirements of EU data protection law did not themselves provide sufficient impediment to the litigant in its quest for evidence residing in the EU, in many nations (i) employment law will provide additional impediments, and (ii) works councils n11 will add yet another layer of difficulty.

The Conflict. Accordingly, it may be quite difficult to comply with both U.S. and EU law with regard to collecting documents subject to a valid U.S. litigation or investigative request, and located in the EU. A rather similar analysis may be made for the other enumerated tasks, n12 except task (4) transfer. Transfer of personal data out of the EU (or, more accurately the European Economic Area n13) is subject specifically to its own set of controls, set forth in Articles 25 (which permits transfer to a nation offering an adequate level of protection) and Article 26 of the Directive. While not identical to the necessities of Article 7, the necessities of Article 26(1) are generally similar to the Article 7 necessities, and no more helpful to the U.S. litigant. n14 However, Article 26(2) and Article 26(4) are more promising. Under the first of these, a member state may authorize a transfer to an inadequate nation where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals . Pursuant to this provision, the EU and the U.S. agreed to the Safe Harbor Principles, under which many U.S. companies today, in accordance with EU law, receive personal data from the EU. And Article 26(4) provides that the EU may approve certain standard contractual clauses that offer sufficient safeguards; if the EU approves such clauses, the member states must recognize them as adequate. And indeed, the EU has approved three alternative sets of standard contractual clauses. Thus, export from the EU of the documents sought may be in compliance with EU law if transferred to a U.S. recipient that has certified to the Safe Harbor Principles, or if done pursuant to a set of contractual clauses approved by the EU and executed by the EU exporter and the U.S. importer. But these mechanisms legitimize only the transfer. What goes on in the EU prior to the transfer, and what transpires in the U.S. after the transfer, must find their own justifications in EU law.

Precedent. The author knows of but one U.S. case pitting U.S. discovery rules against EU data protection law. In *Volkswagen, AG v. Valdez,* n15 a products liability case, the Texas Supreme Court considered plaintiffs request for the German defendants (VWAG) current corporate phone book. Plaintiff contended that this document might identify individuals with relevant information concerning alleged defects in the vehicle in question, a 1970 Volkswagen. n16 VWAG contended that production would violate German data protection law, n17 a contention it supported with affidavits from experts and German officials. The court opined that when information sought in U.S. discovery is located outside the U.S., a court should rely on the precepts set forth in section 442 of the Restatement *(Third) of Foreign Relations Law*. Noting that under the Restatement, a U.S. court may order such production, the court adopted the five considerations set out in the Restatement for use in balancing the interests of the domestic court or agency against those of the foreign sovereign: (1) the importance to the investigation/litigation of the documents or information; (2) the degree of specificity of the request; (3) whether the information or document originated in the U.S.; (4) the

availability of alternative means for securing it; and (5) the extent to which noncompliance would undermine important U.S. interests, or compliance would undermine important foreign interests.

It was uncontested that the request was quite specific, and that the book originated in Germany. The court noted that alternatives were available, as VWAG had produced its 1969 phone book n18 and its U.S. subsidiary had produced its current phone book. A VWAG engineer who was with the company in 1969 had identified some 29 persons knowledgeable in the design of the 1970 VW. He also supplied much information about VWAGs organizational structure and identified the single person who did most of the design and development work in door latches (an item of specific interest). The court concluded that, not only did plaintiff have alternative means, but the information in the current phone book had little importance to the litigation. The court held that Germanys interests would be undermined by disclosure (because German law would then be violated), whereas there was no suggestion that failure to produce would undermine any important U.S. interest (especially given the alternative means available). Finding that the trial court abused its discretion, the court granted defendants petition for a writ of mandamus and directed the trial court to vacate its order compelling production.

Document Retention. Likewise, data retention is complicated by conflicting requirements on the two sides of the Atlantic. In the U.S., destruction of documents pertinent to ongoing litigation or to matters where litigation is reasonably likely constitutes spoliation and is punishable. In the EU the rule is that personal data may be retained only for so long as is necessary for the purpose for which it was collected. n19 Retaining data for a period longer than so necessary violates EU law, even if necessary for U.S. litigation.

Two Distinguishing Features. One aspect of this genre of dispute that differentiates it from the three high-profile U.S./EU cross-border transfer disputes that preceded it (and have been resolved at least of sorts) is nature of the parties. In each of the three earlier matters the actor on one side who interacted directly with the actor on the other side was a governmental entity. n20 And in each of those three instances, the involved governmental entity found a way to interact with a governmental entity on the other side, and the two governments resolved the matter. But the nature of the parties is different in the instant situation, which exists in two varieties one involving private party litigation, and the other involving a governmental document demand. In the former variety, the private party demanding discovery is pitted against the private party from whom discovery is sought. And in the latter, the non-governmental party to the dispute is the recipient of the demand, an entity in the U.S., so that there is no EU actor directly involved. The presence of a governmental direct protagonist on one side facilitated attracting governmental attention on the other side, thus easing the way for resolution.

Another characteristic in which the present dispute differs from its three predecessors is that the present dispute is much more splintered. The discovery disputes are proliferating and they are manifold. Every time a U.S. discovery demand is made for documents located in the EU, another instance occurs. But there was only a single PNR dispute, only a single SWIFT dispute, and only a very small number of SOX disputes. The limited number of disputes in the three earlier matters may have rendered it less difficult to resolve them.

Practice Tips

. Before you commence litigation, include in your considerations the issue of whether documents containing necessary personal data may be located in the EU.

. If so, ask yourself whether there is an alternative way to get the important information contained in those documents.

. If the only way to obtain critical information is by demanding documents in the EU, give serious thought to

whether the action should be commenced.

. If you receive a demand for documents located in the EU, become familiar with the restrictions imposed by the data protection laws of the pertinent nation(s), lest you run afoul of them.

. Consider having job applicants for EU positions give consent for the processing (including without limitation transfer) of documents containing personal data in response to litigation demands, keeping in mind that the propriety and enforceability of such consents will differ from country to country, and that in some countries consents may be withdrawn at any time.

Return to Text

n1 . *See F. R. Civ. P., Rule 34(a)*.

n2

[2]. *See F. R. Civ. P., Rule 30*.

n3

[3]. *See F. R. Civ. P., Rule 33*.

n4

[4]. *See F. R. Civ. P., Rule 34(a)*.

n5

[5]. 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, OJ L 281, p. 31 (23 Nov. 1995). [This Directive is reproduced in 1 D. Bender, Computer Law App. 2A[1].]

n6

[6]. Pursuant to Article 2 of the Directive, processing means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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.

n7

[7]. Depending on exactly what is to be done with the data, other steps might also be involved, and a legal basis for each of them would also be necessary.

n8

[8]. Whether consent may serve as a basis where the data subject is an employee differs from member state to member state, and also on the facts of the situation. Some DPAs take the position that is not possible for an employer to obtain freely given consent from its employee because of the leverage inherent in the employment relationship. In this regard, it may be better to obtain consent from job applicants than from employees. Consent must be unambiguous, and in at least some member states it must be freely given and may be withdrawn at any time without prejudice.

n9

[9]. I.e., where (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).

n10

[10]. See, e.g., Art. 29 Data Prot. Working Party, WP 117, Opin. 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fights Against Bribery, Banking and Finl Crime, 00195/06EN (1 Feb. 2006).

n11

[11]. A works council within a company is a group, consisting of employee representatives, that is empowered in some EU nations with veto rights over certain types of management decisions.

n12

[12]. For certain types of documents, e.g., employee e-mails, the impediments to processing are even greater than for most other types of documents. *See, e.g.,* Societe Nikon France. v. Onof, Cass. Soc., 2 Oct. 2001, Bull Civ. V, No. 291, where a French court held that an employer that explicitly stated that employees were not to use their company computers for personal use nevertheless had no right to monitor employee e-mail. Cases in other nations have reached results consistent with this.

n13

[13]. The EEA consists of the EU member states along with Iceland, Liechtenstein, and Norway.

n14

[14]. Nor does the public register exception of Article 26(1)(f) provide assistance, as in general the data sought in discovery will not so qualify.

n15

[15]. *Volkswagen, AG v. Valdez, 909 SW.2d 900 (Tex. 1995).*

n16

[16]. The book contained names, job titles, position, and direct dial numbers of some 20,000 employees, and home numbers of managers.

n17

[17]. The German Federal Data Protection Act (Bundesdatenschutzgesetz). This case was decided in the same year as the EU released the Directive. However, some EU member states, such as Germany, had data protection laws that predated the Directive.

n18

[18]. Data in the 1969 phone book was old enough not to be governed by the German law.

n19

[19]. Directive Article 6(1)(e) provides: Member States shall provide that personal data must be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

n20

[20]. These were the disputes involving PNR airline data (where the U.S. Bureau of Customs and Border Protection was one of the protagonists), the Sarbanes-Oxley Act (where several DPAs were protagonists), and SWIFT wire transfer messaging (in which the U.S. Department of Justice was a protagonist). [An extensive discussion of the PNR and SWIFT matters will be found in 1 D. Bender, Computer Law § 2A.02 (LexisNexis Matthew Bender). An extensive discussion of the SOX matter will be found in 1 D. Bender, Computer Law § 2A.03[8] (LexisNexis Matthew Bender)]

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

David Bender is Senior Privacy Counsel at DLA Piper in New York City, with extensive experience in information technology, privacy, and intellectual property matters involving litigation, counseling, and transactional work. He came to DLA Piper from White & Case, where he headed the privacy practice, which he helped found. Before practicing in the privacy area, Mr. Bender advised on various types of information technology transactional and counseling matters. A founder of White & Cases IP practice, he handled many IP matters, ranging from patent, copyright, and trade secret litigation to due diligence inquiries and the negotiation and drafting of various types of IP-related agreements. Mr. Bender served in-house at AT&T (mostly before its divestiture), and for five years was the General Attorney responsible for all IP litigation brought by or against any Bell System company. Prior to that, he litigated antitrust cases in a law firm. He is a past president of the International Technology Law Association (ITechLaw, previously called Computer Law Association CLA). Mr. Bender has made over 250 presentations on topics in the fields described above across the nation and in some 16 foreign countries at conferences sponsored by numerous organizations. He has also authored many law review articles and conference handbook proceedings. Before turning to the law, Mr. Bender served as an Engineer with Ford Aerospace, and as a mathematician with Hughes Aircraft.

David Bender on the Definition of "Personal Data"

2008 Emerging Issues 1068

David Bender on the Definition of "Personal Data"

By David Bender

November 20, 2007

SUMMARY: A paper recently released by the EU sheds light on one of the most central concepts attendant to data protection the notion of just what exactly constitutes "personal data," which is the type of information protected by this genre of law. The paper, promulgated by the Article 29 Working Party, adopts a broad view of the term. This Emerging Issues Analysis discusses some of the important observations set out in that paper.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Introduction. The notion of what constitutes personal data is a most important concept that goes right to the heart of the purpose and operation of the European Union Data Protection Directive 95/46/EC. Lack of common agreement on this point across the EU has not gone unnoticed by the Article 29 Working Party (the group comprising the directors of the 27 EU member state data protection authorities). The Directive defines personal data as any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In mid-2007, after conducting a survey across the member states to determine the various rules in effect, the Article 29 Working Party adopted a guidance document, WP136. Art. 29 Data Prot. Working Party, WP136, Opinion 4/2007 on the concept of personal data, 01248/07/EN (adopted 20 June 2007). In WP136 the Article 29 Working Party concluded that some member states were using a definition that was too narrow. Working on a common definition of the notion of personal data is tantamount to defining what falls inside or outside the scope of the data protection rules. WP136 focused on four elements in the definition of the term: applicability to any information; extension to information relating to; focus on identified or identifiable information; and relationship to information of a natural person.

Any Information. The Article 29 Working Party began by returning to the definition of personal data in the Directive any information relating to an identified or identifiable natural person , and interpreted this to indicate that a broad definition was intended. This may include any sort of statement about a person, both objective and subjective. It includes information touching the individuals private or family life, and also information regarding activity the individual undertook. The form of the information is irrelevant, as the term includes information in alphabetical, numerical, graphical, photographical, or acoustic form, by way of example. If not electronic, it must be in, or intended for inclusion in, a structured database. But if electronic, such as e-mail, free text may qualify. Example 2 given in WP136 states that in telephone banking the recorded instructions in the customers voice are personal data. Example 3

states that images of individuals captured by video surveillance are personal data to the extent recognizable. Example 4 states that a drawing of a childs family made by the child as a result of a neuro-psychiatric test on her in the context of court custody proceedings, is personal data, as indicative of her mood and how she felt about family members. Biometric properties that are both unique to the individual and measurable are personal data. Examples are fingerprints, retinal patterns, facial structure, voices, hand geometry, vein patterns, and deeply engrained skill or other behavioral characteristics (e.g., handwritten signature, keystrokes, particular manner of walking or talking). Human tissue is not personal data, but is a source of personal data (e.g., a blood sample).

Relating To. Information relates to an individual when it is about him or her. Example 5 informs that the value of a particular house is information about an object, but in some situations will constitute personal data of the owner, such as when it is a basis for determining the owners taxes. Example 6 deals with service records of a car maintained by a mechanic, and that contain data about mileage, dates of service, technical problems, and material condition. If these are all associated with a vehicle registration number and an engine number, which can be linked to the owner, they may constitute personal data. If the garage establishes the link to the owner, e.g., for billing, that data will relate to the owner. And if there is a means of connecting it to the mechanic, it will relate to the mechanic. data relates to an individual if it refers to the identity, characteristics or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated. The notion of relate requires an element of either content, purpose, or result. A content element is present where information is given about a particular person, regardless of purpose or impact. A purpose element exists when data is used or likely to be used to evaluate, treat, or influence behavior. The result element exists when the use of data is likely to impact an individuals interests such that he or she may be treated differently from others as a result of the processing of the data. The three elements are alternative to each other. Example 8 deals with a satellite system that determines in real-time the location of taxis. The purpose is to save fuel and provide better service. Even though it relates directly to vehicles, it permits monitoring of drivers as to speeds, itineraries, etc., and therefore relates to them.

Identified or Identifiable. A person can be identified directly by name, or indirectly by phone number, SSN, car registration number, etc., or by a combination of significant criteria that permits narrowing down the group to which he or she belongs (e.g., age, occupation). Whether an individual is identified depends on the circumstances. It may even be necessary to combine name with other pieces of information to identify a person. Indirect identification results from unique combinations of identifiers. Example 10 speaks to information published about a renowned criminal case completed years ago. In a present publication about the case, no identifiers are given. Nevertheless, it is not difficult to obtain identities from old newspapers. This information would be considered to be about identifiable persons and as such, personal data. Nor is identification by name always necessary. When other identifiers (such as one assigned by a computer) are used to single out individuals, that may suffice. Example 11 deals with asylum seekers hiding their names, and given a code number. If a photo or other biometric data are connected to the number, the person is an identified person.

On the issue of means to identify, account should be taken of all means likely reasonably to be used to identify the person. Mere hypothetical possibility to identify a person is insufficient, but the determination should take account of the possibility of technological progress that may render it possible in the future to make an identification.

Pseudonymization is the practice of disguising identities. This is especially prevalent in research and statistical situations. It can be done retraceably (with two-way cryptography) or non-retraceably (with one-way cryptography). Its effectiveness depends on a number of factors. Retraceably pseudonymized data is data on individuals who are indirectly identifiable. Key-coded data, one example of pseudonymization, uses a code for each individual, with a separately kept key noting the correspondence between the code and the common identifiers of the individual (e.g., name, data of birth). Example 17 describes a situation where an institute processes personal information to generate statistics but, at early stages, data is not aggregated and relates to specific individuals designated with a key code. The correspondence list is separately maintained. This key would be considered reasonably likely to be used by the institute for statistics, and therefore the set of individual-related information is personal data in the hands of the institute. After the coded list is released, another assessment must be made as to whether it is personal data. This would involve considering the

likelihood that someone at the institute would furnish the key, the risks of hacking, etc.

WP136 also discusses FAQ 14 (7) of the Safe Harbor FAQs, which deals with key-coded data in pharmaceutical research, where the key code is held only by the researcher, and not communicated to the sponsoring pharma company. The issue addressed in that FAQ is whether a transfer of that data from the EU to the US constitutes a transfer of personal data subject to the Safe Harbor Principles. The FAQ answers in the negative, and WP136 states that that is not inconsistent with the reasoning in WP136 so long as the transfer is to a US recipient who will never know the identity of the patients.

Anonymous data is data that relates to a natural person who cannot be identified by anyone, taking into account means likely reasonably to be used to identify the individual. Example 18 deals with statistical surveys done by statisticians forbidden to publish non-anonymous data. In each situation a threshold must be determined, below which identification is possible. Example 19 discusses a surveillance camera installed in a store that publishes the pictures of thieves caught by means of the system. After police intervention the shopkeeper blanks out the thieves faces. Nevertheless, the persons photographed may still be recognized by acquaintances.

Natural Person. The definition of personal data is not limited by means of nationality or residence. However, the term applies only to living individuals. Nevertheless, the data of deceased persons will sometimes indirectly be protected. An example occurs where the controller is unable to discern whether a data subject is dead. Or even if that can be determined, if the system for processing the data of deceased individuals is the same as that for processing the data of living individuals, then the data of deceased individuals will be treated the same as that of living individuals. Another example occurs where the data on a deceased individual refers to personal data of a living individual, such as the fact that an identified woman suffered from hemophilia, which indicates that her (living) son must also suffer from it. WP136 notes that nothing prevents a member state from enacting national legislation that goes beyond the provisions of the Directive, so long as no other element of EU law precludes that. Judgment of the European Court of Justice C-101/2001 of 06/11/2003 (Lindqvist), § 98.

Another issue is whether the term includes an unborn child. WP136 states that this should be determined by referring to the position national law generally takes on the rights of an unborn child.

And yet another issue is posed by legal persons (who are not covered by the Directive). WP136 notes that certain data protection rules may nevertheless apply indirectly to data relating to a business or a legal person. Directive 2002/58/EC, which complements the Directive, provides for the protection of the legitimate interests of subscribers who are legal persons. Also, information about legal persons may relate to natural persons, e.g., where the name of the legal person derives from a natural persons name. Corporate e-mail normally used by a particular employee, and data regarding a small business that may describe its owners behavior, may also qualify. Again WP136 notes that nothing prevents a member state from enacting legislation that goes beyond what is required in the Directive, so long as no other element of EU law would preclude that. And WP136 notes that Austria, Italy and Luxembourg have extended certain provisions of their laws so that they apply to the processing of data on legal persons. And again, the arrangements of the data processor may result in data about legal persons de facto receiving the same treatment as data relating to individuals.

WP136 also addresses the issue of what result should obtain for data that falls outside the definition. First, as noted above, the fact that data falls outside the Directive does not necessarily mean it will be outside a given member states implementing legislation. And even if it is, other law may apply to it.

Conclusion. The discussion and examples set forth in WP136 shed significant light on what the Article 29 Working Party (and probably most of the data protection authorities) views as included in the term personal data. Nevertheless, there is still much uncertainty attached to the term, and it will likely require more data protection authority activity and pronouncements to clarify the definition further.

For an in-depth discussion of the EU Data Protection Directive, and its interpretation, *see* 1 D. Bender *Computer Law* §§ 2A.02, 2A.03 (LexisNexis Matthew Bender).

Practice Tips

. A close reading of WP136 is a worthwhile endeavor for any who will be required to make decisions about whether certain categories of information constitute personal data.

. Given the broad, inclusive interpretations taken by the Article 29 Working Party in WP136, in situations where it is difficult to determine whether information constitutes personal data, a conservative course of action would generally be preferred.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

David Bender is Senior Privacy Counsel at DLA Piper in New York City, with extensive experience in information technology, privacy, and intellectual property matters involving litigation, counseling, and transactional work. He came to DLA Piper from White & Case, where he headed the privacy practice, which he helped found. Before practicing in the privacy area, Mr. Bender advised on various types of information technology transactional and counseling matters. A founder of White & Case's IP practice, he handled many IP matters, ranging from patent, copyright, and trade secret litigation to due diligence inquiries and the negotiation and drafting of various types of IP-related agreements. Mr. Bender served in-house at AT&T (mostly before its divestiture), and for five years was the General Attorney responsible for all IP litigation brought by or against any Bell System company. Prior to that, he litigated antitrust cases in a law firm. He is a past president of the International Technology Law Association (ITechLaw, previously called Computer Law Association CLA). Mr. Bender has made over 250 presentations on topics in the fields described above across the nation and in some 16 foreign countries at conferences sponsored by numerous organizations. He is the author of Computer Law (LexisNexis Matthew Bender). Mr. Bender has also authored many law review articles and conference handbook proceedings. Before turning to the law, Mr. Bender served as an Engineer with Ford Aerospace, and as a mathematician with Hughes Aircraft.

18 of 18 DOCUMENTS

David Bender on the Enforceability of Modifications to Browse-wrap Licenses

2008 Emerging Issues 1039

David Bender on the Enforceability of Modifications to Browse-wrap Licenses

By David Bender

November 16, 2007

SUMMARY: According to recent cases, users are not obligated to check for changes to the terms of use each time they go online. If users are not given reasonable notice of changes, they are not bound by those changes. This Emerging Issues Analysis, written by David Bender, author of Computer Law, discusses these cases and the resulting rule.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: The Problem. One nagging question regarding browse-wrap agreements has been to determine exactly what is required in order to modify them. Just what obligations should be thrust on users of online services with regard to keeping track of the contractual provisions to which they are subject? Should they be required to read the entire browse-wrap each time they log on, maintain a copy of it, and make a comparison? Two recent cases shed some much-needed light on this issue.

The Ninth Circuit Speaks. In *Douglas v. Talk America, 495 F.3d 1062 (9th Cir. 2007),* the only notice of the modified browse-wrap terms that a service provider gave its subscribers was to post the four changes on its website. The changes related to additional charges, a class action waiver, an arbitration clause, and a choice of New York law. After becoming aware of the changes, plaintiff subscriber brought a putative class action in a California federal court charging breach of contract and other causes. The district court granted defendants motion to compel arbitration. Plaintiff sought a writ of mandamus, a *sine qua non* for which is a showing that the lower courts order was clearly erroneous. The Ninth Circuit held that the lower courts order was indeed clearly erroneous.

Plaintiff could have learned of the modification only by visiting defendants website. But he claimed he had no occasion to do so, as he paid his bills automatically by credit card. And even had he visited the site, he would have had no reason to look at the contract posted there. Parties to a contract have no obligation to check the terms on a periodic basis to learn whether they have been changed by the other side. *Id. at 1066.* Nor would a party know *when* to check without being notified that the contract has been changed and how. Douglas would have had to check the contract every day for possible changes. Without notice, an examination would be fairly cumbersome, as Douglas would have had to compare every word of the posted contract with his existing contract in order to detect whether it had changed. Id., note 1 (emphasis by the court).

A party cannot unilaterally change the terms of a contract. Even if continued use of a service after such a posting

could be considered assent, that assent could be inferred only if the user received valid notice. Plaintiff claimed such notice was never given. In the cases relied on by the district court the subscriber received notice of the modified contract by mail. And a California case had held that a revised contract containing an arbitration clause is unenforceable against existing customers even when they are given notice by mail. The Ninth Circuit concluded that the district court erred in binding plaintiff to the revised contract when he had not been notified of the changes.

Further, the court stated that the new terms were probably not enforceable in the forum (California) for conflict with that states fundamental policy regarding unconscionable contracts (which requires both procedural and substantive unconscionability). Although the district court found procedural unconscionability because plaintiff had meaningful alternatives, the appellate court noted that after the district court decision, California law was modified. Accordingly, procedural unconscionability may now exist where a service provider with overwhelming bargaining power offers a take it or leave it contract, even if the customer has a meaningful alternative. Also, a class action waiver may be unconscionable under California law under certain circumstances. Thus, the Ninth Circuit held that the district court erred in enforcing the modified contract.

A District Court Chimes In. While not squarely on point, *Southwest Airlines Co. v. Boardfirst*, L.L.C. (Civ. No. 3:06-cv-0891-B opin. 12 Sept. 2007) held that a set of modified browse-wrap terms of use constituted an enforceable contract. Southwest issued passengers on each flight, on a first come, first served basis, a boarding designation of A, B, or C, which controlled the order of boarding. Passengers could check in over the Southwest website up to 24 hours before scheduled departure. For a $5 fee, Boardfirst offered to check the passenger in online, attempting to secure an A designation. The Southwest website terms of use stated: Unless you are an approved Southwest travel agent, you may use Southwest web sites and any Company information only for personal, non-commercial purposes. The terms were later modified to state explicitly that checking customers in online and obtaining a boarding pass was a commercial purpose. After sending Boardfirst two cease-and-desist letters, Southwest sued for breach of contract and other causes. The court considered Southwests motion for partial summary judgment.

Again, the critical issue was whether there was a valid contract. The court noted that to manifest tacit assent to a contract through conduct, one must engage in the conduct and understand or have reason to understand that the other party may infer assent from that conduct. The home page stated that use constituted acceptance of the terms. Southwest contended that the websites terms of use bound Boardfirst to a contract once the latter commenced use with knowledge of the terms. If not before, Boardfirst had knowledge of the terms on receipt of the first cease-and-desist letter. Acceptance of a browse-wrap license requires no signature or click, and its validity vel non depends on whether the user had actual or constructive knowledge of the terms.

The court looked to two Second Circuit cases to make this distinction. In *Specht v. Netscape Communications, 306 F.3d 17 (2d Cir. 2002)*, the user had to scroll down beyond the first screen to reach the terms. When a user sued, Netscape sought to invoke the arbitration provision in the terms. The Second Circuit held that, because notice of the license was not reasonably conspicuous to the average user, plaintiffs were not on notice (even constructively) of the existence of the license and therefore not bound by it. By way of contrast, that same court, in *Register.com v. Verio, 356 F.3d 393 (2d Cir. 2004)*, bound users who clearly had notice of the terms posted on the site. Verios argument that it learned of the terms only after it had received the information it sought from the site was undercut by the fact that Verio submitted queries on a daily basis. Thus, the *Boardfirst* court juxtaposed these two Second Circuit results: clear notice before use resulted in assent, but where there was no notice, there was no assent and no contract.

The court concluded that the instant case resembled *Verio* more than *Specht*. There was no dispute that Boardfirst had actual knowledge of Southwests terms. In short order, the court found that Boardfirsts use was commercial, and therefore breached the terms.

Conclusion. These two cases suggest the distinction that will be followed on the issue of whether a user will be bound to browse-wrap modifications posted by website operators. A user who does not have reason to view the suggested modification, or does not recognize it as such, is unlikely to be held to it.

For an extensive discussion of the enforceability generally of wrap agreements (i.e., shrink-wrap agreements, click-wrap agreements, and browse-wrap agreements), *see* 3 D. Bender, *Computer Law*, § 4A.02[4] (LexisNexis Matthew Bender).

Practice Tips

o *Dont hide proposed modifications*. To modify terms of use for your browse-wrap, set out the modifications so that, to use the site, users must (1) see the modified terms, and (2) recognize them as modifications. Absent a good case on each of these points, a court will likely hold that there was no user assent to the modified terms through continued use, even if the terms state that continued use is deemed to be consent. For click-wraps, it is useful to identify modifications clearly and conspicuously near the I agree button, and to require the user to acknowledge (by pushing a button) that he or she has read the modifications and agrees to them.

o *Avoid terms that violate public policy*. Where you include a choice of law and/or choice of forum, you can often identify provisions and situations that violate the public policy in the one or two jurisdictions identified, and that therefore are unenforceable, even with user assent. If the law of a pertinent jurisdiction will not, for example, permit enforcement of adhesion contracts, or of an arbitration clause in certain circumstances, think long and hard before inserting such a provision, whether in the original agreement, or a modification.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

David Bender, the author of Computer Law, is Senior Privacy Counsel at DLA Piper in New York City, with extensive experience in information technology, privacy, and intellectual property matters involving litigation, counseling, and transactional work. He came to DLA Piper from White & Case, where he headed the privacy practice, which he helped found. Before practicing in the privacy area, Mr. Bender advised on various types of information technology transactional and counseling matters. A founder of White & Case's IP practice, he handled many IP matters, ranging from patent, copyright, and trade secret litigation to due diligence inquiries and the negotiation and drafting of various types of IP-related agreements. Mr. Bender served in-house at AT&T (mostly before its divestiture), and for five years was the General Attorney responsible for all IP litigation brought by or against any Bell System company. Prior to that, he litigated antitrust cases in a law firm. He is a past president of the International Technology Law Association (ITechLaw, previously called Computer Law Association CLA). Mr. Bender has made over 250 presentations on topics in the fields described above across the nation and in some 16 foreign countries at conferences sponsored by numerous organizations. He has also authored many law review articles and conference handbook proceedings. Before turning to the law, Mr. Bender served as an Engineer with Ford Aerospace, and as a mathematician with Hughes Aircraft.