St. Mary's Law Journal

Volume 39 | Number 4

Article 3

1-1-2008

Loose Lips Sink Attorney-Client Ships: Unintended Technological Disclosure of Confidential Communications Essay.

Bill Piatt

Paula deWitte

ESSAY

LOOSE LIPS SINK ATTORNEY-CLIENT SHIPS: UNINTENDED TECHNOLOGICAL DISCLOSURE OF CONFIDENTIAL COMMUNICATIONS

BILL PIATT[*]
PAULA DEWITTE[**]

[*] Ryan Professor of Law and former Dean (1998–2007), St. Mary's University School of Law. I am indebted to my legal secretary and former coordinator, Grace M. Garcia, and to my research assistant, Rebecca Covarrubias, for their assistance. I wish to thank Vincent Johnson, Professor of Law and former Associate Dean, St. Mary's University School of Law, for sharing his research and insights with me.

[**] Paula deWitte is a candidate for J.D., St. Mary's University School of Law, May 2009. Ms. deWitte holds a B.S. in Mathematics from Purdue University, a M.S. in Education from Purdue University, and a Ph.D. in Computer Science from Texas A&M University.

I. INTRODUCTION

In general, attorneys must not reveal confidential information relating to the representation of their clients.[1] Moreover, attorneys must make reasonable efforts to ensure that the attorneys they supervise, as well as their nonlawyer employees, maintain client confidences.[2] In a bygone era, attorney-client communications consisted of face-to-face meetings (which might have included notes of the discussion) and exchanges of written letters.[3] Today, however, technology virtually guarantees that attorneys and clients will communicate electronically and that these electronic communications will be memorialized, copied, archived, and perhaps accessed by others with whom the attorneys

[1] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2007) ("A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [Rule 1.6(b)]."); *cf. id.* 1.6(b) (permitting lawyers to reveal confidential client information if they reasonably believe it is necessary to prevent "certain death or substantial bodily harm," or other certain crimes and fraudulent activities committed by the client in which the lawyer's services have been used).

[2] *See id.* 5.1 (providing that supervising attorneys must "make reasonable efforts to ensure [subordinate attorneys] conform to the Rules of Professional Conduct"); *id.* 5.3 (detailing that supervising attorneys must ensure that the nonlawyer assistant's "conduct is compatible with the professional obligations of the lawyer").

[3] *See* Jesse J. Richardson, Jr., *How a Sole Practitioner Uses the "Electronic Office" to Maintain a Competitive Law Practice*, 3 DRAKE J. AGRIC. L. 141, 147 (1998) (highlighting that in the past lawyers relied on telephone and mail service rather than electronic communications); Ronald W. Staudt, *Does the Grandmother Come with It?: Teaching and Practicing Law in the 21st Century*, 44 CASE W. RES. L. REV. 499, 520 (1994) ("Electronic mail supplants some communications that previously occurred by visit, telephone, and memoranda."); *see also* Robert H. Thornburg, *Electronic Discovery in Florida*, 80 FLA. B.J. 34, 34 (2006) ("Today, over 90 percent of a company's documents are created electronically, but never printed. The filing cabinets of yesteryear have gone by the wayside and have been replaced by desktops and laptops.").

did not intend to share the information.[4] While most attorneys would not knowingly betray client confidences, there is a growing problem of unintended disclosure through technological means, including those both nefarious and accidental.[5] Many attorneys are probably unaware of the magnitude of these risks.[6] How does an attorney gather and utilize the information necessary to represent the client effectively, and at the same time, maintain procedures that prevent the unintended disclosure that could ruin the client's case and subject the attorney to discipline or malpractice claims? Many technology and security protections that are available are not yet widely used in the legal profession.[7] Awareness of the problems and possible solutions are critical first steps to addressing these concerns.

In this essay, we examine why the law recognizes attorney-client confidentiality, what possibilities exist for unintended disclosure through technology, and how attorneys can adapt to these new realities in order to fulfill obligations of effective representation and maintenance of client trust and confidences. We will also discuss a tripartite approach to information security that an attorney can employ to better protect client information.

[4] *See* Debra Cassens Weiss, *Did Lawyer's E-Mail Goof Land $1B Settlement on NYT's Front Page?*, ABA Journal, Feb. 6, 2008, http://www.abajournal.com/news/lawyers_e_mail_goof_lands_on_nyts_front_page/ (illustrating one example of an unintended technological disclosure to a third party: misaddressed e-mail); *see also* SECTION OF SCI. & TECH. LAW, LAW PRACTICE MGMT. SECTION, INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS 167–68 (Sharon D. Nelson et al. eds., 2006) (providing methods to keep a secure message archive).

[5] *See generally* SECTION OF SCI. & TECH. LAW, LAW PRACTICE MGMT. SECTION, INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS 13–23 (Sharon D. Nelson et al. eds., 2006) (highlighting different means in which a lack of information security can lead to accidental disclosure, such as unauthorized access to computer networks through inadequate password protection and failure to maintain operational firewalls, leading to spyware or full compromise of computers).

[6] *See id.* at 35–36 ("Lawyers tend to have less experience and focus less attention upon the stealthy information security risk that arises from their increasing use of information technology as a legal practice tool.").

[7] *See id.* at 48–50 (explaining that there are currently no standards set by the ABA for a minimum amount of information security, but that the adoption of such standards would provide considerable guidance to lawyers who need to respond to the increasing threat).

II. WHY RECOGNIZE ATTORNEY-CLIENT CONFIDENTIALITY?

A. *The Nature of Confidentiality*

Human beings have a basic need to form relationships based upon trust.[8] One element of trust is the mutual willingness of those involved in a trust relationship to keep within the group. Perhaps an early example involved tribal members keeping secrets within the tribe as to the location of food stores or supplies.[9] Similarly, the safety of a group would be compromised if information regarding defense systems was spread to hostile outsiders.[10]

On an emotional level, we seek to find someone with whom we can share our innermost thoughts, ambitions, concerns, and fantasies with the expectation that these shared matters of intense personal concern will not be broadcast to others. Consider, for example, the lyrics composed by Paul McCartney and John Lennon: "Do you want to know a secret, [d]o you promise not to tell?"[11] A negative response to the second of these inquiries would end the hope of a relationship held by the person making the inquiry. The first of these inquiries points to perhaps another

[8] *See* J. David Lewis & Andrew Weigert, *Trust As a Social Reality*, 63 SOC. FORCES 967, 968 (1985) (stating that "trust may be thought of as a functional prerequisite" to form other types of societal relationships).

[9] Few records exist of early tribal decisions to secrete food stores, but plainly the ability to gather food and keep its location secure would have increased the chances for group survival among early humans. As one example, dotted throughout modern Israel are archaeological sites which include hidden, underground access routes to water wells. *See* AMIHAI MAZAR, ARCHAEOLOGY OF THE LAND OF THE BIBLE 10,000-586 B.C.E. 478–85 (1990) (describing underground water systems in ancient Israeli cities designed to limit access to the city's inhabitants).

[10] Hiding weapons stores seems to be another obvious method to ensure group survival. Searching out these secret caches is an important undertaking when another group seeks to minimize their threat. *See* Terry Frieden, *Feds Find Weapons Cache Near Mexican Border*, CNN.COM, Feb. 4, 2006, http://www.cnn.com/2006/US/02/03/laredo.arsenal/index.html (discussing the capture by federal authorities of an arsenal of illegal weapons belonging to Mexican drug trafficking groups); *Major Weapons Cache Seized in Iraq*, MILITARY.COM, Feb. 26, 2007, http://www.military.com/NewsContent/0,13319,126519,00.html (reporting the seizure of a large cache of weapons used to create roadside bombs in Iraq); *Weapons Cache Found in Afghanistan*, BBC NEWS, Apr. 18, 2003, http://news.bbc.co.uk/2/hi/south_asia/2959261.stm (describing the efforts of coalition forces to locate weapons caches in Afghanistan and in the process discovering the largest weapons cache in Afghanistan).

[11] THE BEATLES, DO YOU WANT TO KNOW A SECRET? (Parlophone 1963), *available at* http://www.dmbeatles.com/song.php?song=56.

basic human interest: people seem to want to know secrets, although, as discussed below, learning and maintaining a secret may create significant burdens for the person who must keep that secret.[12]

The law recognizes this deep-seated human need to create and maintain confidential relationships for reasons of physical and emotional well-being. For example, communications with health care providers[13] and clergy[14] are afforded evidentiary privileges and privacy protection. Spouses enjoy the legal right to communicate in most regards without being subjected to forced disclosure of the discussion.[15] Educational records are protected by federal law.[16] In addition, a host of privacy laws and precedent afford a remedy against prying eyes, ears, and hands.[17]

[12] *See* Anita E. Kelly et al., *What Is It About Revealing Secrets that Is Beneficial?*, 27 PERSONALITY & SOC. PSYCHOL. BULL. 651, 651 (2001) (reporting that people who do not reveal negative secrets "are more depressed, anxious, and shy and have lower self-esteem and higher levels of general symptomatology" (citations omitted)).

[13] *See* TEX. R. EVID. 509 (defining the Texas physician-patient privilege); FED. R. EVID. 501 (stating that federal privilege shall be governed by common law and applicable state laws); *see also* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 264(a), 110 Stat. 1936, 2033 (1996) (requiring the Secretary of Health and Human Services to promulgate rules determining privacy standards for patient health records). The final HIPAA rule promulgated by the Secretary became effective April 14, 2003 and created a substantial list of privacy requirements to protect patient information. 45 C.F.R. §§ 164.500–.534 (2007).

[14] *See In re* Grand Jury Investigation, 918 F.2d 374, 384 (3d Cir. 1990) (recognizing the clergy-communicant privilege as long as the communication was conducted in confidence with a clergyperson acting in an official capacity).

[15] *See* Blau v. United States, 340 U.S. 332, 333 (1951) ("[C]onfidential communication between husband and wife [is] privileged."). *But see* Trammel v. United States, 445 U.S. 40, 52–53 (1980) (outlining the limits of spousal privilege when one spouse chooses to testify against the other in a criminal matter).

[16] *See* Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g(b) (Supp. III 2003) (denying federal funds to educational institutions that violate confidentiality by releasing student records to unauthorized individuals or agencies).

[17] *See* 12 U.S.C. §§ 3402–3403 (2000) (prohibiting financial institutions from releasing customers' financial records except in compliance with subpoena or search warrant); 18 U.S.C. § 1702 (2000) (providing criminal penalties to anyone who opens mail "to obstruct the correspondence, or to pry into the business or secrets of another"); *id.* § 2511 (providing criminal penalties to anyone who intentionally intercepts "any wire, oral, or electronic communication"); *id.* §§ 2701–2702(a) (providing criminal penalties for anyone who knowingly discloses electronic communication provided through the means of communication or access to the electronic storage); *id.* § 2710 (creating a civil cause of action for a video tape service provider who releases consumer information to an unauthorized person); Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971) (explaining that the First Amendment does not give the media "a license to trespass, to steal, or to intrude by electronic means into the precincts of another's home or office"

Even where the law does not recognize a legally-enforceable privilege, various professions often seek to afford a shelter from disclosure. For example, journalists routinely agree to speak to sources "off the record" and insist upon maintaining confidences even in the face of court orders to the contrary.[18]

Yet, there is still conflicting sentiment about maintaining confidences. By definition, the person who guards a secret is being secretive; he or she is not being completely "open." Indeed, when inquiries are directed to the person regarding the confidential matter, the response by the person maintaining the secret may be fairly characterized as evasive at best or even downright dishonest. Ironically, journalists, who are among the strongest proponents for maintaining the confidentiality of their own sources, are also among the most vocal advocates for open record and sunshine laws.[19] This conflict between maintaining trust and, at the same time, affording transparency or openness is reflected in conflicting claims of privilege and privacy.

B. *The Attorney's Obligation to Maintain Confidences*

It should come as no surprise that, as members of a profession charged with protecting the well-being of their clients, attorneys are required to maintain their clients' secrets.[20] It should also come as no surprise that some of the societal ambivalence about keeping secrets, coupled with public distrust of attorneys, makes the attorney's role particularly challenging. Under the general

even for criminal investigative reporting); Camp, Dresser & McKee, Inc. v. Steimle & Assocs., Inc., 652 So. 2d 44, 47–48 (La. Ct. App. 1995) (affirming an injunction barring the defendants "from entering the [plaintiff's] trash dumpsters and disseminating the information collected from the trash" based on anti-scaving and deceptive trade practices statutes).

[18] *See In re* Grand Jury Subpoena, Judith Miller, 397 F.3d 964, 970 (D.C. Cir. 2005) (applying a Supreme Court ruling that the press does not enjoy a privilege of confidentiality and must comply with court orders to reveal sources in grand jury proceedings). After the D.C. Circuit upheld the court order compelling her to testify, reporter Judith Miller still refused to testify and reveal her source for the leak of covert C.I.A. agent Valerie Wilson's name. Adam Liptak & David Johnston, *A Reporter Jailed: The Overview; Reporter Jailed after Refusing to Name Source*, N.Y. TIMES, July 7, 2005, at A1. Miller spent over twelve weeks in jail before deciding to testify after her sources waived confidentiality. *Id.*

[19] *See* Gordon Dickson, *Lawsuit Filed to Keep Documents Private*, FT. WORTH STAR-TELEGRAM, June 25, 2005, at B5 (reporting that newspapers made open records requests in regards to contracts concerning the Trans-Texas Corridor).

[20] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2007).

obligation to maintain confidentiality as set out in Rule 1.6 of the Model Rules of Professional Conduct, attorneys are precluded from revealing "information relating to the representation of a client."[21] Rule 1.6 allows disclosure only under carefully defined circumstances.[22] The underlying reason for the existence of the rule is that the maintenance of the confidentiality "contributes to the trust that is the hallmark of the client-lawyer relationship."[23] This trust in the attorney will result in the client feeling "encouraged to seek legal assistance and to communicate fully and frankly with the attorney even as to embarrassing or legally damaging subject matter."[24] The importance of maintaining attorney-client confidentiality and allowing attorneys to decline to reveal confidential information obtained from their clients has been recognized as necessary "to encourage full and frank communication between attorneys and their clients."[25] Even where the attorney has preliminary discussions with a prospective client that do not result in the creation of an attorney-client relationship, the attorney nonetheless must maintain the confidences acquired in those communications.[26] Supervisory attorneys must "make reasonable efforts to ensure that" subordinate attorneys[27] and nonlawyer assistants[28] comply with the professional rules, including maintaining confidences.

On a practical level, maintaining confidence is of utmost importance to both attorneys and their clients.[29] Attorneys who

[21] *Id.*

[22] *See id.* 1.6(b) (permitting a lawyer to reveal confidential client information if the lawyer reasonably believes it is necessary "to prevent reasonably certain death or substantial bodily harm," or other certain crimes and fraudulent activities committed by the client in which the lawyer's services have been used).

[23] *Id.* 1.6 cmt. 2.

[24] *Id.*

[25] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981). "The attorney-client [evidentiary] privilege is one of the oldest recognized privileges for confidential communications." *Id.*

[26] *See* MODEL RULES OF PROF'L CONDUCT R. 1.18(b) (2007) (enumerating the duties owed by lawyers to prospective clients).

[27] *See id.* 5.1 (explaining the duties of supervisory attorneys, including reasonable efforts to guarantee that subordinate lawyers comply with the professional conduct rules).

[28] *See id.* 5.3 (explaining the responsibilities of supervisory attorneys regarding nonlawyer assistants, including reasonable efforts to ensure that nonlawyers are complying with the professional conduct rules).

[29] *See* Daniel R. Fischel, *Lawyers and Confidentiality*, 65 U. CHI. L. REV. 1, 3–9 (1998) (explaining the importance of confidentiality to both lawyers and clients). Within

fail to adequately protect their clients' information may face a number of repercussions including: discipline (e.g., sanctions, suspension, or disbarment) for violating professional responsibility rules;[30] liability or sanctions under federal or state statutes;[31] malpractice claims for incompetence or negligence;[32] and loss of

the legal profession, however, there exists some controversy regarding the underlying purpose of confidentiality. Some critics suggest that the legal profession, not the client or society, is the primary beneficiary of confidentiality requirements because confidentiality increases the demand for legal services. *See id.* at 3 (recognizing that confidentiality rules "made clients more willing to hire attorneys").

[30] *See, e.g.*, People v. Hohertz, 102 P.3d 1019, 1022–24 (Colo. 2004) (relating disbarment of attorney because the attorney committed several ethics violations, including revealing client confidences); *In re* Bryan, 61 P.3d 641, 649, 661 (Kan. 2003) (affirming censure of an attorney for disclosing confidential information to opposing counsel about his client's unrelated pending defamation case); Akron Bar Ass'n v. Holder, 102 Ohio St. 3d 307, 2004-Ohio-2835, 810 N.E.2d 426, at ¶¶ 40–43 (upholding a two year suspension imposed on an attorney for improperly disclosing his client's confidences during a deposition); State v. Chappell, 2004 OK 41, ¶¶ 13–28, 93 P.3d 25, 28–31 (imposing a one year suspension upon an attorney who used confidential information in a court document); *In re* Disciplinary Proceeding Against Schafer, 66 P.3d 1036, 1040 (Wash. 2003) (approving a six month suspension for a lawyer who revealed his client's confidences); *In re* Disciplinary Proceedings Against Harman, 2001 WI 71, ¶¶ 21–22, 29, 244 Wis. 2d 438, ¶¶ 21–22, 29, 628 N.W.2d 351, ¶¶ 21–22, 29 (ordering a six month suspension of an attorney for disclosing a client's medical records to a prosecutor who was prosecuting the client's cohabitant).

[31] *See, e.g.*, Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 264–72 (2005) (analyzing the duty to protect database information). Professor Johnson's article discusses the possibility of liability under the Gramm-Leach-Bliley Act of 1999, codified in scattered sections of Title 12 and Title 15 of the United States Code. *Id.* at 266–70. Under the Gramm-Leach-Bliley Act, financial institutions must protect the security of customers' nonpublic personal information. 15 U.S.C. § 6801(a) (2000) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."). While the plain language of the Act "generally does not cover retail merchants that do not issue their own credit," the Federal Trade Commission nonetheless has aggressively used the Gramm-Leach-Bliley Act to pursue actions against nonfinancial companies. Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, 54 FED. LAW., Sept. 2007, at 39, 40–41 (discussing FTC enforcement actions of the Gramm-Leach-Biley Act against nonfinancial institutions); *see* Heath Dixon, *FTC Nails Company for Failing to Implement Reasonable Security*, PRIVACY SPOT, Nov. 21, 2004, http://privacyspot.com/?q=node/view/429 (reporting charges against Petco Animal Supplies for failing to have reasonable security to protect its online customers). *See generally* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 263–80 (2005) (discussing liability under state statutes).

[32] *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 272–76 (2005) (discussing a potential cause of action for negligence when a business fails to safeguard confidential information); *see also* MODEL

reputation, including professional embarrassment or negative media exposure.[33] Attorneys may believe they are using good faith and competent, reasonable actions to protect their clients' information from security breaches, and yet, through an act of carelessness, may inadvertently allow unauthorized access to the information.[34] These disclosures may result in problems such as identity theft, loss of intellectual property protection, client embarrassment, exposure of legal strategy, or other detrimental effects—any of which could result in significant losses to the clients.[35]

III. UNINTENDED DISCLOSURE VIA TECHNOLOGY

Before computers, attorneys generally wrote down a client's information and stored the file in a lockable file cabinet in a lockable office.[36] During this time, securing file cabinets and offices, usually through locks, was considered a reasonable precaution to safeguard client information.[37] Although offices

RULES OF PROF'L CONDUCT R. 1.6 cmt. 2 (2007) (discussing the duty of lawyers with regard to confidential information).

[33] *See, e.g.*, Chris Dettro, *Court Disbars Attorney Involved in Drug Probe*, ST. J.-REG., June 5, 2007, at Local 31 (reporting disbarment of an attorney for drug use with clients and for profiting from the sale of confidential reports); Bob Egelko, *The BALCO Case: Admitted Leaker Agrees to Longer Prison Term*, S.F. CHRON., July 6, 2007, at B4 (reporting about a lawyer who accepted a plea agreement to serve two years and nine months in prison for leaking confidential information to a newspaper); Gregory D. Kesich, *Court Disbars Lawyer for String of Complaints*, PORTLAND PRESS HERALD, Apr. 15, 2004, at 2B (detailing the reasons for disbarring a lawyer, including "client neglect, excessive fees, incompetency, [and] unauthorized disclosure of confidential information"); Jonathan Saltzman, *Lawyer May Face Disbarment,* BOSTON GLOBE, July 2, 2005, at B5 (reporting an attorney facing disbarment for posting confidential information on her website about a boy being sexually abused by his father and for negligently failing to use a pseudonym for the boy's name in court proceedings).

[34] *Cf.* Erik Runge, *Gold Mine for ID Thieves: Thousands of Records Found in Dumpster*, http://www.woai.com/news/local/story.aspx?content_id=1a103b0d-d2bd-4ba9-99c2-214020cbed75 (last visited May 20, 2008) (reporting how confidential material belonging to a law firm, including clients' social security numbers and medical records, was found in a dumpster).

[35] *Cf. In re* Huffman, 983 P.2d 534, 543 (Or. 1999) (discussing potential harm to client due to the attorney's disclosure of confidential information).

[36] *See* Jesse J. Richardson, Jr., *How a Sole Practitioner Uses the "Electronic Office" to Maintain a Competitive Law Practice*, 3 DRAKE J. AGRIC. L. 141, 147 (1998) (noting that historically lawyers did not use electronic means of communication).

[37] *See* Peter E. Moll & J. Michael Hennigan, *Using Document Imaging and Technology as Marketing Tools*, 13 No. 1 ALA NEWS, Dec. 1993–Jan. 1994, at 36 (describing how traditional methods of safeguarding client information recorded on paper

could be broken into or client conversations surreptitiously listened to with tapping, this was usually considered too far-fetched to be a legitimate concern to law firms.[38]

As computers became more prevalent, the legal profession, like other businesses, began to rely on the convenience of electronic files stored on computers within networks and transmitted through e-mails.[39] However, the ease of electronic transmission also seemingly made it less apparent whether an electronic file had been inappropriately accessed, altered, or copied.[40] Additionally, relatively inexpensive listening devices and cameras are available and can now be used to spy remotely on conversations.[41] Attorneys who continue to secure their offices with locks alone may not realize that walls and windows are permeable to sound waves and electromagnetic transmissions, potentially allowing unauthorized access.[42] While attorneys may respond that this type

files have become outdated by modern electronic files).

[38] *See* Dalia v. United States, 441 U.S. 238, 252 (1979) (explaining the difficulties of installing wiretapping devices at that time). *But see* David F. Halbfinger, *Investigator to the Stars Is Convicted in Wiretaps*, N.Y. TIMES, May 16, 2008, at C1, *available at* http://www.nytimes.com/2008/05/16/business/16pellicano.html (discussing the extensive wiretapping operations of private investigator Anthony Pellicano and the possible involvement of entertainment attorney Bert Fields); David Jackson, *Watergate's Tidal Wave: 25 Years Later, Scandal's Imprint Remains on Government, Society*, DALLAS MORNING NEWS, June 15, 1997, at 1A (discussing the events and consequences of the break-in and attempted wiretapping of the Democratic National Committee headquarters in the Watergate Hotel).

[39] *See* Jesse J. Richardson, Jr., *How a Sole Practitioner Uses the "Electronic Office" to Maintain a Competitive Law Practice*, 3 DRAKE J. AGRIC. L. 141, 147 (1998) (explaining the benefits of transmitting documents via e-mail).

[40] *See* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 180–81 (2002) (describing how to avoid detection while accessing documents on a computer). *But see* Microsoft, HOW TO: Audit Active Directory Objects in Windows Server 2003, http://support.microsoft.com/kb/814595 (last visited May 20, 2008) (providing step-by-step instructions to enable auditing on a Windows Server). Windows auditing allows administrators to track failed and successful access to documents. *Id.*

[41] *See* Spy Associates, http://www.spyassociates.com (last visited May 20, 2008) (advertising and selling information gathering items such as cameras, tracking devices, recorders, and computer software). *See generally* Christopher J. Selin, *Eavesdropping on the Compromising Emanations of Electronic Equipment: The Laws of England and the United States*, 23 CASE W. RES. J. INT'L LAW 359, 359–60, 363 (1991) (describing the history of spy technology, which started as physical eavesdropping and evolved into commonplace listening devices).

[42] *See* Michael Evans, *Inside the Most Bugged Offices in the World*, TIMES ONLINE, Feb. 27, 2004, http://www.timesonline.co.uk/tol/news/uk/article1031533.ece (describing a "laser aimed at the window of a targeted office [that] can detect minute reverberations in

of behavior from opposing counsel would violate the rules of professional responsibility, the fact remains that the "adversarial party" is not always another attorney who is bound to play by the professional rules.[43] Instead, the adversarial party may be someone who is able or willing to disregard legal and ethical constraints on gathering information.[44] Further, there is an even higher risk associated with law firms that handle cases involving national security.[45] The various ways which information might be unintentionally exposed or disclosed are limitless.[46] The following scenarios and accompanying discussions illustrate the potential problems. After examining these problems, we will outline an approach attorneys should use in fulfilling the obligation to protect

the glass caused by conversations"); *see also* Kevin Murphy, *Consumers Set Sights on Tiny Cameras*, CONTRA COSTA TIMES, Jan. 29, 2006, at F4 (stating that spy technology is available for purchase by the common consumer).

[43] *See In re* Meador, 968 S.W.2d 346, 349 (Tex. 1998) (recounting how an employee at a company found and used information from the company's legal department against her employer).

[44] *See, e.g.*, *id.* at 348–49 (explaining that an employee who wanted to bring a sexual harassment lawsuit against a former manager of the company gave her attorney confidential papers prepared by the corporation's legal staff); David F. Halbfinger, *Investigator to the Stars Is Convicted in Wiretaps*, N.Y. TIMES, May 16, 2008, at C1, *available at* http://www.nytimes.com/2008/05/16/business/16pellicano.html (reporting that a jury found private investigator Anthony Pellicano guilty on seventy-six counts, most related to illegal wiretapping). As another example of parties willing to disregard the law, a recent *Business Week* story detailed an attempted e-mail attack on Booz Allen Hamilton. Brian Grow, Keith Epstein & Chi-Chu Tschang, *The New E-spionage Threat*, BUS. WK., Apr. 21, 2008, http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm (describing an e-mail sent to a Booz Allen Hamilton executive which was crafted to trick the recipient into clicking on a link in the e-mail, thereby installing spyware on the computer). While similar attacks aimed at broad audiences (called *phishing*) are common, the Booz Allen Hamilton e-mail was unusual because it was aimed at a specific individual (called *spear-phising*). *Id.* The information used to tailor the e-mail to the Booz Allen Hamilton executive was gleaned from public information. *Id.*

[45] *See, e.g.*, Douglas Jehl, *U.S. Expanding Its Effort to Halt Spying by Allies*, N.Y. TIMES, Apr. 13, 2007, at 34 (discussing the attempts by the French government to engage in corporate espionage against United States corporations working in aerospace and other government-related industries); *see also* Jason Kirby, *Corporate Espionage Is Big Business*, MACLEAN'S MAG., July 2, 2007, at 34 (discussing courts' and prosecutors' slow responses to claims of corporate espionage).

[46] *See generally* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 13–242 (2002) (describing the different ways confidential information can be leaked). One organization provides running totals of data breaches. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited May 20, 2008) (listing data breaches, including an up-to-date total number of records lost due to breaches).

these confidences.

A. *Hotel Room Security*

In the first scenario, several attorneys are working on a case away from home and staying in a hotel. After a hard day's work, the attorneys return to their hotel and make dinner plans. They consider leaving their laptops in the trunks of their rental cars, but they fear the risk of having the cars broken into or stolen. Instead, they decide that it is safer to leave their computers in their hotel rooms: because the rooms were cleaned earlier in the day, no one is expected to come into their rooms for the rest of the evening. When they return to their hotel rooms, nothing appears out of the ordinary. Yet, once back in their home office, it seems that opposing counsel anticipates their legal strategy and is knowledgeable about the confidential aspects of the case.

Was there a security breach? Consider this possibility: an investigator bribes hotel personnel to inform him when members of a certain law firm check into the hotel. Perhaps the maid or bellboy learns this information from the luggage tags on the attorneys' bags identifying their firm.[47] While the attorneys are enjoying dinner, the investigator enters their rooms using the informant's key card. This allows the investigator an opportunity to access the attorneys' computers and to attempt to copy files. Maybe the investigator successfully installs software on the laptops to create a secret account whereby the investigator can access the computer remotely.[48] Alternatively, the software may send files back to the investigator whenever the computer is connected to

[47] *Compare* Studio 6 Extended Stay Hotel, Accor Privacy Protection Policy, http://www.staystudio6.com/about/privacy.asp (last visited May 20, 2008) (providing the hotel's privacy policy, including the policy not to give guest information to third parties), *and* Four Seasons Hotels and Resorts Privacy Policy, http://fourseasons.com/privacy.html (last visited May 20, 2008) (assuring that no guest information will be given to third parties), *with* Marcus Bruninghaus, *Protecting Guest Data: Why Hotel Information Security Awareness Training Is So Important*, ENTER. INNOVATOR, Apr. 21, 2006, http://enterpriseinnovator.com/index.php?articleID=7291&sectionID=25 (urging hotels to properly train employees regarding information security issues to prevent the majority of incidents that are caused by human error and improper training).

[48] *See, e.g.*, AceSpy, http://www.acespy.com/details.html (last visited May 20, 2008) (selling spy software products). "AceSpy Spy Software makes it easy to secretly see what others do online. After you install, it will begin secretly recording EVERYTHING that is done on [the personal computer]. AceSpy is COMPLETELY hidden from others. They won't know it's running unless you tell them!" *Id.*

the Internet.[49] The attorneys never realize what has happened, and therefore cannot trace the adversarial party's actions to this incident.

What security precautions could have prevented these security breaches? Should laptops never be left unattended?[50] Would it matter if the laptops were password protected?[51] In reality, attorneys should take only limited comfort in password protection, as passwords can sometimes be broken using automated tools.[52] Short of carrying a laptop around (with the possibility of either leaving the laptop or having it stolen), what can be done? The problem with this type of post hoc analysis is that it is reactive and typically establishes a "band-aid"[53] approach to fix the problem. For example, today a firm has a laptop stolen from an attorney's car at lunch, so tomorrow it establishes a rule that laptops are not to be left in cars during lunch. Unfortunately, such solutions do not possess the necessary preventative aspect to counter future, unknown attacks.

B. *Insider Threat and Social Engineering*

In the second scenario, a large law firm routinely and diligently trains its support staff personnel in security processes and establishes rules for all aspects of computer security.[54] For

[49] *See* NetVizor, http://www.spytech-web.com (last visited May 20, 2008) (selling computer monitoring software that records and transmits all information and keystrokes from one computer to another computer). There are several versions of computer monitoring software available with a variety of spyware features, including remote capabilities and the ability to control the targeted computer. *Id.*

[50] *See* Mark Bassingthwaighte, *Ten Technology Traps and How to Avoid Them*, W. VA. LAW., Sept.–Oct. 2006, at 34, 34 (noting that keeping a laptop in sight, carrying it on a plane, using password protection, and using encryption software can keep confidential client information safe).

[51] *See generally id.* (recommending several steps that lawyers and employees may take in order to prevent laptop security breaches).

[52] *See* Yahoo Password Hack Freedownload, http://www.brothersoft.com/downloads/yahoo-password-hack.html (last visited May 20, 2008) (providing users access to free programs that restore user login passwords); Top 100 Network Security Tools, http://sectools.org (last visited May 20, 2008) (listing the top security tools, as voted upon by visitors to the website). The list of network security tools includes several password decrypting tools available for free. Top 100 Network Security Tools, http://sectools.org (last visited May 20, 2008).

[53] *See* WEBSTER'S UNABRIDGED DICTIONARY 162 (2001) (defining band-aid as "a makeshift, limited, or temporary aid or solution that does not satisfy the basic or long-range need").

[54] *See generally* HOWARD I. HATOFF & ROBERT C. WERT, LAW OFFICE POLICY &

example, the firm implements a rule that passwords must consist of a minimum number of letters and numbers and be changed regularly.[55] The law firm also hires a well-known and highly competent computer company for maintenance of its computers and networks. The computers are routinely checked for viruses,[56] worms,[57] spyware,[58] Trojans,[59] and spam[60] by the latest security software. Despite this effort, however, highly confidential information in documents stored on a single computer used only by a long-term and trusted staff member becomes known by an adversary party.

What was the source of a security breach? Consider two possible explanations. The first possibility is rather obvious. Perhaps the once well-trusted staff member has become a disgruntled employee who has provided the adversary with a copy of the files.[61] A less obvious possibility is that the well-trusted

PROCEDURES MANUAL, FORMERLY LAW OFFICE STAFF MANUAL (Am. Bar Ass'n 5th ed. 2006) (providing a basic law office manual that addresses information security and training of new employees at law firms).

[55] *Cf.* Mark Bassingthwaighte, *Ten Technology Traps and How to Avoid Them*, W. VA. LAW., Sept.–Oct. 2006, at 34, 34 (encouraging lawyers to use passwords on their laptops so as not to grant instant access to anyone who might try to use their computers).

[56] *See* WEBSTER'S NEW WORLD HACKER DICTIONARY 348 (2006) (defining virus as "a harmful, self-replicating program usually hidden in another piece of computer code, such as an email message"). A virus relies on user interaction to launch a separate piece of software which allows the virus to propagate. *Id.* at 363.

[57] *See id.* at 363 (defining worm as "a self-replicating, self-contained software program that does not need to be a part of another program to propagate").

[58] *See id.* at 298 (defining spyware as "[c]overt software that captures data about online users' Internet surfing habits").

[59] *See* WEBSTER'S NEW WORLD HACKER DICTIONARY 328 (2006) ("Named after the Trojan Horse of ancient Greek history, it is a particular kind of network software application developed to stay hidden on the computer where it has been installed."). Trojans may harvest user data, provide a backdoor for attackers, or serve as a denial-of-service tool. *Id.*

[60] *See id.* at 298 (defining spam as "[u]nsolicited, unwanted, impersonal email").

[61] If an employee provides an adversary with a copy of the files, this would be an example of an insider threat. *See* CERT, Insider Research Threat, http://www.cert.org/insider_threat (last visited May 20, 2008) ("Current and former employees and contractors have exploited vulnerabilities . . . to commit fraud, theft of sensitive information, and IT sabotage."). While many insider threats are disgruntled employees, some are also "plants," people who obtain jobs for the express purpose of procuring information for another party. Insider threats are one of the fastest growing and hardest to detect security breaches. *See* Computer Crime & Intellectual Property Section, U.S. Dep't of Justice, http://cybercrime.gov (last visited May 20, 2008) (reporting federal computer crime cases and providing information about "cyberethics"); *cf.* SECTION OF SCI. & TECH. LAW, LAW PRACTICE MGMT. SECTION, INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS

staff member may have fallen prey to "social engineering," the technique of obtaining information or access through person-to-person contact.[62] Social engineering relies on deceptive tactics to trick well-meaning and honest people into voluntarily divulging information.[63]

For example, a friendly man[64] approaches an employee with a legitimate identification badge from the computer support company hired to maintain the law firm's equipment.[65] The computer company's personnel often work in the law office, although the employee has never met this particular consultant. The man provides a work order for routine maintenance on the employee's printer. He apologizes profusely for interrupting the staff member's work and offers to finish quickly to minimize the disruption. Because the man appears to have all the proper paperwork and valid identification, the employee allows the "consultant" to sit at the desk while performing maintenance on

300–03 (Sharon D. Nelson et al. eds., 2006) (discussing the problem of "disgruntled employee" insider threats). The authors of *Information Security for Lawyers and Law Firms* detail "real-life nightmares" of companies where insiders stole personal information or trade secrets, crashed systems, or stole personal files; however, none of these incidents occurred at law firms. SECTION OF SCI. & TECH. LAW, LAW PRACTICE MGMT. SECTION, INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS 300–03 (Sharon D. Nelson et al. eds., 2006).

To gauge the damage from an insider threat, consider that the most dangerous spy in FBI history was a trusted FBI agent and supervisor, Robert Hanssen, who used his computer expertise and direct knowledge of the workings of the internal systems to circumvent detection for nearly twenty years. DAVID A. VISE, THE BUREAU AND THE MOLE 224–29 (2002) (highlighting events of Robert Hanssen's times as a double agent). *See generally* Dawn Cappelli, Andrew Moore & Timothy Shimeall, *Protecting Against Insider Threat*, NEWS @ SEI, http://www.sei.cmu.edu/news-at-sei/columns/security_matters/2007/02/security-matters-2007-02.htm (last visited May 20, 2008) (providing an excellent list of practices to prevent insider threats).

[62] *See* SECTION OF SCI. & TECH. LAW, LAW PRACTICE MGMT. SECTION, INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS 293 (Sharon D. Nelson et al. eds., 2006) (defining social engineering as "the art of getting people to divulge information . . . so that there is no necessity of going to the trouble of hacking").

[63] KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY xi (2002).

[64] *See id.* at 8 (describing social engineers as "charming, polite, and easy to like" individuals, who use those traits to gain "rapport and trust").

[65] *See* Philip Cornford, *The Brazen Airport Computer Theft That Has Australia's Anti-terror Fighters Up in Arms*, SYDNEY MORNING HERALD, Sept. 5, 2003, http://www.smh.com.au/articles/2003/09/04/1062548967124.html (describing an incident at the Sydney International Airport where two men, dressed as computer repair technicians and carrying tools, stole two mainframes which may have contained confidential information).

the printer.[66] Nothing occurs to raise the staff member's suspicions about the friendly consultant who is so intent on minimizing the interruption of work. Perhaps the two even chat amicably about their families. The man tells the staff member not to bother logging off of the computer so that he can finish as quickly as possible.[67] While pretending to run printer diagnostics, he inserts a flash drive into the USB port and begins to copy files.[68] Alternatively, he may install spyware as in the preceding scenario. Again, the breach was not prevented, detected, or remedied, resulting in potentially substantial harm.

This scenario illustrates two of the more prevalent and arguably underestimated security intrusion techniques: (1) insider threats[69]

[66] Assuming that the firm's attorneys know nothing of the events transpiring, the law firm will not be responsible for any violation of the rules of professional conduct that results from the staff member's actions. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3(b)–(c) (2007) (stating that a lawyer with direct supervisory authority over a nonlawyer employee is responsible for the conduct of persons that violate rules of professional conduct only if the attorney orders or specifically approves the conduct, or knows of the conduct and takes no action to avoid or mitigate the consequences).

[67] *See* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION, CONTROLLING THE HUMAN ELEMENT OF SECURITY 41 (2002) ("The more a social engineer can make his contact seem like business as usual, the more he allays suspicion.").

[68] *See* How to Use a USB Flash Drive (PC Computer), http://www.hs.iastate.edu/it/support/instructions/How_to_Use_USB_flash_drive_(PC_Version).doc (last visited May 20, 2008) (giving the user steps to properly copy files from a computer to a flash drive). To copy documents from a computer to a flash drive, you first insert the flash drive into a USB port in the computer. *Id.* Then you locate the file that you wish to copy. *Id.* Next, you right-click the folder and highlight "send to." *Id.* You select the appropriate "Removable Disk" according to the drive letter. *Id.* Before removing the flash drive, make sure that the file was copied and then left double-click "My Computer," followed by the "Removable Disk" that you previously selected. How to Use a Flash Drive (PC Computer), http://www.hs.iastate.edu/it/support/instructions/How_to_Use_USB_flash_drive_(PC_Version).doc (last visited May 20, 2008).

One example of a nefarious use of seemingly innocuous technology is "pod slurping," whereby an intruder connects an iPod to a USB port on an active machine on a network and copies the contents of the target machine and documents shared on the network. *See* Sharon D. Nelson, Esq. & John W. Simek, *She Stole Our Company Data and Hid It in Her Underwear*, 70 TEX. B.J. 844, 850 (2007) (describing the removal of data from a company by an employee using an iPod). "[I]n 2 minutes, it's possible to extract about 100MB of Word, Excel, PDF files—basically anything which might contain business data—and with a 60GB iPod, you could probably have every business document in a medium-size firm." Will Sturgeon, *Beware the 'Pod Slurping' Employee*, CNET NEWS.COM, Feb. 15, 2006, http://www.news.com/Beware-the-pod-slurping-employee/2100-1029_3-6039926.html.

[69] *See* John D. Comerford, *Competent Computing: A Lawyer's Ethical Duty to Safeguard the Confidentiality and Integrity of Client Information Stored on Computers and Computer Networks*, 19 GEO. J. LEGAL ETHICS 629, 639 (2006) (discussing briefly insider threats and the lawyer's responsibility for the conduct of employees who handle

and (2) "social engineering."[70] Insider threat is a risk that comes from *within* the organization, either through disgruntled employees or "plants."[71] In fact, it is estimated that 84% of security breaches come from insider threats.[72] There is no reason to believe that law firms are more immune from insider threats than any other company.

The second technique, social engineering, uses deception to mislead individuals into providing information, as explained above. For example, Kevin Mitnick, who excelled at social engineering, used a process of data aggregation to obtain the credit information of his target: by retrieving pieces of seemingly meaningless information from a number of sources, the aggregation of the pieces could be used to attain the desired information.[73] In fact, many computer break-ins occur not

confidential information).

[70] *See generally* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 173–224 (2002) (providing an excellent treatise on social engineering). This book also lists several social engineering ploys which gain access to confidential information over the telephone or in person. *Id.*

[71] *See* CERT, Insider Threat Research, http://www.cert.org/insider_threat (last visited May 20, 2008) (asserting that an insider may be a current or former employee who knows how a company's system works).

[72] *See* SECTION OF SCI. & TECH. LAW, LAW PRACTICE MGMT. SECTION, INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS 303 (Sharon D. Nelson et al. eds., 2006) ("The Gartner Group reports that 84% of high-cost security incidents occur when insiders send confidential information outside the company."); *see also* CERT, Insider Threat Research, http://www.cert.org/insider_threat (last visited May 20, 2008) (providing reports and podcasts from the Software Engineering Institute at Carnegie Mellon University on security issues including protection against insider threats).

[73] *See generally* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY ix–xii (2002) (describing the way Mitnick went about his "art of deception"). Mitnick could begin with just the name of an intended target and within four or five conversations with well-intentioned people, gain enough information to gain access to the target's confidential financial information. *See id.* at 15–29 (giving various examples of people giving out confidential information after a few conversations). One case, documented in his book, concerns a private investigator (PI) who assisted a wife divorcing her husband. *Id.* at 16–22. The wife's attorney was unable to locate the husband's assets. *Id.* The PI called the bank pretending to be an author and obtained the correct terminology ("Merchant ID") for the bank to identify itself to its credit bureau; called the bank a second time and, using the correct lingo, passed himself off as a customer service representative from the bank's credit bureau and obtained the bank's Merchant ID; and finally called the credit bureau and identified himself as the bank with the correct Merchant ID, the husband's name and social security number, and obtained all his financial information. KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF

through hacking into the computer or network but by obtaining system access codes through friendly chats.[74] Clearly, mere password protection rules will not prevent social engineering attacks.

C. *E-mail Correspondence*

The third scenario begins with a client who is upset about the time billed for a particular matter. The client engages in a lengthy sequence of back-and-forth e-mail communications with the accounts receivable department in the law firm. The client requests a complete history of the issue including detailed billing over a two year period.[75] The accounts receivable department gathers the extensive information and e-mails it to the client.[76] Although both the client and the accounts receivable department claim to have used the "reply to" e-mail function during the

SECURITY 16–22 (2002).

Mitnick's books, including *The Art of Deception*, contain a treasure trove of techniques for obtaining confidential information from helpful and friendly staff who never realize the deception. *See id.* xv–xvi (introducing the various techniques that are outlined in the book). Mitnick is fond of saying that the most powerful computer security is useless if hackers can con helpful targets into revealing access information. Rebecca Harrison, *'Computer Terrorist' Kevin Mitnick Now Teaches Antihacking*, COMPUTER WORLD, Mar. 9, 2006, http://www.computerworld.com/securitytopics/security/story/0,10801,109351,00.html.

[74] *See generally* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 15-146 (2002) (providing examples of methods used to obtain information such as building trust, offering help, and using sympathy tactics).

[75] *See* MODEL RULES OF PROF'L CONDUCT R. 1.4 (2007) (laying out the requirements for effective communication between attorneys and clients); *id.* 1.5 (establishing the rules for assessment of fees on a client in exchange for service). These two provisions, when read together, indicate that communication regarding fees is essential to maintaining an open and effective relationship between attorney and client. *See* TEX. DISCIPLINARY R. PROF'L CONDUCT 1.03, *reprinted in* TEX. GOV'T CODE ANN., tit. 2, subtit. G app. A (Vernon 2005) (TEX. STATE BAR R. art. X, § 9) (codifying the Texas Disciplinary Rules of Professional Conduct's stance on the necessity of communication between the client and the attorney); *id.* 1.04 (explaining the Texas rules regarding how attorneys should charge their clients). E-mailing a client may satisfy both the requirement of communication and the exhortation to memorialize fee agreements in writing.

[76] *See generally* TEX. DISCIPLINARY R. PROF'L CONDUCT 1.05, *reprinted in* TEX. GOV'T CODE ANN., tit. 2, subtit. G app. A (Vernon 2005) (TEX. STATE BAR R. art. X, § 9) (codifying the requirements of confidential communication to clients); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) (establishing the ABA's approach to the relationship between the need for confidentiality and e-mail communications).

exchange, the accounts receivable department inadvertently sends the information to the client's old e-mail address at her former employer. Consequently, the law firm erroneously sends the client's information to the wrong party.[77] The law firm does not discover the error until the client again requests the information.

D. *Disposal of Old Computers*

In the last scenario, a law firm acquires new computers either by purchase or lease.[78] Several alternatives exist to dispose of the old computers.[79] Being a good corporate citizen, the law firm could donate to charity any old computers owned by the firm.[80] Prior to donation and conscious of the need to destroy any client information on the hard drives, the firm may engage the services of a business that specializes in removing such information permanently.[81] On the other hand, instead of purchasing the computer equipment, the firm may simply lease its equipment and allow the vendor to switch out and upgrade old workstations.[82] Regardless of the disposal method, law firms need to consider and

[77] It should be noted that even if the information is sent to the correct address, an unencrypted e-mail can be read by anyone who intercepts the e-mail.

[78] *See* Karen A. Clanton, *Ode to Joy*, 18 CBA REC. 43, 44 (2004) ("Law firms on the other hand, upgrade and replace their computers all the time."); *cf.* Steve Bickerstaff, *Shackles on the Giant: How the Federal Government Created Microsoft, Personal Computers, and the Internet*, 78 TEX. L. REV. 1, 30 (1999) (noting "[t]he continuous pressure on personal computer users to upgrade or replace their systems or applications").

[79] *See* Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 29–31 (2004) (providing an excellent list of various scenarios related to ethical considerations stemming from the disposal of hard drives and old computer systems); *see also* Mark Bassingthwaighte, *Ten Technology Traps and How to Avoid Them*, W. VA. LAW., Sept.–Oct. 2006, at 34, 39 (listing proper disposal of sensitive data among the top concerns facing modern-day litigants).

[80] *See, e.g.*, U.S. Environmental Protection Agency, Where Can I Donate or Recycle My Old Computer and Other Electronic Products?, http://www.epa.gov/epaoswer/hazwaste/recycle/ecycling/donate.htm (last visited May 20, 2008) (showing the EPA's extensive computer recycling, disposal, and reuse program). The page provides advice for business and personal donors, as well as useful links to various recycling programs. *Id.*

[81] *See generally* Secure Destruction Bus., http://www.sdbmagazine.com/ (last visited May 20, 2008) (providing links, articles, and trade information to businesses seeking secure destruction of their sensitive documents).

[82] *See e.g.*, Dell Computer Inc., Asset Recovery & Recycling Services, http://www.dell.com/content/topics/global.aspx/services/en/assetrecoveryservices?c=us&l=en&s=corp (last visited May 20, 2008) (describing Dell's computer recovery and recycling program). The Dell program is an example of a recycling program and some of the benefits of allowing the manufacturer to reclaim old workstations. *Id.*

address the possibility that confidential client information remains stored on the computers and may pass into the hands of third parties.

Legal scholars have recently begun examining the many repercussions of this scenario.[83] There is a growing awareness of what can happen to the hard drives of discarded computers, or more precisely, what can happen to the data contained therein.[84] It is also more commonly known that deleting files on computers does not delete the information from the hard drive any more than deleting a card catalogue in a library deletes the books stored there.[85] What is less commonly known is that reformatting a hard drive, even a number of times, does not prevent the recovery of information stored on that hard drive.[86]

As a consequence of the lack of knowledge, there are several well-publicized examples of computers being discarded without proper removal of confidential student,[87] medical,[88] and legal information.[89] In fact, Simson Garfinkel of Massachusetts Institute of Technology has built a database of information gathered from discarded hard drives retrieved from, among other

[83] *See* Mark Bassingthwaighte, *Ten Technology Traps and How to Avoid Them*, W. VA. LAW., Sept.–Oct. 2006, at 34–40 (playing out various scenarios where attorneys may breach their clients' confidences by improperly disposing of sensitive data).

[84] *See* United States v. Stulock, 308 F.3d 922, 924 (8th Cir. 2002) ("[W]hen a computer file is deleted, the contents of the file are not irretrievably lost."). "The space occupied by the file is flagged as available, and until new data is stored in that location the deleted file can be recovered using an undelete tool." *Id.*

[85] *See* Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 29 (2004) (explaining that deleting a file from a computer does not permanently remove the file, as well as exploring the ethical issues regarding this problem).

[86] *See, e.g.*, Will Knight, *'Cleaned' Hard Drives Reveal Secrets*, NEWSCIENTIST, Jan. 16, 2003, *available at* http://www.newscientist.com/article.ns?id=dn3274 (pointing out how researchers employed simple techniques to recover data off hard drives after they had been reformatted). The techniques were so successful that the researchers were able to collect over 6000 credit card numbers, most from a hard drive once used in an automated teller machine. *Id.*

[87] *See generally* Privacy Rights ClearingHouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited May 20, 2008) (providing a detailed, chronological list of reported privacy violations stemming from computer theft, data breaches, and improper disposal methods).

[88] *See generally id.* (providing a detailed, chronological list of reported privacy violations stemming from computer theft, data breaches, and improper disposal methods).

[89] *See* Tom Spring, *Hard Drives Exposed*, PC WORLD MAG., Apr. 3, 2003, *available at* http://www.pcworld.com/article/id,110012-page,1/article.html (exposing several stories of computer users losing sensitive data by improperly disposing of old hard drives).

sources, eBay, city dumps, and small businesses.[90] As Garfinkel notes, people discard "broken" hard drives that frequently can be restored by unconventional procedures.[91] In a similar project, a group of reporters for *PC World Magazine* found a treasure trove of computers with vulnerable data during an excursion in Boston.[92] One computer, previously owned by a Boston-area attorney, contained, among other files, bank account numbers and draft legal documents.[93]

As illustrated by the data retrieval examples above, many individuals (and undoubtedly many attorneys as well) do not know what is required to permanently remove data from a computer, or wrongly assume that data cannot be retrieved from a broken hard drive. What if a computer vendor promises to scrub the hard drives?[94] How does a law firm ensure that confidential client data is not present on discarded machines?[95]

Having examined the possible scenarios of unintended technological disclosure, we turn to constructing a framework that attorneys should implement to fulfill their obligation to reasonably guard their clients' confidences in a technological context.

[90] *See* Simson L. Garfinkel & Abhi Shelat, *Remembrance of Data Passed: A Study of Disk Sanitization Practices*, 1 IEEE SEC. & PRIVACY 17, 24 (2003), *available at* http://www.computer.org/portal/cms_docs_security/security/v1n1/garfinkel.pdf (reviewing and summarizing the research of the authors, who were able to obtain numerous hard drives from various sources and harvest the sensitive data contained on many of them, despite their previous owners' attempts to clear such data).

[91] *See* Posting of Simson Garfinkel to Technology Review, http://www.technologyreview.com/blog/garfinkel/17609/ (May 25, 2007) (describing how data from supposedly broken hard drives may be retrieved by placing the device in the freezer overnight).

[92] *See* Tom Spring, *Hard Drives Exposed*, PC WORLD MAG., Apr. 1, 2003, http://www.pcworld.com/article/id,110012-page,1/article.html ("An examination of ten used hard drives we bought or salvaged in the Boston area disclosed a wealth of sensitive data. On all but one of them, we found data, including confidential business, medical, and legal records; Social Security, credit card, and bank account numbers; e-mail . . . .").

[93] *See id.* (reporting the contents of a salvaged PC previously owned by an area attorney).

[94] *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 5.3 (2007) (explaining that a lawyer must take reasonable steps to ensure that nonlawyers employed by the attorney act in compliance with the professional rules).

[95] The most effective method of preventing others from retrieving confidential information is the physical destruction of the hard drive. *See* Kim Komando, Microsoft, Clean the Hard Drive Before Dumping Your PC, http://www.microsoft.com/australia/smallbusiness/issues/technology/protect/harddrive.mspx (last visited May 20, 2008) ("The only absolute and assured way of protecting your data is to destroy the hard drive.").

IV. REASONABLE MEASURES TO PROTECT CONFIDENCES

The legal profession has begun to educate its practitioners about confidentiality issues involving the use of technology.[96] At a minimum, every attorney should review any relevant technology-related publications by the American Bar Association,[97] state and local continuing legal education providers,[98] academics,[99] and government agencies.[100] Technology changes rapidly, and while attorneys are quite busy keeping up with their own cases and substantive developments in their particular practice areas, it is now likely that maintaining some familiarity with technological advances is going to be part of the "reasonableness" required to guard client confidences.[101]

[96] *E.g.*, Nathan Brooks, *Information Privacy*, 54 FED. LAW., Sept. 2007, at 4 (dedicating the entire issue of the publication to information privacy). However, while the articles therein offer attorneys an excellent summary of developing law in this area, other publications provide little or no practical advice on the application of these standards. *See* Ariz. Bar Ass'n Comm. on the Rules of Prof'l Conduct, Op. 05-04 (2005) (noting the many ethical issues tied to electronic storage of client information).

[97] *See generally* American Bar Association Legal Technology Resource Center, FYI: For Your Information, http://www.abanet.org/tech/ltrc/fyidocs/ (last visited May 20, 2008) (providing advice to attorneys for a variety of technical concerns including computer disposal, wireless networking, and data backup).

[98] *See generally* The Law Practice Management Program of the State Bar of Texas, Disaster Preparedness: Securing the Firm, MCLE Course No. 900023298 (Sept. 2007); John Podvin & Irene Kosturakis, *Identity Theft: How to Protect Your Practice and Clients*, State Bar of Texas (via webcast) May 10, 2006; Merri A. Baldwin & Kathryn Fritz, *Information Ethics for Lawyers: Information Management—Knowing What You Have, Why You Have It, and How to Dispose of It (Without Breaking the Law or Violating Ethical Duties)*, 11253 PRACTICING L. INST. 637, 643 (2007) (discussing steps in preserving all types of documents including "'deleted' files and file fragments recovered from forensically captured image of hard discs"). These sources stand out as excellent examples of CLE courses regarding proper measures to protect client confidences.

[99] *See, e.g.*, Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 1 (2004) (recognizing potential risks with digital data and suggesting measures attorneys should take to avoid violating rules of professional conduct); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 932–69 (2007) (proposing approaches for protection of data leaks).

[100] *See generally* United States Computer Emergency Readiness Team, Cyber Security Tips, http://www.us-cert.gov/cas/tips (last visited May 20, 2008) (laying out in easy-to-click categories how to protect oneself from cyber threats). Many times, the practices of government agencies are considered behind the times. However, when it comes to security, especially cyber security, certain federal government agencies tend to lead commercial practices by a number of years. This may be due to the critical concerns of national security.

[101] *See* Ariz. Bar Ass'n Comm. on the Rules of Prof'l Conduct, Op. 05-04 (2005) (deciding that an attorney is required to take reasonable steps to prevent any client information stored on digital sources from being stolen or lost). It is not out of the

It is also important to recognize that something beyond basic technological understanding may be required when an attorney or a firm is involved in a particularly large or important undertaking.[102] The extent of technological protection afforded by a solo practitioner in a small civil case might not be reasonable if employed by an attorney or law firm handling a large corporate merger or a death penalty case.[103] Some minimum protection should be afforded by all attorneys, but additional safeguards may be needed to satisfy the reasonableness requirement where the risks are heightened.[104]

A review of judicial opinions, ethics opinions, and the Model

question to presume that this level of reasonableness requires underlying knowledge to competently use such data storage; that is, the attorney must have the capability to store information without allowing a third party to access that data. *Id.* (discussing how the lawyer may employ certain technological safeguards to protect confidential materials).

[102] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 ("Special circumstances, however, may warrant special precautions [to protect transmissions of confidential information]. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.").

[103] In general, a lawyer must exercise "reasonable diligence" in representing a client, which is determined, in part, by the importance of the matter to the client. This, in turn, is a factor of the client's own assertions as to the importance of the matter, as well as the attorney's assessment as to the impact of the matter upon the client's affairs. *See* RESTATEMENT OF THE LAW GOVERNING LAWYERS § 52 cmt. c (2007) (listing the various factors that an attorney must consider in order to meet the standard of reasonable diligence). Moreover, attorneys with a particular area of concentration or skill might be held to have a higher duty to clients than those who lack this expertise. SUSAN SAAB FORTNEY & VINCENT R. JOHNSON, LEGAL MALPRACTICE LAW: PROBLEMS AND PREVENTION 71 (2008). Obviously, a death penalty case would require great diligence in many areas, including the use of technology. "Computer problems" were cited by defense attorneys for Michael Richard as the reason they requested that the Texas Court of Criminal Appeals remain open twenty to thirty minutes later than the 5 p.m. closing time on September 25, 2007. Chuck Lindell, *Criticism Grows for Judge over Execution,* AUSTIN AM. STATESMAN, Oct. 11, 2007, at B1. The request was denied; the after-hours appeal was not accepted by the court, and Mr. Richard was executed. *Id.*

[104] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (commenting that special precautions may be necessary in special circumstances to protect transmissions containing confidential information); *see also* Ariz. Bar Ass'n Comm. on the Rules of Prof'l Conduct, Op. 05-04 (2005) (noting the ethical requirements of Arizona lawyers to retain outside assistance if they are unable to adequately meet the needs of protecting their clients' confidences in electronic communications and data storage). Analogously, where the scope of litigation expands, so too must the extent to which an attorney must protect any digital resources; thus, under the Arizona Bar Committee's ruling, highly complex litigation would require more attention to electronic data than would a simple civil suit.

Rules is not particularly helpful in this regard.[105] Most of the case law regarding inadvertent disclosure of client confidences arises in the context of discovery and is inconsistent regarding the issue of whether the attorney-client privilege is waived under these circumstances.[106] The Model Rules of Professional Conduct probably allow the attorney-recipient of such information to use it, after notifying the unintending sender of the error.[107] Arguably

[105] *See* Richard J. Heafey, *Return to Sender?: Inadvertent Disclosure of Privileged Information*, 28 AM. J. TRIAL ADVOC. 615, 615 (2005) (noting that even the Model Rules can directly conflict with ethics opinions from the same organization—the ABA).

[106] *See id.* at 615–16 (stating that the reported court decisions do not provide clear guidance regarding the issue of waiver).

[107] *See* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2007) (detailing the required conduct for a lawyer who inadvertently receives information). "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." *Id.* The comments to the rule then "punt" on the use attorneys may make of such material:

> [1] Responsibility to a client requires a lawyer to subordinate the interests of others to those of the client, but that responsibility does not imply that a lawyer may disregard the rights of third persons. It is impractical to catalogue all such rights, but they include legal restrictions on methods of obtaining evidence from third persons and unwarranted intrusions into privileged relationships, such as the client-lawyer relationship.
>
> [2] Paragraph (b) recognizes that lawyers sometimes receive documents that were mistakenly sent or produced by opposing parties or their lawyers. If a lawyer knows or reasonably should know that such a document was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person. For purposes of this Rule, "document" includes e-mail or other electronic modes of transmission subject to being read or put into readable form.
>
> [3] Some lawyers may choose to return a document unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer. See Rules 1.2 and 1.4.

Id. 4.4 cmts. 1–3.

This rule and its comments replaced the prior view of the ABA requiring the receiving attorney to refrain from examining the confidential information, notify the attorney who inadvertently sent it, and follow that attorney's instructions for the return or disposal of the document. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992).

the best way to structure a plan to protect client information is to use experts in the area of information assurance.[108] Those involved with effective information security programs would take a broad perspective on the obligations of attorneys to safeguard client information.[109] It is likely that their views will become the standard for reasonableness expected of attorneys, particularly in view of new state statutes discussed below.[110] We will approach this discussion the way these consultants would, by discussing prevention, detection, and remediation.[111]

A. *Prevention*

The first question the information assurance consultant would ask of an attorney is whether the attorney can effectively and

[108] *See* Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 33–34 (2004) (discussing ethical concerns and possible solutions regarding attorneys' use of technology). Professor Beckerman-Rodau suggests that hiring a consultant might be required "to fully understand the potential risks of reliance on technology as a prerequisite to evaluating the reasonableness of conduct." *Id.* at 10; *see also* Ariz. Bar Ass'n Comm. on the Rules of Prof'l Conduct, Op. 05-04 (2005) (imposing an ethical requirement to hire a consultant if the attorney personally lacks the requisite competence to secure client information).

[109] *See* Certifications, http://www.issa.org/Resources/Industry-Certifications.html (last visited May 20, 2008) (listing information security certifications by topic area). Within the information security community, there are several organizations that provide certification based on experience in the industry and successful testing. *Id.*

[110] *See, e.g.*, COBIT, http://www.isaca.org/Template.cfm?Section=COBIT6 (last visited May 20, 2008) (providing an overview of the Control Objectives for Information and related Technology (COBIT) framework for auditing information resources); Perkins Coie, Security Breach Notification Chart, http://www.perkinscoie.com/files/upload/securitybreach.pdf (last visited May 20, 2008) (charting security breach legislation enacted in jurisdictions throughout the United States).

[111] *See* 16 C.F.R. § 314 (2007) (outlining the standards for keeping customer information safe). It is likely that federal and state statutes and regulations may codify some of these good practices and eventually make them binding upon attorneys. *See id.* § 314.1 (describing the scope for safeguarding customer information). The Federal Trade Commission (FTC) has implemented safeguard rules setting forth a standard of care to protect customer records. *Id.* These rules are applied to financial institutions the FTC regulates and include at least three important requirements. *Id.* §§ 314.1–.4. First, designate a coordinator for the information security system. *Id.* § 314.4. Second, conduct a risk assessment involving personnel training, information systems and detection, prevention, and response to breaches. 16 C.F.R. § 314.4 (2007). Third, design and implement safeguards and regularly analyze the effectiveness of those safeguards, and update the entire security program as necessary. *Id.* *See generally* SECTION OF SCI. & TECH. LAW, LAW PRACTICE MGMT. SECTION, INFORMATION SECURITY FOR LAWYERS AND LAW FIRMS 5–8 (Sharon D. Nelson et al. eds., 2006) (suggesting practices for physical security in law firms).

appropriately prevent unauthorized access to the client's information.[112] This requires an assessment of the physical environment (including people), the electronic environment, and the relative value of the information.[113]

The physical environment is that which can be seen and readily observed, and includes the physical structures and people in the environment.[114] The physical structure includes the tangibles—the building, offices, walls, windows, and other physical assets (e.g., computers, paper files)—contained within.[115] Physical security secures the physical environment against intrusion, which can be either physical (i.e., someone breaking into the office space or surreptitiously listening in to conversations through a wall) or electronic (e.g., listening in through electronic means, viruses on computers, or intercepting e-mails).[116] Attorneys may want to secure walls and windows, not because they are valuable and may be stolen, but because they allow access to what is inside.[117]

Included within the physical environment are people and personnel. Unfortunately, people, some with only the best of intentions, are often the weakest link in the security chain.[118] For example, many significant intrusions to computers begin with social engineering. Attorneys will need to work with security consultants to screen potential employees and educate current

[112] *See* Ariz. Bar Ass'n Comm. on the Rules of Prof'l Conduct, Op. 05-04 (2005) (advising that attorneys have an obligation to ensure that clients' files are protected from any potential electronic threat).

[113] Telephone Interviews with Keith Frederick, Founder and President, Computer Network, Inc., in College Station, Tex. (Apr. 7, 2006, Sept.—Nov. 2007, Sept. 28, 2007). Mr. Frederick's forthcoming book will discuss integrating physical and electronic security as an effective business process.

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] Brenna G. Nava, Comment, *Hurricane Katrina: The Duties and Responsibilities of an Attorney in the Wake of a Natural Disaster*, 37 ST. MARY'S L.J. 1153, 1156–61 (2006) (discussing the various issues that come to pass after a natural disaster, the lawyer's standard of care during that time, and a proposal for a paperless system to effectively prepare and recover from such a disaster).

[118] *See generally* United States v. Miller, 984 F.2d 1028, 1029 (9th Cir. 1992) (affirming the conviction of Richard Miller as the first FBI officer ever to be found guilty of espionage); United States v. Walker, 796 F.2d 43, 45 (4th Cir. 1986) (affirming the conviction of Arthur James Walker for "transmittal of classified United States defense information to agents of the Soviet Union"); Ames v. United States, 155 F. Supp. 2d 525, 525–27 (E.D. Va. 2000) (denying Aldrich H. Ames's petition to vacate his guilty plea of "conspiracy to defraud the United States" and "conspiracy to commit espionage").

ones regarding these dangers, to prevent the damage from an insider threat.[119]

The distinction between physical and electronic becomes important when one considers the ways access can be obtained, possibly through a combination of intrusions against the physical and electronic environments.[120] The nature of security is that it is tempting to emphasize one environment over the other or neglect the fact that it is the integration of the environments that must be secured.[121] Consider the electronic environment of the computer system, including the mode of communication (wireless or hard-wired), the network, and the computers themselves. Some companies protect the electronic environment without considering that one of the most effective means of gaining access to computer data is to steal the computer—a physical intrusion.[122] In fact, laptop thefts are one of the most critical vulnerabilities that can be exploited, including theft from hotel rooms, "smash and grab" thefts from automobiles, and switching machines at an airport.[123]

Finally, to formulate a plan for preventing access to client information, the consultant would need to have some idea of the relative value of the information.[124] The more valuable the information, the greater the obligation of the attorney to secure it, and the more sophisticated prevention systems would need to be

[119] KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 245, 324 (2002).

[120] Telephone Interviews with Keith Frederick, Founder and President, Computer Network, Inc., in College Station, Tex. (Apr. 7, 2006, Sept.–Nov. 2007, Sept. 28, 2007).

[121] *Id.*

[122] *See* Absolute Software, Computer Theft & Recovery Statistics, http://www.absolute.com/resources/computer-theft-statistics-details.asp (last visited May 20, 2008) (stating that computer theft or loss accounts for 54% of breaches related to identify theft and that 47% of surveyed computer security professionals indicated a laptop theft sometime in the last twelve months); *see also* Philip Cornford, *The Brazen Airport Computer Theft That Has Australia's Anti-terror Fighters Up in Arms*, SYDNEY MORNING HERALD, Sept. 5, 2003, http://www.smh.com.au/articles/2003/09/04/ 1062548967124.html (describing an incident at the Sydney International Airport where two men stole two mainframes).

[123] *See* Nationwide, Curb 'Smash-and-Grab' Theft, http://www.nationwide.com/ newsroom/smash-and-grab.jsp?oys=car-theft&pos=archive (last visited May 20, 2008) (addressing "smash and grab" theft and listing laptops as among the items vulnerable to such thefts).

[124] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2007) (discussing instances in which a lawyer should take special precautions to prevent a client's information from "coming into the hands of unintended recipients").

implemented.[125]

To satisfy the requirements of Model Rule 1.6, we recommend that attorneys conduct a prevention analysis by working with a qualified consultant[126] to implement a security plan, including a plan for backing up data[127] and destroying files where appropriate.[128] These preventive measures represent a significant step towards fulfilling the attorney's obligation to reasonably protect the client's confidential information.[129]

B. *Detection*

How does an attorney know if a security breach has occurred? Some breaches might be obvious, particularly if the breach involves an alteration of the physical environment.[130] Broken or unlocked doors and windows, missing computers, and other related physical changes would give cause for the attorneys to call in the technology consultant to determine the nature and extent of

[125] *Id.*; Ariz. Bar Ass'n Comm. on the Rules of Prof'l Conduct, Op. 05-04 (2005).

[126] *See* CERT, CERT-Certified Computer Security Incident Handler, http://www.cert.org/certification/ (last visited May 20, 2008) (outlining a certification program for individuals with experience handling computer security who wish to "achieve[] the knowledge, skills, and abilities to be a highly successful security professional").

[127] *See* SearchStorage.com, Backup Basics: Three Backup Plans, Oct. 2, 2003, http://searchstorage.techtarget.com/tip/1,289483,sid5_gci930542,00.html (outlining backup plan basics which advise users to backup files daily, perform a full backup weekly, and test the backup process monthly or quarterly, as well as off-site storage and removable data storage media).

[128] *See* National Association for Information Destruction, Inc., NAID: Membership Info, http://www.naidonline.org/join/membership.html (last visited May 20, 2008) (outlining the mission of this international association for companies that provide services to destroy information: "to educate business, industry and government of the importance of destroying discarded information and the value of contract destruction services").

[129] *See* MODEL RULES OF PROF'L CONDUCT R. 1.0(h) (2007) ("'Reasonable' or 'reasonably' when used in relation to conduct by a lawyer denotes the conduct of a reasonably prudent and competent lawyer."). A "[r]easonable belief" refers to the fact "that the lawyer believes the matter in question and that the circumstances are such that the belief is reasonable." *Id.* 1.0(i). "Reasonably should know" is used to "denot[e] that a lawyer of reasonable prudence and competence would ascertain the matter in question." *Id.* 1.0(j).

[130] *See* Mary Brandel, *Data Scandal: Do You Know How to Respond to the Inevitable Security Breach? You'd Better*, COMPUTERWORLD, Oct. 3, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,105065,00.html (discussing the importance of immediate response, teamwork, and deliberate speed needed when responding to a security breach).

loss.[131] A change in personnel, particularly if someone leaves under unpleasant circumstances, would also give cause for the consultant to review and reset security measures.[132]

Unfortunately, many breaches, particularly those involving the electronic environment, may not be readily apparent.[133] Files can be copied and transferred to compact discs, flash drives, or other machines. The very nature of the ongoing acceleration of the transfer of data will probably increase the likelihood of data theft. No system now, or in the future, is or ever will be, totally secure.[134] Unfortunately, the first sign of data loss might be when an adversary suddenly seems to know confidential communications or litigation strategies.

Before that point, however, the most reasonable method of both prevention and detection is a regular auditing process involving internal personnel and external security consultants.[135] Auditing, in this sense, means determining the status of the security system and producing a snapshot of the current security.[136] The

[131] *See* CERT, CERT-Certified Computer Security Incident Handler, http://www.cert.org/certification/ (last visited May 20, 2008) (offering a certification program example for experienced individuals in the computer security field).

[132] *See* Brian Contos, *Enemy at the Watercolor: Inside IT Threats Increasing*, TECHNEWSWORLD, Apr. 13, 2006, http://www.technewsworld.com/story/49652.html (recognizing that companies must understand that threats from inside their organization may be more dangerous than threats from outside the organization). *But see* Larry Downes, *Shareholder Values*, CIO INSIGHT, Nov. 6, 2006, at 2, http://www.cioinsight.com/c/a/Past-Opinions/Shareholder-Values/ (pointing out that while companies may have individuals devoted to finding sources of information leaks, it should take care not to go about it in appropriate ways).

[133] *See* Sharon Gaudin, *Asking for Trouble: Most Companies Don't Have Plans to Handle Data Breach*, INFO. WK., May 22, 2007, http://www.informationweek.com/story/showArticle.jhtml?articleID=199701313 (reporting the results of a survey done by the Ponemon Institute of over 700 security and IT managers finding "[a]round 85% of IT and security managers say they've suffered a data breach, but less than half have a plan in place for when it happens again").

[134] *See* Alison Fitzgerald, *Careless Workers Expose IRS Data*, SEATTLE TIMES, Aug. 4, 2007, at E4 (describing an incident where auditors posing as help-desk technicians persuaded IRS employees to give out their passwords and change them to ones suggested by the auditors); *see also* Steve Brewer, *Programmer who Allegedly Broke into NASA Computers is Indicted*, HOUS. CHRON., Apr. 27, 2007, at 21 (explaining that a hacker obtained encrypted passwords and "used an Internet password-cracking tool" to decipher the passwords and gain entry to NASA computers).

[135] *See* RICK LEHTINEN, DEBORAH RUSSELL & G.T. GANGEMI SR., COMPUTER SECURITY BASICS 108 (2006) (describing a security audit and noting possible problem areas). "A *security audit* is a search through your system for security problems and vulnerabilities." *Id.*

[136] *See* NATIONAL STATE AUDITORS ASSOCIATION & THE U.S. GENERAL

consultants' goal is to determine what must be done to improve security based on the snapshot assessment and to develop a migration plan.[137] Auditing is a necessary component of the security process as a way to monitor status constantly.[138] Another use of auditing is to close the gap between what is intended and what is actually practiced.[139] For example, prevention of insider threats might include an auditing exercise to determine if an employee would allow an outsider—through social engineering—to breach security. Although the employee has been trained, the efficacy of that training should be tested with an actual exercise. Throughout the security process, auditing is used to determine not only what might happen, but also to identify the weak links in the process.[140]

ACCOUNTING OFFICE, A JOINT INITIATIVE: MANAGEMENT PLANNING GUIDE FOR INFORMATION SYSTEMS SECURITY AUDITING 6 (2001), http://www.gao.gov/special.pubs/mgmtpln.pdf ("IS security auditing involves providing independent evaluations of an organization's policies, procedures, standards, measures, and practices for safeguarding electronic information from loss, damage, unintended disclosure, or denial of availability."); ISACA, http://www.isaca.org/Content/NavigationMenu/About_ISACA/Overview_and_History/Overview_and_History.htm (last visited May 20, 2008) (providing an overview and history of ISACA, an organization composed of security and auditing professionals).

[137] *See* NATIONAL STATE AUDITORS ASSOCIATION & THE U.S. GENERAL ACCOUNTING OFFICE, A JOINT INITIATIVE: MANAGEMENT PLANNING GUIDE FOR INFORMATION SYSTEMS SECURITY AUDITING 24 (2001), http://www.gao.gov/special.pubs/mgmtpln.pdf (describing the role of consultants relating to information security). "Consultants may offer immediate capabilities not otherwise available without considerable start-up time and cost." *Id.*

[138] *See* RICK LEHTINEN, DEBORAH RUSSELL & G.T. GANGEMI SR., COMPUTER SECURITY BASICS 108 (2006) (discussing the importance of conducting audits to evaluate security systems). "It's a good idea to check on the security of your system by performing periodic security audits." *Id.*

[139] *See* DAVID CODERRE, GLOBAL TECHNOLOGY AUDIT GUIDE CONTINUOUS AUDITING: IMPLICATIONS FOR ASSURANCE, MONITORING, & RISK ASSESSMENT 4 (2005), http://www.acl.com/pdfs/IIA_GTAG-May05.pdf (explaining that the other component of continuous auditing, besides risk assessment, is to focus on control deficiencies). In essence, auditing aims to assure that controls that were developed in order to achieve a particular purpose are operating efficiently. *Id.* at 5. "Continuous control assessment will allow internal auditors to assess the adequacy of management monitoring activities and provide . . . assurance that the controls are working effectively and that the organization can respond quickly to correct deficiencies that arise." *Id.*

[140] *See id.* at 4 (specifying control assessment and risk assessment are the two main components to continuous auditing). Control assessment focuses on whether the processes that are in place are suffering any deficiencies, and risk assessment focuses on processes that are "experiencing higher than expected levels of risk." *Id.*

C. *Remediation*

In addition to the reasonableness requirement set out in the Model Rules, recent legislation has added to attorneys' obligations. At the time of this writing, thirty-five states require businesses to notify their customers or clients if there is a security breach involving sensitive personal information.[141] These laws generally apply to any business maintaining the information of a resident of the state which enacts the statute.[142] Thus, an attorney might be subject to laws of various states depending upon the domiciles of the individuals whose sensitive personal information the attorney possesses.[143] Further complicating the matter is the fact that these laws are not completely uniform.[144] To understand the remediation obligations and some questions concerning the applicability of this legislation, consider the impact and applicability of Texas statutes, patterned after similar legislation in California.

In 2007, the Texas 80th Legislature enacted the following law as part of the Texas Business and Commerce Code:

> Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[145]

[141] David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 No. 7 INTELL. PROP. & TECH. L.J. 5, 5 (2007). An interesting assertion in Silverman's article is that these laws may reach beyond a state's borders to anyone maintaining personal information in any state, thus making the holder of information potentially subject to the strictest law. *Id.* at 7. *See generally* State Breach and Freeze Laws, http://www.pirg.org/consumer/credit/statelaws.htm#breach (last visited May 20, 2008) (providing links to breach laws of thirty three states).

[142] *See, e.g.*, TEX. BUS. & COM. CODE ANN. § 521.053(b) (Vernon Supp. 2007) (requiring someone who conducts business in Texas to notify any resident of this state when a breach occurs). Notification is required if the personal information "was, or is reasonably believed to have been, acquired by an unauthorized person." *Id.* § 521.053(c).

[143] *See id.* § 521.053(b) (implying that a lawyer with a client in Texas, whose personal information was accessed, would be subject to the laws of Texas).

[144] *See* David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 No. 7 INTELL. PROP. & TECH. L.J. 5, 5 (2007) (describing the differences among the states and their respective notification laws relating to security breaches).

[145] Act of May 15, 2007, 80th Leg., R.S., ch. 885, § 2.01, 2007 Tex. Gen. Laws 1905, 1906 (codified at TEX. BUS. & COM. CODE ANN. § 521.053(c) (Vernon Supp. 2007)).

The law defines sensitive personal data as:

> "Sensitive personal information" means, subject to Subsection (b), an individual's first name or first initial and last name in combination with any one or more of the following items, if the names and the items *are not encrypted*:
>
> (A) social security number;
> (B) driver's license number or government-issued identification number; or
> (C) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.[146]

This statute seems to impose a notification requirement on any attorney who loses enough confidential client information to risk theft of the victim's identity.[147] Because many discovery documents have, at a minimum, identifying information such as a social security number or driver's license number,[148] this law seems to apply to more circumstances than most attorneys are probably aware.[149]

For example, if an attorney loses, either by theft or accident, a laptop, PDA, flash drive, or CD containing clients' sensitive personal information, the attorney must contact affected clients

[146] TEX. BUS. & COM. CODE ANN. § 521.002(a)(2) (Vernon Supp. 2007) (emphasis added). Subsection (b) excludes any "publicly available information that is lawfully made available to the public from the federal government or state or local government." *Id.* § 521.002(b).

[147] *See id.* § 521.053(c) (explaining that an individual who maintains a data system with personal information has a duty to notify the owner of the personal information when a breach occurs and sensitive information is reasonably believed to have been compromised).

[148] *Id.* § 521.002(a)(2)(A)–(B).

[149] *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 933 (2007) ("[Model One] is marked by a low threshold for notification" and, as such, it would not be surprising that many Texas attorneys are in situations where the laws could be implicated). Professors Schwartz and Janger have classified the Texas statute in their terms as a "Model One" law, exemplified by California Senate Bill 1386, on which the Texas statute is modeled (if not explicitly copied). *Id.* at 933. The Model One characterization, as a pure notification model, has a "low threshold for notification" and "lacks a coordination infrastructure to mitigate the harm flowing from a data security incident." *Id.* Their article makes an argument for even more effective and useful models than Model One for notifying clients of data security breaches. *Id.* at 933–35.

"immediately after discovering the breach,"[150] even though the attorney may have all files backed up and neither the clients nor the attorney would notice any disruption in their work. This is true because when a breach occurs, the information has been acquired by a third party who, by definition, is an unauthorized person.[151]

Theoretically, attorneys could avoid the statute by encrypting the sensitive personal information.[152] The term "encryption," however, is not particularly helpful. While encryption is generally understood to be the means of translating data into something that is not understandable by those who are not authorized access, there are no mandatory, industry-wide encryption standards.[153] Some vendors may use encryption techniques based on the vendors' proprietary algorithms.[154] Peter Coffee, a well-known writer on computer security issues, took issue with an encryption

[150] TEX. BUS. & COM. CODE ANN. § 521.053(c) (Vernon Supp. 2007). Most lawyers do not realize that this type of legislation might apply to them. As generally acceptable and reasonable standards become more pervasive, lawyers will find themselves held to the generally accepted standard. These standards are developing through application of ethical rules. For example, Opinion No. 05-04 by the Arizona Bar Association Committee on the Rules of Professional Conduct discusses the ethical duty of law firms in Arizona to protect client information, especially data stored in electronic format. Ariz. Bar Ass'n Comm. on the Rules of Prof'l Conduct, Op. 05-04 (2005). A standard is emerging through statutes and regulations. *See* 16 C.F.R. § 314.3(a) (2007) (requiring maintenance of "a comprehensive information security program"); *see also* David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 No. 7 INTELL. PROP. & TECH. L.J. 5, 5 (2007) (stating that at least thirty-five states have enacted notification laws concerning data security breaches).

[151] TEX. BUS. & COM. CODE ANN. § 521.053(b) (Vernon Supp. 2007).

[152] *See* RICK LEHTINEN, DEBORAH RUSSELL & G.T. GANGEMI SR., COMPUTER SECURITY BASICS 141 (2006) (defining encryption as "transform[ing] original information . . . into transformed information" so that others cannot read or understand the original information).

[153] *See id.* at 36 (outlining the movement toward creating a standard encryption algorithm and the movement's subsequent demise). Today, a host of powerful encryption tools are readily available as open source programs. *Id.*; *cf.* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197: ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES) (2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (announcing the adoption of the Rijndael algorithm as the federal government's Advanced Encryption Standard (AES)). Over the past seven years numerous vendors have adopted AES as the de facto standard encryption algorithm.

[154] *See* Winn Schwartau, *To Hell with Proprietary Encryption Algorithms*, NETWORK WORLD, Aug. 27, 2001, http://www.networkworld.com/columnists/2001/0827schwartau.html (explaining that vendors continue to create proprietary algorithms for their encryption processes, which are vulnerable to hackers).

provision in a recent California bill.[155] He pointed out that an encryption is not a yes-or-no attribute and explained that "[w]eak crypto algorithms or poor implementations of good algorithms or poorly administered deployments of even robust crypto products are equally hollow in their promises of protection."[156] As a result, many attorneys would encounter difficulty in ascertaining whether their files are encrypted, and if so, how "strong" the encryption is.[157]

There are other questions raised by state statutes, including issues related to whether or not notice of a breach is even required.[158] The complexity of these issues once again points to the need for the attorney to utilize a competent consultant in planning and implementing any remediation scheme.[159]

Moreover, attorneys will likely face tort liability for security breaches.[160] In a recent article, Professor Vincent Johnson

[155] *See* Peter Coffee, *Computer Literacy Isn't Kid Stuff*, EWEEK.COM, May 2, 2006, http://www.eweek.com/c/a/IT-Management/Computer-Literacy-Isnt-Kid-Stuff/ (taking exception to the California legislature's use of the word "encryption").

[156] *Id.*

[157] How strong is an encryption? The word "CAT" can be encrypted "BZS" by substituting a letter with the previous letter in the alphabet. That is how IBM became HAL in the movie 2001 Space Odyssey. In a technical sense, this is encrypted data, although the encryption is extremely weak. Thus, attorneys cannot simply rely on a software vendor's vague assurance to encrypt the data. On the other hand, the level of confidence warranted in a vendor using a known and widely accepted standard—such as AES—would be much higher.

[158] *See, e.g.*, IND. CODE ANN. § 24-4.9-2-2 (LexisNexis 2007) (providing exceptions to Indiana's notification requirements). One particularly disturbing aspect of the Indiana statute is that it renders notice to affected parties unnecessary if there is unauthorized access to a portable electronic device "if access to the device is protected by a password that has not been disclosed." *Id.* However, assuming that the attacker has access to the device or file, it is sometimes possible to break passwords. In the case of laptops, the hard drive can be removed from a password-protected machine and accessed by another machine, unless the contents of the hard drive are encrypted. *See* Donna L. Beatty, *Malaysia's "Computer Crimes Act 1997" Gets Tough on Cybercrime but Fails to Advance the Development of Cyberlaws*, 7 PAC. RIM L. & POL'Y J. 351, 373 (1998) ("Virus how-to guides and code generators are available on underground world-wide Web sites and bulletin boards. System passwords can easily be broken using software programs such as 'CRACK'—a program freely available on the Internet.").

[159] *See* Mark Bassingthwaighte, *Ten Technology Traps and How to Avoid Them*, W. VA. LAW., Sept.–Oct. 2006, at 34 (discussing ten technology traps and how attorneys can avoid them); *see also* Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 14–15 (2004) (suggesting the use of a single password system).

[160] *See* John D. Comerford, *Competent Computing: A Lawyer's Ethical Duty to Safeguard the Confidentiality and Integrity of Client Information Stored on Computers and*

analyzed the growing concerns relating to cyber security, and although his article did not focus on attorney-client obligations, there is no reason to assume that attorneys are immune to liability under the principles he discusses.[161]

Attorneys should expect that some breaches will occur and make plans to minimize the impact on their clients, even where statutes do not now require it. Attorneys working with consultants should develop plans to copy data and store it securely off-site in order to assist in remediation efforts following a physical breach or destruction of data.

V. CONCLUSION

Attorneys have an ethical obligation to act in a reasonable fashion to protect their clients' confidences.[162] This includes the obligation to protect data stored electronically from unintended disclosure either through inadvertent release of the information or from failure to secure the data against unauthorized access.[163] Attorneys must act reasonably to prevent, detect, and remedy security breaches.[164]

State statutes are becoming more specific and are imposing

Computer Networks, 19 GEO. J. LEGAL ETHICS 629, 642 (2006) (discussing possible malpractice liability for failing to take appropriate precautions).

[161] *See generally* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 296–310 (2005). Courts have found liability for actual damages where plaintiffs proved how their identities were stolen. *See, e.g.*, Daly v. Metro. Life Ins. Co., 4 N.Y.S.2d 887, 893 (N.Y. Sup. Ct. 2004) (holding that a life insurance company had a duty to protect its client's private information from theft); Bell v. Mich. Council 25 of the Am. Fed'n of State, County, and Mun. Employees, No. 246684, 2005 WL 356306, at *5 (Mich. Ct. App. Feb. 15, 2005) (per curiam) (holding that a union was liable for the identity theft of its members' information because it "knew confidential information was leaving its premises and no procedures were in place to ensure the security of the information").

[162] *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2007) ("A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)."); TEX. DISCIPLINARY R. PROF'L CONDUCT 1.05(b), *reprinted in* TEX. GOV'T CODE ANN., tit. 2, subtit. G app. A (Vernon 2005) (TEX. STATE BAR. R. art. X, § 9) ("[A] lawyer shall not knowingly [r]eveal confidential information of a client . . . .").

[163] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2007).

[164] *See id.* 1.6 cmt. 17 (setting forth a lawyer's duty to take reasonable steps to prevent unauthorized access to privileged information); *see also* Andrew Berkerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 27–32 (2004) (discussing possible security breaches and ways to avoid them).

greater obligations on attorneys to provide notice to the client when loss of personal information has occurred.[165] Some of these statutes create a civil cause of action against attorneys[166] and all of them undoubtedly raise the bar on what an attorney is reasonably required to do when a breach occurs, thus implicating a higher ethical standard. After all, it is certainly reasonable to comply with mandatory state statutes and not reasonable to violate them.[167]

How do attorneys meet these obligations? Most attorneys are not trained in the increasingly complicated area of information assurance.[168] Even if they are, they do not have the time to practice both law and information assurance on a full-time basis.[169]

Other areas of commerce and industry, however, may be making more progress in information assurance because of the new statutes and regulations requiring heightened protection of health

[165] *See, e.g.*, CAL. CIV. CODE § 1798.82(a) (West 2007) (imposing a duty to disclose a security breach); MONT. CODE ANN. § 30-14-1702 (2007) (discussing the duty to notify any resident of Montana of any breach of personal information); MONT. CODE ANN. § 30-14-1704 (2007) (defining personal information); Perkins Coie, Security Breach Notification Chart (last visited May 20, 2008), http://www.perkinscoie.com/files/upload/securitybreach.pdf (providing information regarding security breach notification laws in various jurisdictions).

[166] *See, e.g.*, CAL. CIV. CODE § 1798.45 (West 2007) (allowing a civil suit for any violation of the statute).

[167] *See* SUSAN SAAB FORTNEY & VINCENT R. JOHNSON, LEGAL MALPRACTICE LAW: PROBLEMS AND PREVENTION 15 (2008) (explaining that one area where attorneys face liability for failure to comply with statutory requirements is in the area of deceptive trade practices); *see also* Perkins Coie, Security Breach Notification Chart, http://www.perkinscoie.com/files/upload/securitybreach.pdf (last visited May 20, 2008) (discussing violations of the Consumer Fraud and Deceptive Business Practices Act). Proof of a violation of a rule or statute governing the conduct of attorneys may be considered by a trier of fact in order to understand the duty owed by the attorney but does not, of itself, create liability to a client. SUSAN SAAB FORTNEY & VINCENT R. JOHNSON, LEGAL MALPRACTICE LAW: PROBLEMS AND PREVENTION 72–73 (2008).

[168] John D. Comerford, *Competent Computing: A Lawyer's Ethical Duty to Safeguard the Confidentiality and Integrity of Client Information Stored on Computers and Computer Networks*, 19 GEO. J. LEGAL ETHICS 629, 630 (2006) ("[F]ew practicing attorneys possess the expertise necessary to effectively implement computer security measures.").

[169] *See id.* at 632 ("[B]uilding a robust computer network defense is neither cheap nor easy."). According to one author, nationwide statistics place the median attorney work week at fifty hours. Maria Pabon Lopez, *The Future of Women in the Legal Profession: Recognizing the Challenges Ahead by Reviewing Current Trends*, 19 HASTINGS WOMEN'S L.J. 53, 84 (2008). Most attorneys would likely report their work week does not leave many hours available for information assurance and practice.

care records,[170] financial matters,[171] and other areas.[172] The legal profession can learn from these industries and from professionals who are developing and implementing the necessary plans to prevent, detect, and remediate security breaches.[173]

Indeed, it appears incumbent upon attorneys to utilize this expertise. Attorneys rely on experts from any number of fields in representing their clients and managing their practices.[174] Given the risks to clients and attorneys from security breaches exposing confidential information, it appears reasonable for attorneys to employ information assistance experts to design and implement security plans and to conduct periodic audits to provide the necessary client protection and statutory compliance.[175] In addition to the immediate benefits to clients, attorneys who utilize these experts might more easily convince a factfinder, should a breach and loss occur, that the attorneys acted reasonably and did not act in an unethical, unlawful, or liability-producing fashion.[176]

[170] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 264(a), 110 Stat. 1936, 2033 (1996) (alluding to the "record keeping requirement" imposed by the statute).

[171] *See* 16 C.F.R. § 314.1 (2007) (requiring all financial institutions subject to FTC jurisdiction to protect customer information); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 269–70 (2005) (describing statutory obligations of financial institutions).

[172] Pui-Wing Tam & Robin Sidel, *Security Software's Mini-Boom*, WALL ST. J, Oct. 2, 2007, at B3 (concerning the heightened standards for credit card processing and the vendor-imposed fines in place for not adhering to these industry standards).

[173] *See* 16 C.F.R. § 314.4 (2007) (listing the elements necessary "to develop, implement, and maintain [an] information security program"); *see also* Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 33–34 (2004) (explaining that attorneys may need to hire computer personnel to protect client information).

[174] Lawyers can locate experts in bar journal publications. In some fields, expert testimony is required. Plaintiffs in legal malpractice cases ordinarily must present expert testimony establishing the standard of care. Television Capital Corp. of Mobile v. Paxson Comm'ns Corp., 894 A.2d 461, 469 (D.C. 2006) (noting that the rule requiring plaintiffs to present expert testimony to establish the standard of care in legal malpractice cases is widely followed). *But see* Hickox *ex rel.* Hickox v. Holleman, 502 So. 2d 626, 635 (Miss. 1987) (stating that the general rule requiring expert testimony to support a malpractice claim does not apply when the attorney's conduct is "negligent as a matter of law and the plaintiff is entitled to a directed verdict on liability").

[175] *See* John D. Comerford, *Competent Computing: A Lawyer's Ethical Duty to Safeguard the Confidentiality and Integrity of Client Information Stored on Computers and Computer Networks*, 19 GEO. J. LEGAL ETHICS 629, 630 (2006) (acknowledging that few attorneys possess the necessary expertise to implement the proper computer security measures on their own).

[176] A CONCISE RESTATEMENT OF THE LAW GOVERNING LAWYERS 127 (2007)

Finally, when a security breach occurs, attorneys will want to send more than a cold, technical notice of the breach to their clients. Even if such a notice satisfies the statutory requirements,[177] it certainly would not help to maintain the goodwill of their clients, unless the attorney offers some assistance in minimizing losses the clients may suffer as a result of the breach. Moreover, there might be instances where attorneys learn of a security breach that does not fall within the notice requirements of the statutes, but nonetheless could prove damaging or embarrassing to their clients. Here the attorneys should be willing to notify their clients[178] and take reasonable measures to protect their clients' interests.

Maintaining client confidences is important to both attorneys and clients. Preserving clients' confidence in their attorneys and our legal system is critical to the success of the legal profession.[179]

("Expert testimony by those knowledgeable about the legal subject matter in question is relevant in applying the standard."). "A defending lawyer [defending himself or herself on a civil liability claim] may also introduce expert evidence on what constitutes care in the circumstances of the case or to support a defense . . . ." *Id.* at 130.

[177] *See* TEX. BUS. & COM. CODE ANN. § 48.103(b) (Vernon Supp. 2007) (putting forth the statutory requirement of notice upon breach).

[178] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 95-398 (1995) ("[S]hould a significant breach of confidentiality occur within a computer maintenance company . . . a lawyer may be obligated to disclose such breach to the client or clients whose information has been revealed.").

[179] Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 6 (2004); *see also* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2007) (imposing on attorneys a duty to keep client information confidential).