BEYOND TECHNOPHOBIA: LAWYERS' ETHICAL AND LEGAL OBLIGATIONS TO MONITOR EVOLVING TECHNOLOGY AND SECURITY RISKS

Timothy J. Toohey*

Cite as: Timothy J. Toohey, *Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks*, 21 RICH. J.L. & TECH. 9 (2015), http://jolt.richmond.edu/v21i3/article9.pdf.

I. INTRODUCTION

[1] Lawyers and technology have an uneasy relationship. Although some lawyers are early adapters, others take pride in ignoring technology because they believe it is alien to the practice of law. As Jody R. Westby observed, lawyers confronted with technology and security issues tend to have their "eyes glaze over" and "want to call in their 'IT guy' and go back to work."[1] But this technophobic attitude may no longer just be harmless conservatism. In the world of growing security risks, ignorance of technology may lead to violations of lawyers' fundamental ethical duties of competence and confidentiality.

[2] As with other businesses, lawyers are part of a constantly evolving and interconnected data ecosystem. The pervasiveness of electronic data in all aspects of commercial and personal life and its easy transmission through the Internet have not only fundamentally altered the manner in which lawyers interact with clients and with one another, but potentially expose confidential and proprietary information to rapid and unauthorized dissemination. As vast amounts of data are created and stored,

* Partner, Head of Cyber, Privacy and Data Security Practice at Morris Polich & Purdy, Los Angeles, California; Certified Information Privacy Professional United States and European Union (CIPP/US/E); Certified Information Privacy Manager (CIPM).

[1] Jody R. Westby, *Cybersecurity & Law Firms: A Business Risk*, 39 L. PRACTICE MAG. 4, 46 (July–Aug. 2013), *available at* http://www.lawpracticemagazine.com/lawpracticemagazine/july_august_2013#pg1,

confidential data—including attorney-client communications—can be readily transferred or accessed by unauthorized parties. With rapidly changing technology and threat vectors, lawyers are increasingly challenged in maintaining the security of their information and that of their clients.

[3] Rapid technological change has been a constant for the practice of law for at least a generation. E-mail, which in the early 1990s was not widely used in the profession, is now the main form of communication within law firms, as well as with counsel and clients outside the firm. Despite the growth of text messaging, e-mail continues to expand as a means of business communication. In 2011 there were on average 105 e-mails sent or received by corporate users per day, and it is predicted that this will increase to 125 e-mails per day by 2015.[2] While in 2011 there were over 3.1 billion e-mail accounts (of which 788 million were corporate), it is predicted that in 2015 there will be four billion accounts (of which over one billion would be corporate).[3]

[4] The use of the Internet, which impacts almost every aspect of the practice of law, has also grown substantially in the last twenty years. In 1995 there were sixteen million users worldwide, in 2005 over a billion, and as of June 2014 it is estimated that there are over three billion users.[4] In the past, lawyers used their own in-house computing resources. But now, facilitated by the Internet, lawyers frequently use remote provisioning of computing and storage services known as "cloud computing." It is predicted the future will show a 44% annual growth in

archived at http://perma.cc/VBR2-2RAM.

[2] *See* SARA RADICATI & QUOC HOANG, EMAIL STATISTICS REPORT, 2011-2015 3 (2011), *available at* http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf, *archived at* http://perma.cc/2SLA-4CD8.

[3] *See id.* at 2–3.

[4] *See Internet Growth Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/emarketing.htm (last updated Dec. 1, 2014 *archived at* http://perma.cc/27N9-68YE.

public cloud workloads, in comparison to an 8.9% annual growth for computing services located in the premises of businesses.[5] In 2014 it was estimated that there was one exabatye (i.e., 10^{18} bytes of data) stored in the cloud, and CISCO predicts data center traffic will triple by 2017.[6]

[5] This article argues that because of the evolving security risks brought by the changes wrought by e-mail, the Internet, and cloud computing, lawyers must reassess their ethical duties of competence and confidentiality. Although lawyers may have been comforted by ethical opinions finding the use of e-mail or cloud computing appropriate in the past, they can no longer rely on those opinions given dramatically altered security risks.

[6] This article also argues that lawyers must develop a greater awareness of the risks posed by the technology than they have had in the past because—like their clients—they are subject to rapidly escalating security threats. Whether they are aware of it or not, lawyers and law firms are increasingly the target of sophisticated hackers who deliberately seek out the confidential information they store on behalf of clients.[7] Although lawyers should not (and, indeed, cannot) abandon e-mail and cloud computing, they must shoulder greater responsibility in protecting data against evolving security risks. Lawyers must take concrete steps to protect data which they store for themselves and their clients, including developing risk management and incident response programs to prepare for cyberattacks and the consequences of such attacks. As with their corporate counterparts, security and privacy are no longer a matter for

[5] *See* Jack Woods, *20 Cloud Computing Statistics Every CIO Should Know*, SILICONANGLE (Jan. 27, 2014), http://siliconangle.com/blog/2014/01/27/20-cloud-computing-statistics-tc0114/, *archived at* http://perma.cc/GVQ2-MHRR.

[6] *See id.*

[7] *See, e.g.*, Andrew Conte, *Unprepared Law Firms Vulnerable to Hackers*, TRIBLIVE (Sept. 13, 2014, 10:40 PM), http://triblive.com/news/allegheny/6721544-74/law-firms-information#axzz3S2IsKaPf, *archived at* http://perma.cc/9DUR-HQXF (stating that computer hackers are targeting top international law firms to steal intellectual property data and trade secrets).

specialists, but for all who deal with private, proprietary, and confidential data—including lawyers.[8]

II. LAWYERS AND TECHNOPHOBIA

[7] Although it is unlikely there will ever be a comprehensive study of the subject, a portion of the legal profession—if not outright Luddites—are uncomfortable with technology and consider an understanding of its workings to be unnecessary—if not inimical—to the practice of law.[9] In a 1963 article on "Lawyers and Machines," Colin Tapper observed that "[l]awyers are traditionally conservative" and resistant to change, including when it comes to adopting machines for their work.[10] Tapper presciently suggested what we would now call computerized databases could be useful in the practice of law, but feared that lawyers may be slow to accept such tools.[11] Although Tapper believed technology had brought

[8] *See, e.g.*, Richard Blackwell, *C-Suite Survey: Cybersecurity Becomes A Top Priority After Data Breaches*, BUS. NEWS NETWORK (Oct. 20, 2014, 10:09 AM), http://www.bnn.ca/News/2014/10/20/C-Suite-Survey-Cybersecurity-becomes-a-top-priority-after-data-breaches.aspx, *archived at* http://perma.cc/Y4X7-WPHP; *see also* JODY R. WESTBY, GOVERNANCE OF ENTERPRISE SECURITY: CYLAB 2012 REPORT: HOW BOARDS & SENIOR EXECUTIVES ARE MANAGING CYBER RISKS 5–6 (2012), *available at* http://www.hsgac.senate.gov/imo/media/doc/CYBER%20Carneigie%20Mellon%20report.pdf, *archived at* http://perma.cc/3CXW-4QKM (reporting that boards of directors are still "not actively addressing cyber risk management").

[9] *See* Maureen O'Neill, *Lawyers Must Conquer Technophobia to Provide Competent Counsel*, DISCOVER READY (May 24, 2012), http://discoverready.com/blog/lawyers-must-conquer-technophobia-to-provide-competent-counsel/, *archived at* http://perma.cc/92TG-NLT5; *see also* Mitch Kowalski, *New Legal Tech Audit Will Scare Lawyers into Embracing Technology*, LEGAL POST, (Aug. 29, 2014, 2:12 PM), http://business.financialpost.com/2014/08/29/new-legal-tech-audit-will-scare-lawyers-into-embracing-technology/, *archived at* http://perma.cc/U46T-3V35 ("Lawyers have traditionally revelled in their technophobia—much to their client's chagrin."); Kenneth N. Rashbaum et al., *Cybersecurity: Business Imperative for Law Firms*, N.Y. L.J. (Dec. 10, 2014), http://www.newyorklawjournal.com/id=1202678493487/Cybersecurity-Business-Imperative-for-Law-Firms, *archived at* http://perma.cc/2GVN-4XFT (referencing the "reputed technophobia of many lawyers").

[10] *See* Colin Tapper, *Lawyers and Machines*, 26 MOD. L. REV. 121, 122 (1963).

improvements, including the use of the Dictaphone, he noted that as late as the 1960s the Chancery Division of the English law courts resisted using "typewriters, the postal service and telephones."[12]

[8] Like their English counterparts, some U.S. lawyers have historically been resistant to adopting new technology. When future U.S. Secretary of State John Foster Dulles joined Sullivan & Cromwell in 1911, telephones and stenographers were not widely accepted and some "partners felt that the only dignified way of communication between members of the legal profession was for them to write each other in Spencerian script,[13] and to have the message thus expressed [sic] delivered by hand."[14] Clarence Seward, the managing partner of what would become Cravath, Swaine & Moore "'sought in vain to save the office from the machine [including elevators and typewriters], which was destroying the simplicity of American life.'"[15]

[9] Notwithstanding initial resistance, the U.S. legal profession eventually embraced elevators, typewriters and Dictaphones—as it would later adopt the Telex, copiers, fax machines, personal computers,

[11] *See id.*

[12] *Id.* at 122 n. 1.

[13] Spencerian script was a "script style that was used in the United States from approximately 1850 to 1925 and was considered the American *de facto* standard writing style for business correspondence prior to the widespread adoption of the typewriter." *Spencerian Script*, WIKIPEDIA, https://en.wikipedia.org/wiki/Spencerian_script, *archived at* https://perma.cc/2FHM (last modified June 24, 2014, 12:59 PM).

[14] Catherine J. Lanctot, *Attorney-Client Relationships in Cyberspace: The Peril and the Promise*, 49 DUKE L. J. 147, 164 (1999) (quoting John Foster Dulles, *Foreword* to ARTHUR H. DEAN, WILLIAM NELSON CROMWELL 1854–1984, at iii (1957)).

[15] *Id.* at 165 (quoting ROBERT T. SWAINE, THE CRAVATH FIRM AND ITS PREDECESSORS, 1819-1947, at 448 (1946)). Lanctot writes that "[i]n a story so telling that it can only be apocryphal, one colleague described the time that Seward refused to take an elevator up four flights to a hearing in federal court and insisted instead on walking. When he finally arrived at the courtroom, Seward was reportedly so out of breath that the argument had to be cancelled and the case submitted on the briefs." *Id.*

electronic mail, mobile phones, and electronic research databases.[16] Today's lawyers are unlikely to reject technology outright, because that would render them virtually incapable of communicating with one another and their clients and practicing law. Nonetheless, a substantial number of lawyers exhibit a sometimes studied indifference to technology, believing it to be either irrelevant to the practice of law or the purview of non-lawyers—including the IT department.[17]

III. SECURITY RISKS AND THE PRACTICE OF LAW

[10] Given their unsettled relationship with technology, lawyers have been slow to recognize that hackers have lawyers in their sights as a potentially easy target. Lawyers who "have a hard enough time just figuring out how to work their BlackBerry or iPhone"[18] may have difficulty understanding that they are "basically the same as any other company when it comes to countering cyberattacks and protecting their confidential and proprietary data."[19] But, in fact, lawyers have been warned for at least the last five years that they are susceptible to cyberattacks because of the substantial amounts of data they safeguard for themselves and their clients.[20]

---

[16] *See* Robert Ambrogi, *A Chronology of Legal Technology, 1842–1995*, L. SITES (Feb. 14, 2010), http://www.lawsitesblog.com/2010/02/chronology-of-legal-technology-1842.html, *archived at* http://perma.cc/NU4C-NFVX; *see also* Nicole Black, *10 Technologies That Changed the Practice of Law*, MYCASE (July 29, 2014), http://www.mycase.com/blog/2014/07/10-technologies-changed-practice-law/, *archived at* http://perma.cc/SRT5-A6QS.

[17] *See* Westby, *supra* note 1, at 46–47.

[18] Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, WALL ST. J., June 26, 2012, *available at* http://www.wsj.com/articles/SB10001424052702304458604577486761101726748, *archived at* http://perma.cc/2V83-AP92.

[19] Westby, *supra* note 1, at 46.

[20] *See* Michael Cooney, *FBI Warns of Spear Phishing Attacks on Lawyers, PR Firms*, NETWORKWORLD (Nov. 18, 2009, 3:20 PM),

[11] As cyberattacks have grown in number, so has the exposure of the legal profession to such attacks. In the last two years, cyberattacks on U.S. enterprises have been constantly in the news. 2014 has been proclaimed the "year of the data breach" because of the well-publicized attacks on Target, Home Depot, Sony Pictures Entertainment (SPE), and numerous other businesses.[21] Even before the SPE breach in November 2014, Forrester Research predicted that "[a]t least 60% of brands will discover a breach of sensitive data in 2015, with the actual number of breached entities being as high as 80% or more . . . ."[22]

[12] The Verizon 2014 Data Breach Investigations Report, which is based on reported events from 2013, referenced 63,437 reported security incidents and 1,367 breaches in almost every economic sector.[23] Of interest to lawyers is the fact that the Verizon Report found that attacks on "professionals" have grown significantly in recent years with only the public sector, finance and retail having more security incidents than professionals in 2013.[24]

[13] The primary attack vectors for professionals include "denial of service" (DoS) attacks and cyber espionage.[25] DoS attacks typically

---

http://www.networkworld.com/article/2232563/security/fbi-warns-of-spear-phishing-attacks-on-lawyers--pr-firms.html, *archived at* http://perma.cc/HDV5-4LXZ.

[21] *See* Tom Huddleston, Jr., *The Sony Hack Should Make Cyber Security a Hot Boardroom Topic*, FORTUNE (Dec. 23, 2014, 1:55 PM), http://fortune.com/2014/12/23/sony-hack-security-boardroom/, *archived at* http://perma.cc/R62B-NEUF.

[22] *60% of Brands Will Discover a Breach of Sensitive Data in 2015*, FORRESTER (Nov. 12, 2014), https://www.forrester.com/60+Of+Brands+Will+Discover+A+Breach+Of+Sensitive+Data+In+2015/-/E-PRE7425, *archived at* https://perma.cc/C9S6-A88J.

[23] *See* VERIZON, 2014 DATA BREACH INVESTIGATIONS REPORT 2 (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/, *archived at* http://perma.cc/B2KR-4LT9.

[24] *See id.* at 15.

compromise the availability of networks and systems through network and computer applications.[26] DoS attacks may be launched by either individuals or entities, including foreign governments, competitors and disgruntled employees. The aim of a DoS attack is to slow or shut down legitimate traffic to the victim's website.[27] Almost any type of business may be subject to a DoS attack and such attacks may be launched for a wide variety of reasons, including shutting down a controversial project, preventing access to financial or other key services, gaining publicity for a cause, or benefiting a foreign government or competitor.[28]

[14] Another major source of attacks against professionals is cyber espionage, in which state-affiliated actors, particularly from Asia and Eastern Europe, target enterprises to obtain information of competitive or strategic value.[29] Cyber espionage attacks are often conducted through malware implanted on computer systems by way of a social engineering attack, such as "spear-phishing" e-mails.[30] In a targeted attack, the user

[25] *See id.*

[26] *See id.* at 43–45.

[27] *See* TIMOTHY J. TOOHEY, PRIVACY AND DATA SECURITY TRENDS AND DESIGN PROFESSIONALS 1–2 (Morris Polich & Purdy 2014) [hereinafter PRIVACY AND DATA SECURITY TRENDS AND DESIGN PROFESSIONALS], *available at* http://www.mpplaw.com/files/Publication/c76f880b-a26b-4d33-91eb-e629890feeca/Presentation/PublicationAttachment/de6cbf28-77b2-4389-ad01-e6a0f3a741eb/DR-Privacy-and-Data-Security-Trends-and-Design-Professionals-TJT-June-2014.pdf, *archived at* http://perma.cc/WKC2-JNDX.

[28] *See id.* at 2; *see also* Bob Tarzey, *Why Would They DoS Us?*, COMPUTERWEEKLY (Feb. 10, 2014, 7:54 AM), http://www.computerweekly.com/cgi-bin/mt-search.cgi?blog_id=119&tag=Denial-of-service%20attack&limit=20, *archived at* http://perma.cc/XYS6-KARF.

[29] *See, e.g.*, PRIVACY AND DATA SECURITY TRENDS AND DESIGN PROFESSIONALS, *supra* note 27, at 2.

[30] *See* Pieter Danhieux, *Email Phishing Attacks*, OUCH! (Sans Institute), Feb. 2013, at 1, *available at* http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_en.pdf, *archived at* http://perma.cc/M3WW-MCVD.

typically receives a seemingly bona fide e-mail from what appears to be a colleague which in fact comes from a hostile party.[31] When the recipient clicks on an executable file in the e-mail, malware is launched that is implanted into the recipient's computer system.[32]

[15] Although some of the details are unclear, the massive breach against SPE's computer systems in November and December 2014 is in key respects akin to a cyber espionage attack. Using malware with the capability to, among other things, access files stored on a computer system, the hackers mounted an attack on SPE that created backdoor access to the system, destroyed and "clean[ed]" computer systems, and paralyzed the company's computer systems for weeks.[33] The attack, which the U.S. attributes to North Korea, arose in conjunction with the James Franco and Seth Rogen film *The Interview* which featured a fictional plot to assassinate North Korean leader Kim Jong Un.[34] The attack rendered SPE's computer system inaccessible, and significant amounts of sensitive and proprietary data were exfiltrated from its system.[35] The attack also resulted in the release and public distribution of

[31] *See id.*

[32] *See id.* at 1–2.

[33] *See, e.g.*, Brian Krebs, *Sony Breach May Have Exposed Employee Healthcare, Salary Data*, KREBS ON SECURITY (Dec. 2, 2014, 11:21 AM), http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/, *archived at* http://perma.cc/3TNS-RC67; *see also Alert (TA14-353A): Targeted Destructive Malware*, U.S. COMPUTER EMERGENCY READINESS TEAM (Dec. 19, 2014), https://www.us-cert.gov/ncas/alerts/TA14-353A, *archived at* https://perma.cc/KB5E-29AR (analyzing malware used to attack SPE).

[34] *See, e.g.*, David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea After Sony Case*, N.Y. TIMES, Jan. 3, 2015, at A1, *available at* http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html, *archived at* http://perma.cc/4QVA-NPKE.

[35] *See* Ben Fritz and Danny Yadron, *Sony Hack Exposed Personal Data of Hollywood Stars*, WALL ST. J., Dec. 5, 2014, *available at* http://www.wsj.com/articles/sony-pictures-hack-reveals-more-data-than-previously-believed-1417734425 *archived at* http://perma.cc/6UHK-RQBY.

sensitive attorney-client communications, including materials relating to labor matters handled by a prominent U.S. law firm, e-mails from SPE executives, and 47,000 social security numbers of current and former SPE employees, including actors and directors.[36]

[16] Social engineering attacks are not limited to those engaging in cyber espionage. For example, in the 2013 Target hack, a social engineering attack against one of Target's vendors launched malware that allowed cyber criminals in Eastern Europe to obtain credit card information from Target's customers at the point of sale (POS).[37] The malware lurked on Target's system for weeks and automatically sent credit card information for 70–110 million individuals to the hackers.[38]

[17] Cyber espionage attacks are particularly difficult to detect. The Verizon 2013 Report found that 62% of the attacks took months to discover and 5% of attacks took years to detect.[39] Aside from the SPE attack, which appears to have been motivated less by economic than political motives, attacks are typically launched by foreign nation states to obtain information to allow them to gain advantage for a particular project. For example, in May 2014 the U.S. Department of Justice announced it had charged Chinese military hackers with cyber espionage aimed at

[36] *See id.*; *see also* Debra Cassens Weiss, *Sony Pictures Hires David Boies, Who Warns Media to Destroy Documents Leaked by Hackers*, ABA Journal (Dec. 15, 2014 11:38 AM), http://www.abajournal.com/news/article/sony_pictures_hires_david_boies_who_warns_media_to_destroy_hacked_documents, *archived at* http://perma.cc/33FK-8XBZ.

[37] *See* Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KREBS ON SECURITY (Feb. 5, 2014, 1:52 PM), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/, *archived at* http://perma.cc/F2JR-9ZYE.

[38] *See* Elizabeth A. Harris and Nicole Perlroth, *For Target, The Breach Numbers Grow*, N.Y. TIMES, Jan. 11, 2014, at B1, *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0, *archived at* http://perma.cc/GH83-UUQD.

[39] *See* VERIZON, *supra* note 23, at 41.

obtaining "confidential and proprietary technical and design specifications" from several U.S. companies, including Westinghouse, to advantage Chinese state-owned enterprises.[40]

[18] Law firms are far from immune to security attacks, including DoS and cyber espionage attacks.[41] In its August 2014 cybersecurity resolution, the ABA found that "[t]he threat of cyber attacks against law firms is growing" and that "[l]awyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices."[42] Lawyers and law firms are targets because "[t]hey collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-[D]iscovery."[43] As a former FBI agent has observed, law firms are vulnerable to attack because they "'have incredibly valuable and sensitive information, and the Internet just provides a whole other methodology through which the information can be accessed and pilfered.'"[44] Lawyers may also be targets

[40] *See* Press Release, U.S. Dept. of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, *archived at* http://perma.cc/XYJ8-DQJX.

[41] *See* Rashbaum et al., *supra* note 9.

[42] JUDITH MILLER AND HARVEY RISHIKOF, ABA, CYBERSECURITY LEGAL TASK FORCE SECTION OF SCIENCE & TECH. LAW REPORT TO THE HOUSE OF DELEGATES 4 (2014), *available at* http://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf, *archived at* http://perma.cc/ACE4-GAKC; *see also American Bar Association House of Delegates Adopts Resolutions on Cybersecurity, Domestic Violence*, ABA (Aug. 12, 2014), http://www.americanbar.org/news/abanews/aba-news-archives/2014/08/american_bar_associa.html, *archived at* http://perma.cc/G9AL-8T9N.

[43] MILLER AND RISHIKOF, *supra* note 42, at 4.

[44] Smith, *supra* note 18 (quoting Shawn Henry, a "FBI veteran former executive assistant director of the agency's criminal, cyber, response and services branch.").

of attacks because "it is generally easier for a hacker to break into a law firm's network to steal client data than it is to hack into the clients' networks to steal the data."[45]

[19] Few law firm hacks have been publicized, most likely because the firms are reluctant publicly to expose their vulnerability and may not legally be required to inform the public of hacks.[46] However, it has been reported that an unnamed "major New York law firm" was attacked in 2012 by Chinese hackers seeking information about a business deal.[47] When this hack was announced, the FBI "convened a meeting with the top 200 New York City law firms to address the rising number of cyberattacks on law firms."[48] The FBI reportedly warned lawyers at the meeting "that they were easy prey for hackers trying to obtain their clients' valuable data."[49] Law firms were an "easy target," according to the FBI, because "partners insist on mobility—including the ability to review case documents at home on the weekend or while travelling—which means highly sensitive documents are routinely transferred by e-mail, leaving them vulnerable to attack."[50] The FBI informed lawyers at the meeting that it had "'seen specific documents from law firms on specific deals being exfiltrated from cyberattacks.'"[51]

---

[45] Lynn Watson, *At the Crossroads of Lawyering and Technology: Ethics*, PRACTICE INNOVATIONS, July 2012, at 17, 18, *available at* http://info.legalsolutions.thomsonreuters.com/signup/newsletters/practice-innovations/2013-jan/Jan13_PracticeInnovations.pdf, *archived at* http://perma.cc/H67Z-NE5F.

[46] *See* Conte, *supra* note 7.

[47] *See* Mike Mintz, *Cyberattacks on Law Firms-A Growing Threat*, MARTINDALE.COM BLOG (Mar. 19, 2012), http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat, *archived at* http://perma.cc/H67Z-NE5F.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Smith, *supra* note 18 (quoting Mary Gallian of the FBI).

[20] Documents held by law firms are of undoubted interest to hackers. In some instances, documents originating from law firms have been exposed when hackers attack a firm's clients. For example, in the recent SPE attack, documents originating from a prominent labor and employment firm were published on the Internet, including documents that apparently contained details regarding termination of employees.[52] In another attack said to have been launched by Wikileaks in retaliation for the claim of a security firm that boasted it could identify individuals belonging to that hacktivist organization, documents were put on line from a national law firm relating to representation of clients such as Bank of America and the U.S. Chamber of Commerce.[53]

IV. LAWYERS' LEGAL AND ETHICAL OBLIGATIONS TO SECURE DATA

[21] In common with other enterprises, lawyers are legally required to secure personal data they hold on behalf of others and for themselves. In addition to being obligated to secure personal data, lawyers are also ethically bound as professionals to maintain the confidentiality of client documents and communications, which is a much broader category than "personal" information.

A. Lawyers' Legal Obligations to Secure Data

[22] Federal and state laws impose legal obligations on law firms, like other enterprises, to implement "reasonable" security measures to protect data that they store on behalf of themselves and others. These laws also require enterprises to report any breaches in the security of personal data.

[23] For example, Cal. Civ. Code § 1798.81 requires businesses to take

[52] *See* Krebs, *supra* note 33 (showing screen shot of file tree including references to law firm and employee data).

[53] *See* Brian Baxter, *Hunton & Williams Linked to Hacked E-Mail Affair*, AMLAW DAILY (Feb. 15, 2011, 11:11 AM), http://amlawdaily.typepad.com/amlawdaily/2011/02/hunton-wikileaks.html, *archived at* http://perma.cc/7RKU-V6LG.

"reasonable steps to dispose, or arrange for the destruction of customer records within its custody or control containing personal information."[54] Cal. Civ. Code § 1798.81.5 also requires businesses that "own" or "license" personal information about a California resident to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification, or disclosure."[55] As of January 1, 2015, California will also require businesses that "maintain" information on behalf of others to implement such security measures, for "information that a business maintains but does not own or license."[56]

[24] California and forty-seven other states require persons and businesses, including lawyers, to notify residents regarding breaches of unencrypted personal information.[57] In California, which has led the way in such data breach notification laws, "personal information" includes (1) an individual's first name or first initial and last name in combination with a social security number, a driver's license or identification card number, an account number, credit or debit card number in combination with a

[54] CAL. CIV. CODE § 1798.81 (Deering 2005). The statute further requires that records are to be shredded or erased or that the personal information in the records should be made "unreadable or undecipherable through any means."

[55] *Id.* at § 1798.81.5.

[56] *See* A.B. 1710, 2013–2014 Gen. Assemb., Reg. Sess. (Cal. 2014)., *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710, *archived at* http://perma.cc/HL69-CJDV; *see also* Timothy J. Toohey, *California Modifies Its Data Breach Notification Requirements Again*, MORRIS POLICH & PURDY (Oct. 3, 2014) [hereinafter *California Modifies Its Data Breach Notification Requirements Again*], http://privacydatasecurity.com/CA-Modifies-Data-Breach-Notification-AB-1710-TJT-10'3'14.pdf, *archived at* http://perma.cc/SK3S-8LGD.

[57] *See* CAL. CIV. CODE § 1798.82 (Deering 2005). A list of the data breach laws is maintained by the National Conference of State Legislatures. *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, *archived at* http://perma.cc/V9JZ-UYJZ (maintaining a list of data breach laws).

required security code, access code or password, medical information, or health insurance information or (2) a user name and e-mail address in combination with a password or security question and answer that would permit access to an online account.[58] Moreover, if the personal information that is breached is not owned by the person or business that was breached, they must "notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[59] Failures of businesses, including law firms, to maintain appropriate security or to comply with data breach notification laws, may subject them to fines and/or lawsuits for damages.[60]

[25] Federal authorities may also penalize businesses that do not maintain appropriate security measures. For example, the Federal Trade Commission (FTC) has broad authority under Section 5 of the FTC Act[61] to bring actions against enterprises that do not maintain "reasonable and appropriate data security for consumers' sensitive personal information."[62]

[58] *See* CAL. CIV. CODE § 1798.82(e).

[59] *Id.* at § 1798.82(b).

[60] *See id.* at § 1798.84. For example, the California Attorney General brought an action against Kaiser Foundation Health Plan alleging that the disclosure of a breach was unreasonably delayed when personal data was found in a hard drive being sold at a thrift store. *See* Ronald W. Breaux, Emily Westridge Black, and Timothy Newman, *California AG Cracks Down on Timing of Data Breach Disclosures*, HAYNES BOONE (Feb. 5, 2014), http://www.haynesboone.com/california-ag-cracks-down-on-timing-of-data-breach-disclosures-02-04-2014/, *archived at* http://perma.cc/M8CK-KCWA. Kaiser settled the matter for $150,000.00. *Id.*

[61] *See* 15 U.S.C. § 45(a)(1) & (2) (2012). The Act declares unlawful "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce . . . ." *Id.* The FTC's enforcement generally proceeds under either the "unfairness" prong which focuses on consumer injury or the "deception" prong which focuses on "[a] representation, omission, or practice [which] misleads or is likely to mislead the consumer." *See* TIMOTHY J. TOOHEY, UNDERSTANDING PRIVACY AND DATA PROTECTION: WHAT YOU NEED TO KNOW 107–08 (2014) [hereinafter UNDERSTANDING PRIVACY AND DATA PROTECTION].

The FTC may take administrative actions against entities that do not maintain reasonable security measures, which typically result in consent decrees requiring businesses to put in place a comprehensive security program and undertake periodic audits or reviews by a certified third party for up to 20 years.[63]

[26] Law firms, like other enterprises, are also subject to federal laws that require implementation of security measures. For example, law firms may be considered "business associates" under the Health Information Privacy Protection Act (HIPAA)[64] because they perform functions for health care clients, such as reviewing documents that contain health care information.[65] As HIPAA business associates, law firms must follow the

[62] Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 13-1887 (ES), 2014 U.S. Dist. LEXIS 84913, at *1 (D.N.J. June 23, 2014).

[63] *See* Press Release, Fed. Trade Comm'n, Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information (Jan. 31, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it, *archived at* http://perma.cc/K6ST-U33C. The settlement with the company in question (GMR Transcription) was the 50th data security case settled by the FTC. *Id.*

[64] *See* Matthew H. Meade, *Lawyers and Data Security: Understanding a Lawyer's Ethical and Legal Obligations That Arise from Handling Personal Information Provided by Clients*, 28 COMPUTER & INTERNET LAWYER 1, 7 (Oct. 2011), *available at* http://www.bipc.com/files/Publication/ae615839-5e8f-4ce6-99af-a6aed9bc6a69/Preview/PublicationAttachment/2ea3d9ea-61bc-4324-8cee-5df5f01e07dd/CIL_1011_Meade.pdf, *archived at* http://perma.cc/2WT5-36J8.

[65] According to the United States Department of Health and Human Services, a "business associate" is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." U.S. DEP'T OF HEALTH AND HUMAN SERV., BUSINESS ASSOCIATES 1 (2009), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf, *archived at* http://perma.cc/8HWY-QNGR. The rules relating to business associates are set forth in 45 C.F.R. § 164.502(e) (2014), 45 C.F.R. § 164.504(e) (2014), 45 C.F.R. §164.532(d) (2014) and 45 C.F.R. §164.532(e) (2014). A "covered entity" is a provider of health care services and "protected health information" (sometimes referred to as PHI) is all "individually identifiable health information" held or sent by a "covered entity or its

HIPAA Security Rule[66] requiring them to put in place safeguards to secure electronic protected health information. Although the HIPAA Security Rule does not require specific security measures, it recommends implementing procedures to insure the confidentiality, integrity, and availability of electronic protected health information to protect against reasonably anticipated threats and impermissible uses or disclosures, and to ensure compliance by an entity's employees.[67] If a law firm is a HIPAA business associate, it must also report breaches of protected health information to the United States Department of Health and Human Services and may be subject to fines for such breaches.[68]

B. Lawyers' Ethical Obligations to Maintain Client Confidences

[27] In addition to being subject to state and federal laws affecting other enterprises, lawyers also have independent ethical duties requiring them to be aware of the risks of technology and to implement measures to protect against unauthorized disclosure of confidential information.

[28] The ABA Model Rules of Professional Conduct ("ABA Model Rules"), which are followed by most states, establish a competence requirement in Rule 1.1 that "[a] lawyer shall provide competent

business associate, in any form or media, whether electronic, on paper, or oral." *See Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERV., *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html, *archived at* http://perma.cc/483U-CWKY (last visited Jan. 20, 2014).

[66] *See* 45 C.F.R. § 164.502(a)(1) (2013).

[67] *See* UNDERSTANDING PRIVACY AND DATA PROTECTION, *supra* note 61, at 37–38.

[68] *See California Modifies Its Data Breach Notification Requirements Again*, *supra* note 56, at 37–39.

representation to a client."[69] The ABA Model Rules further state "[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[70] Since 2012, comment 8 to Rule 1.1 has provided that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."[71]

[29] Rule 1.6 of the ABA Model Rules establishes the duty for lawyers to maintain the confidentiality of information and requires that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . . ."[72] Rule 1.6 further provides that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[73]

[30] Since 2012, comment 18 to ABA Model Rule 1.6(c) has "require[d] a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."[74]

---

[69] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2014).

[70] *Id.* States have adopted these changes, including Pennsylvania. *See* Shannon Brown, *Pennsylvania's New, Technology-related Ethics Rule Changes for Lawyers*, SHANNON BROWN LAW (Mar. 21, 2014), http://www.shannonbrownlaw.com/archives/2109, *archived at* http://perma.cc/Z5V8-2CEK.

[71] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2014) (emphasis added).

[72] *Id.* at R. 1.6(a).

[73] *Id.* at R. 1.6(c).

[74] *Id.* at R. 1.6 cmt. 18.

[31] If the lawyer has "made reasonable efforts to prevent the access of disclosure" the Rule is not violated.[75] Comment 18 further states that

> Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.[76]

[32] In Formal Opinion 2010-179, the California Standing Committee on Professional Responsibility and Conduct addressed an issue similar to that addressed in the 2012 comments to the ABA Model Rules. Opinion 2010-179 discussed the issue of whether an attorney violates the duties of confidentiality and competence owed to a client "by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties."[77] The specific

[75] *Id.*

[76] *Id.*

[77] State Bar of California Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 at 1 (discussing whether an attorney violates duties of confidentiality and

context for the opinion was whether an attorney using a laptop to conduct legal research and e-mail a client through a public wireless Internet connection and through the attorney's personal wireless system violated any ethical rules.[78]

[33] Opinion 2010-179 concluded that the use of a public wireless connection without using precautions, such as encryption or a personal firewall, risked violating the attorney's duties of confidentiality and competence because of the "lack of security features provided in most public wireless access locations."[79] In contrast, the opinion found that the use of the attorney's personal wireless system would not violate the attorney's duties if the system were "configured with appropriate security features."[80]

[34] Opinion 2010-179 adopted a flexible analytic approach to technology, recognizing that technology is "ever-evolving" and is now integrated in "virtually every aspect of our daily lives."[81] The opinion further recognized that "guidance to attorneys in this area has not kept pace with technology" and "[m]any attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy."[82] Although the opinion found it was unnecessary for attorneys to develop a mastery of the security features and deficiencies of each technology available, *the duties of confidentiality and competence that attorneys owe*

competence when using technology to transmit or store confidential client information that may be susceptible to unauthorized access by third parties), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836, *archived at* http://perma.cc/Z2NX-ZWF5.

[78] *See id.*

[79] *Id.* at 7.

[80] *See id*. (noting that features such as firewalls, antivirus and anti-spam software, secure username and password combinations, and file permissions as "appropriate.").

[81] *Id.* at 1.

[82] *Id.* at 1, 5.

to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.[83]

[35] Opinion 2010-179 further emphasized that attorneys must ensure that law firm personnel are "appropriately instructed regarding client confidentiality and are supervised in accordance with rule 3-110."[84] Because of "the evolving nature of technology and differences in security features that are available, the attorney *must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps*."[85]

[36] California Formal Opinion 2010-179, combined with the 2012 revisions to the ABA Model Rules, place an affirmative obligation on lawyers not merely to be generally aware of the risks of technology, but to understand how risks relating to a specific technology are evolving. A technology that may have been safe when it was introduced may no longer be secure if risks have developed that undermine confidentiality protections.

[37] In addition, both the ABA Model Rules and California Formal Opinion 2010-179 place an obligation on lawyers to implement a security

[83] State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 at 5, (emphasis added) (citing Cal. Rules Prof. Conduct, R. 3-110(C) (2013) ("If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by (1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or (2) by acquiring sufficient learning and skill before performance is required.")), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836, *archived at* http://perma.cc/F337-JV48.

[84] *Id.* at 6.

[85] *Id.* at 7 (emphasis added).

program protecting confidential data. Although the precise elements will differ for each lawyer or firm, a security program should include governance standards, "development of security strategies, plans, policies and procedures; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training."[86] Lawyers and law firms should also put in place a cyber response plan allowing them to detect problems, determine the cause of the problem, and resolve the problem.[87] As the ABA Cybersecurity Task Force has recommended, response plans "should be able to accommodate the full array of threats, not just data breaches."[88] Finally, as both the ABA Model Rules and the California Opinion 2010-179 recognize, law firms must put training programs in place to ensure that law firm personnel are aware of security risks and know how to help prevent cyberattacks.

V. LAWYERS' USE OF E-MAIL

[38] E-mail has become the most frequently used means of communicating within law offices and to clients, obtaining electronic alerts regarding deadlines and court filings, coordination of meetings, and accessing seemingly endless announcements of CLE seminars and communications from vendors. Because of its ubiquity, many lawyers likely believe that e-mail poses few ethical or security risks, other than the inadvertent use of "reply all."

[39] State bar associations addressing the ethics of e-mail have generally given it a green light, including lawyer use of Internet-based e-mail services, such as Gmail or Yahoo! Mail. Notwithstanding these opinions, e-mail poses significant ethical challenges for lawyers, particularly in preserving the confidentiality of communications because of security risks associated with its transmission and storage. Some web-

[86] MILLER AND RISHIKOF, *supra* note 42, at 6.

[87] *See id.* at 6.

[88] *See id.* at 9.

based e-mail providers—including Gmail—present additional challenges, because these services use e-mail content to target advertising to users and have taken the position that users have no privacy in e-mails. Finally, unencrypted e-mail entails substantial security risks, including dissemination of private communications to third parties.

A. Lawyers' Ethical Obligations and E-mail

[40] The use of unencrypted e-mail by lawyers received the blessing in 1999 of the American Bar Association Standing Committee on Ethics and Professional Responsibility ("ABA Standing Committee").[89] In Formal Opinion 99-413, the ABA Standing Committee concluded that "[a] lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[90] In reaching the conclusion, Opinion 99-413 found "[t]he same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail."[91]

[41] From today's perspective, the conclusion in Opinion 99-413 that e-mail has the "same privacy" as mail is not merely "obsolete," but misguided.[92] The fact that e-mails can be saved electronically and readily forwarded (deliberately or inadvertently) to third parties, makes them considerably less secure than mail, facsimiles, and telephone calls. To take but one current example, the embarrassing e-mails disseminated through the SPE hack that have threatened the careers of several

[89] The ABA's opinion was preceded by those of other organizations, including state bar associations. *See* Rebecca Bolin, Symposium, *Risky Mail: Concerns in Confidential Attorney-Client Email*, 81 U. CIN. L. REV. 601, 616–18 (2012).

[90] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (discussing protection of confidentiality of unencrypted e-mail).

[91] *Id.*

[92] *See* Bolin, *supra* note 89, at 603, 618.

prominent executives—including the co-chairman of the company—would not have come to light if the executives in question had confined their views to a telephone conversation or a note sent by mail.[93]

[42] In reaching its 1999 conclusion regarding e-mail privacy, the ABA Standing Committee relied on a 1998 article by David Hricik with the comforting title *E-mail and Client Confidentiality: Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*.[94] As has been noted by other commentators, Professor Hricik's reassuring conclusions regarding e-mail privacy and confidentiality depended on the then state of e-mail technology. In the mid and late 1990's, e-mails typically traveled to personal computers with limited storage space. Service providers like AOL "deleted mail off [their] servers after a few days to save on then-expensive storage."[95] In contrast, storage space today is extremely inexpensive and recipients often preserve vast numbers of sent and received e-mails for many years. E-mails are routinely backed up on an enterprise's servers and can be accessed—like those of SPE—by malicious parties or disseminated by careless insiders. Moreover, e-mails sent from web-based services such as Gmail, Yahoo!, or Outlook may be stored indefinitely in large numbers in the cloud and may thus exist "without a user's knowledge as an archival or back-up copy."[96]

[43] In 2011, the ABA Standing Committee issued an opinion that

[93] *See* Daniel Miller, *Future of Sony's Amy Pascal Questioned After Hacked Email Revelations*, L.A. TIMES (Dec. 11, 2014, 6:20 PM), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-amy-pascal-apologizes-20141212-story.html#page=1, *archived at* http://perma.cc/2JAM-JLCY.

[94] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (discussing confidentiality of unencrypted e-mail) (citing David Hricik, *E-mail and Client Confidentiality: Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 479 (1998)).

[95] Bolin, *supra* note 89, at 609.

[96] *See id.*, at 611–12.

qualified its 1999 opinion regarding the propriety of e-mail use.[97] In Formal Opinion 11-459, the ABA Standing Committee concluded that lawyers:

> [S]ending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access.[98]

Opinion 11-459 specifically cautioned lawyers about having their clients communicate with them using an employer's computer or device because employers "often have policies reserving a right of access to employees' e-mail correspondence via the employer's e-mail account, computers or other devices, such as smartphones and tablet devices, from which their employees correspond."[99] Opinion 11-459 also recognized that e-mail subject to access by third parties may compromise a lawyer's ethical duties to preserve client confidences.[100]

B. Lawyers' Use of Web-Based E-mail

[44] Although many lawyers rely on enterprise e-mail systems run by their law firms, other lawyers—particularly those in small to medium size firms—may use web-based e-mail systems such as Gmail, Outlook, Yahoo! Mail, or AOL. Particularly popular is Google's Gmail, which is

[97] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) (discussing the duty to protect confidentiality of e-mail communications with clients), *available at* http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf, *archived at* http://perma.cc/UG3HFVCX; *see also* Bolin, *supra* note 89, at 622.

[98] *Id.*

[99] *Id.*

[100] *Id.*

free and offers 1 GB of storage.[101] An analyst estimated 60% of mid-size companies had their e-mail hosted by Google in 2014 and that 92% of startups or very small companies use Google.[102] From the point of view of their ethical obligations, lawyers may have concerns that Google scans e-mails to provide targeted advertising to its users. For example, a lawyer using Gmail to communicate with a client regarding a meeting at a particular hotel may find that she is being targeted with advertisements for that hotel. Although this sort of advertising may be innocuous, there may be greater concerns if advertisements are based on more sensitive content, such as a client's medical condition or employment relationship with a particular company.

1. The Ethics of Gmail

[45] In 2008, the New York State Bar Association Committee on Professional Ethics in Ethics Opinion 820 addressed the question of whether lawyers may use programs that scan e-mails.[103] Although the opinion did not mention Gmail by name, it clearly referenced the service by posing the question of whether "a lawyer [may] use an e-mail service provider that scans e-mails by computer for keywords and then sends or displays instantaneously (to the side of the e-mails in question) computer-generated advertisements to users of the service based on the e-mail communications."[104]

---

[101] *See Lots of free storage*, GOOGLE, https://www.gmail.com/intl/en_us/mail/help/features.html#storage, *archived at* https://perma.cc/6NDC-NKBC (last modified Apr. 14, 2014) (indicating that users get 15GB of free storage across Gmail, Google Drive, and Google+ Photos).

[102] *See* Dan Frommer, *Google is Stealing away Microsoft's Future Corporate Customers*, QUARTZ (Aug. 1, 2014), http://qz.com/243321/google-is-stealing-away-microsofts-future-corporate-customers/, *archived at* http://perma.cc/WB79-W9LT.

[103] *See* New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 820 (2008) (discussing use of e-mail services that scan e-mail for advertising purposes), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&template=/CM/ContentDisplay.cfm&ContentID=55868, *archived at* http://perma.cc/XB8V-JCGJ.

[104] *Id.*

[46] Ethics Opinion 820 found the "risks posed to client confidentiality [by the e-mail service] are not meaningfully different from the risks in using other e-mail service providers that do not employ this practice" because "no individuals other than e-mail senders and recipients read the e-mail messages."[105] The opinion further stated that the committee would have reached "the opposite conclusion if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission (or a lawful judicial order)."[106]

2. Gmail and Google's Terms of Service

[47] The conclusion that Google's Gmail passes ethical muster because no human being reviews e-mails does not address all the potential risks posed by web-based e-mail services. For example, Ethics Opinion 820 did not discuss the implications that Google's Terms of Service ("TOS"), privacy policies, and other Google statements regarding e-mail privacy have on expectations of privacy in Gmail.

[48] E-mail providers' policies and terms of service have been called "the persistent elephant in the room" regarding e-mail privacy.[107] The current version of Google's TOS—which applies not only to Gmail, but to

[105] *Id.*

[106] *Id.*; *see also* Kevin Raudebaugh, *Trusting the Machines: New York State Bar Ethics Opinion Allows Attorneys to Use Gmail*, 6 WASH. J.L. TECH. & ARTS 83, 90–91 (2010). The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility also found that the use of Gmail is acceptable. Pennsylvania Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2011-200 (2011), *available at* http://forctlawyers.com/wp-content/uploads/2012/04/PA-opinion-2011-200.pdf, *archived at* http://perma.cc/U6GM-EEG6 (discussing ethical obligations for attorneys using cloud computing software as a service).

[107] Bolin, *supra* note 89, at 640–41 ("The assumed privacy protections [for e-mail] are now hazy or even hostile to privacy interests, and the assumed practices to keep e[-]mail confidential will obviously depend on the privacy policy. Today's user should be very concerned about the case-specific policies relating to e[-]mail.").

all of Google's "Services," including popular cloud-based products such as Google Apps—contains several provisions that may impact lawyers' expectations of privacy and confidentiality in their communications to clients.[108]

[49] For example, although Google's TOS states that users "retain ownership of any intellectual property rights that [they] hold in . . . content" that is uploaded, submitted, stored, send or received through its services, it also states that users

> [G]ive Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.[109]

This "license"[110] is "for the limited purpose of operating, promoting, and improving our Services, and to develop new ones."[111]

[50] Regarding targeted advertising, Google's TOS states that "[o]ur automated systems analyze your content (including e[-]mails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."[112]

---

[108] *See Google Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms/, *archived at* http://perma.cc/7R26-WU66 (last modified April 14, 2014) [hereinafter *Google Terms of Service*].

[109] *Id.*

[110] *See* Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 248–49 (2011) (expressing doubt that a "license" is indeed created through the Google TOS).

[111] *Google Terms of Service*, *supra* note 108.

[51] Google also reserves the right to "suspend or stop a Service altogether," although "where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service."[113] Google further disclaims all warranties and reserves the right to "modify these terms or any additional terms that apply to a Service . . . ."[114] Google also warns that it may modify the terms in the future and requests users to "look at [its] terms regularly."[115] If a user does not "agree to the modified terms for a Service, [the user] should discontinue . . . use of the Service."[116]

[52] A lawyer using Gmail may have concerns regarding several aspects of Google's TOS, including the company's unilateral right to "communicate, publish, publicly perform, publicly display and distribute" the content of potentially privileged or confidential e-mails.[117] Although publication is ostensibly for the "limited purpose" of "operating, promoting, and improving our Services, and to develop new ones," the provision is broad enough to encompass several troubling scenarios, including Google's analyzing attorney-client privilege documents to establish a new product aimed at lawyers.[118] Lawyers may also be given pause by the fact that Google can unilaterally suspend services, disclaim all warranties, and place the onus of determining whether the TOS has changed on the users of the service whose only option if they agree with

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Google Terms of Service*, *supra* note 108.

[118] *Id.*

the new TOS is to quit using Gmail.[119]

3. Gmail Users' Expectations of Privacy

[53] Nothing in Google's TOS states that users have any expectation of privacy for the electronic communications they send or receive through Gmail. Indeed, Google has taken the position that individuals sending e-mails to Gmail accounts have no expectation of privacy. When Google was sued in federal court in 2010 for violating state and federal anti-wiretapping laws for intercepting, reading and acquiring the content of e-mails sent or received by Gmail users while the e-mails were in transit, Google argued in a motion to dismiss the complaint that those sending e-mails to Gmail users had consented to Google processing their messages, including accessing the content of messages.[120] Google stated in the motion that

> Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based e-mail today cannot be surprised if their communications are processed by the recipient's E[lectronic] C[ommunication] S[ervice] provider in the course of delivery. Indeed, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[121]

[119] *See* Trope & Hughes, *supra* note 110, at 248–49 (prior Google TOS created an "[i]ncreased [r]isk of [i]nadvertent [g]rant of [l]icense to [c]lient's [i]ntellectual [p]roperty" and raised a "serious ethical risk[] for a law firm or lawyers that use, or allow their staff to use, Google Docs when generating or revising documents that contain client confidential data and content in which the client has intellectual property rights").

[120] *See* Steven Musil, *Google Filing Says Gmail Users Have No Expectation of Privacy*, CNET (Aug. 13, 2013, 7:57 PM), http://www.cnet.com/news/google-filing-says-gmail-users-have-no-expectation-of-privacy/, *archived at* http://perma.cc/EKG4-X9XL.

[121] Defendant Google Inc.'s Motion to Dismiss Plaintiffs' Consolidated Individual and Class Action Complaint at 19, *In re* Google Inc. Gmail Litig., No. 5:13-md-02430-LHK (N.D. Cal. June 6, 2013) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)),

Google further argued that "the automated processing of e[-]mail is so widely understood and accepted that the act of sending an e[-]mail constitutes implied consent to automated processing as a matter of law."[122]

[54] In rejecting Google's argument, the court found that there was no support for Google's "far-reaching proposition" that users do not have an expectation in privacy when using a web-based e-mail service.[123] The court instead held that senders only "consent[] to the *intended recipient's recording of the e-mail*—not, as has been alleged here, interception by a third-party service provider."[124]

> Google has cited no case that stands for the proposition that users who send e[-]mails impliedly consent to interceptions and use of their communications by third parties other than the intended recipient of the e[-]mail. . . . Accepting Google's theory of implied consent—that by merely sending e[-]mails to or receiving e[-]mails from a Gmail user, a non-Gmail user has consented to Google's interception of such e[-]mails for any purposes—would eviscerate the rule against interception.[125]

available at http://www.consumerwatchdog.org/resources/googlemotion061313.pdf, *archived at* http://perma.cc/J46Z-SZRM.

[122] *Id.*

[123] *See In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784, at *55–57 (N.D. Cal. Sept. 26, 2013).

[124] *Id.* at 55–56 (emphasis added).

[125] *Id.* at 56. Although Judge Koh rejected many of Google's arguments in its motion to dismiss, she later denied plaintiffs' motion for class certification, finding that many of the issues regarding implied consent were factual in nature and thus created substantial differences among class members. *See In re* Google, Inc. Gmail Litig., No. 13-MD-02430-LHK, 2014 WL 1102660, at *18 (N.D. Cal. Mar. 18, 2014).

[55] Google's argument that those who send e-mails to Gmail users have no expectation of privacy may raise red flags for lawyers using Gmail to make or receive confidential client communications. The fact that Google has not only taken that position but also makes no commitment to preserve the privacy of communications sent through Gmail raises doubts as to whether lawyers using Gmail can reasonably comply with their duty of confidentiality.[126] Although Google—like most companies—has a privacy policy, that policy only restricts the manner in which Google shares personal information with "companies, organizations and individuals *outside of Google*."[127] Google's privacy policy does not restrict *Google's own use* of personal information and is inapplicable to sensitive or confidential information, such as attorney-client communications, that contains no "personal" information.[128]

[56] In arguing that those who send e-mails through Gmail have no expectation of privacy, Google cited the controversial "third party doctrine" set forth in the 1979 case of *Smith v. Maryland*.[129] Under the third party doctrine, an individual voluntarily turning over information to a third party assumes the risk that the third party will turn the information

[126] The protection of users' e-mails by the Electronic Communication Privacy Act (ECPA) and the Stored Communications Act (SCA) of 1986, 18 U.S.C. § 2510 *et seq.* is beyond the scope of this article, but is widely discussed elsewhere. *See, e.g.*, Jacob M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet*, 23 GEO. MASON U. C.R. L.J. 255, 266 (2013).

[127] *Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy/, *archived at* http://perma.cc/ZGP6-B357 (last modified Dec. 19, 2014) (emphasis added). Google states that it shares personal information with "companies, organizations and individuals outside of Google" only with users' consent, with domain administrators, for external processing, and for legal reasons. *Id*.

[128] *See id.* "Personal information" is defined in Google's Privacy Policy as "information which you provide to us which personally identifies you, such as your name, e[-]mail address or billing information, or other data which can be reasonably linked to such information by Google." *Key Terms*, GOOGLE, http://www.google.com/policies/privacy/key-terms/, *archived at* http://perma.cc/Z7VR-37X5 (last visited Jan. 5, 2015).

[129] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

over to another party and thus has no expectation of privacy in the information.[130] As argued by Google (but rejected by the district court), Gmail users may not have an expectation of privacy or confidentiality in e-mail messages because Google reserves the right to access or "process" the e-mails.

[57] Although the Supreme Court has yet to address applicability of the third party doctrine to the digital world, it may have an opportunity to do so in the context of challenges to the National Security Agency's mass collection of telephony metadata that was the centerpiece of Edward Snowden's 2013 revelations regarding NSA practices.[131] The two federal courts that have addressed the constitutionality of the NSA's program to date have reached opposite results.[132]

4. E-mail Security Risks.

[58] Although some lawyers may not be concerned about Google's reliance on the third party doctrine (which was rejected by the court in the Gmail litigation), they may nonetheless have concerns regarding the more general security risks posed by unauthorized distribution of confidential e-mails by insiders and outsiders. Because e-mail can be readily forwarded either deliberately or accidentally to third parties, it is far less secure than

[130] *See id.* at 743–44.

[131] *See* THE WHITE HOUSE, ADMINISTRATION WHITE PAPER BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT (2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf, *archived at* http://perma.cc/7YMA-7ZAN.

[132] In *Klayman v. Obama*, the court found that the program was unconstitutional because technological advances have made the third party doctrine inapplicable. Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. 2013). A week later, the court in *American Civil Liberties Union v. Clapper* reached the opposite conclusion. American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013); *see also* Jack Lerner et al., *The Duty of Confidentiality in the Surveillance Age*, 17 J. INTERNET L., Apr. 2014, at 17 (arguing that lawyers' duty of confidentiality may be compromised by NSA programs and that "NSA surveillance revelations require attorneys to re-evaluate the security of communications over the Internet and 'in the cloud.'").

using postal services—as the SPE executives discovered when their embarrassing e-mails were revealed by hackers.[133] Although mail may be misaddressed or misdelivered, there is no "reply all" button for postal mail, nor is it generally subject to being stolen by malicious outsiders.

[59] As earlier discussed, hackers often use social engineering techniques, including "spear-fishing," which is typically delivered through e-mails, to try to obtain valuable or confidential information. Through these techniques, hackers may gain access not only to e-mails, but to documents containing personal, proprietary or confidential information in the entire computer system.[134]

[60] The security of e-mail also rests to a large extent on the security of passwords, which offer little protection against hackers. Like other forms of personal information, hackers are interested in passwords because they provide a means to access banking and retail accounts. Because many individuals use the same password for several accounts, hackers seek users' passwords either through "phishing" or hacks of large numbers of stored passwords. For example, a hack in 2013 of the online dating service Cupid Media "exposed more than 42 million consumer records, including names, e[-]mail addresses, unencrypted passwords and birthdays . . . ."[135] In 2012, a Russian hacker site posted 6.5 million passwords hacked from LinkedIn.[136] The "Heartbleed" bug in 2014 infected the technology that encrypts communications with websites and exposed millions of passwords.[137]

---

[133] *See* Miller, *supra* note 93.

[134] *See* Danhieux, *supra* note 30; Cooney, *supra* note 20.

[135] Brian Krebs, *Cupid Media Hack Exposed 42M Passwords*, KREBS ON SECURITY (Nov. 20, 2013), http://krebsonsecurity.com/2013/11/cupid-media-hack-exposed-42m-passwords/, *archived at* http://perma.cc/S69D-UHPN.

[136] *See* Sara Gates, *LinkedIn Password Hack: Check to See if Yours Was One of the 6.5 Million Leaked*, HUFFINGTON POST (June 7, 2012, 11:25 AM), http://www.huffingtonpost.com/2012/06/07/linkedin-password-hack-check_n_1577184.html, *archived at* http://perma.cc/HS5F-VEX3.

[61] The evolving security threats to e-mail undermine the assumptions of prior opinions finding that e-mail is an ethical means of communicating client confidential information. As with all technology, lawyers must base their considerations of what is reasonable to preserve client confidences not on past parameters, but on the current state of technology and security risks.[138] Because of current security concerns, lawyers should consider whether the use of unencrypted e-mail for sensitive and confidential communications fulfills their ethical duties.

VI. LAWYERS' USE OF CLOUD COMPUTING SERVICES

[62] "Cloud computing" is a vague and frequently misunderstood marketing term. For example, in a recent *Dilbert* cartoon the perennial malingerer Wally told the "Pointy Haired Boss," "[i]f you need me, I'll be in the cloud fixing a software issue." He also told his boss that because "[t]here's no cell coverage in the cloud, so it might seem to you as if I am at home doing nothing."[139]

[63] In point of fact, the "cloud" is not located in the sky (or in Wally's home) but is instead a name for the outsourcing of computing functions through servers owned by "cloud computing providers" and not by companies themselves.[140] Customers, including law firms, realize benefits from such outsourcing, including cost savings that "allow businesses to avoid the burden of the security and management responsibilities associated with data storage, as well as the complexities of maintaining the

[137] *See* Brian Krebs, *"Heartbleed" Bug Exposes Passwords, Web Site Encryption Keys*, KREBS ON SECURITY (Apr. 8, 2014), http://krebsonsecurity.com/2014/04/heartbleed-bug-exposes-passwords-web-site-encryption-keys/, *archived at* http://perma.cc/4CM7-RP8M.

[138] *See* Bolin, *supra* note 89, at 622.

[139] Scott Adams, *Comics*, DILBERT (Dec. 8, 2014), http://www.dilbert.com/2014-12-08/, *archived at* http://perma.cc/G8L6-P5MQ.

[140] *See* Kenneth L. Bostick, *Pie in the Sky: Cloud Computing Brings an End to the Professional Paradigm in the Practice of Law*, 60 BUFF. L. REV. 1375, 1381–82, 1384–85 (2012).

infrastructure under which the data is held."[141]

[64] According to the working definition of the National Institute of Standards and Technology (NIST), "[c]loud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [142] There are several varieties of cloud computing services, including: cloud software as a service (SaaS), which allows users to run software through a cloud infrastructure; cloud platform as a service (PaaS), which allows users to run their own applications using the programming language provided by the service; and cloud infrastructure as a service (IaaS), which allows "the consumer . . . to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications."[143]

[65] The most frequent law firm uses of the cloud are running software applications (such as word processing, spreadsheets, and accounting) and storing documents. For example, lawyers, like other consumers, may use Amazon's Simple Storage Service (Amazon S3) to store documents,[144] or Google's Docs, Sheets and Slides (available through Google's web browser Chrome) to create documents, spreadsheets and presentation slides.[145] Such services are generally referred to as "public clouds," in

[141] *Id.* at 1376; *see also* Trope & Hughes, *supra* note 110, at 164–65 (describing the history of use of cloud services); Woods, *supra* note 5 (describing the exponential growth of cloud computing services in recent years).

[142] PETER MELL & TIMOTHY GRANCE, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, *archived at* http://perma.cc/ENM9-B4MQ.

[143] Trope & Hughes, *supra* note 110, at 168.

[144] *See Amazon S3*, AMAZON, https://aws.amazon.com/s3/, *archived at* https://perma.cc/2L3D-5TED (last visited Feb. 7, 2015).

other words, services offered to the general public.[146] In addition, law firms may also use free document sharing services—such as Dropbox or Box—for a wide variety of purposes.[147]

[66] Law firms also make use of "private clouds," which are off-site servers not generally available to the public which the firm pays a third party to manage.[148] Law firms use private clouds for wide variety of services, including accounting, software, and storage of documents.[149] Although the following discussion concentrates on the use of the public cloud, it applies in certain respects—including security and control issues—to private clouds.

A. Ethics of Lawyers' Use of Public Cloud Computing Services

[67] Bar organizations have generally concluded that lawyers may entrust confidential documents to cloud computing providers if certain conditions are met. The nineteen different state bodies[150] that have

[145] *See Edit Office Files in Google Docs, Sheets, and Slides*, GOOGLE, https://support.google.com/docs/answer/6049100?hl=en, *archived at* https://perma.cc/35UT-4WTP (last visited Feb. 7, 2015).

[146] *See* Trope & Hughes, *supra* note 110, at 170.

[147] *See Law Firm File Sharing in 2014*, LEXISNEXIS 6 (May 28, 2014), *available at* http://www.slideshare.net/BusinessofLaw/lexisnexis-2014-survey-of-lfile-sharing-survey-report-final, *archived at* http://perma.cc/Z8KM-WAK6. The report also found that lawyers were often unaware of whether other lawyers in their firm used file-sharing services. *Id*. at 7.

[148] *See* Trope & Hughes, *supra* note 110, at 170.

[149] *See* Stephanie L. Kimbro & Tom Mighell, *Popular Cloud Computing Services for Lawyers: Practice Management Online*, L. PRAC. MAG., Sept./Oct. 2011, *available at* http://www.americanbar.org/publications/law_practice_magazine/2011/september_october/popular_cloud_computing_services_for_lawyers.html, *archived at* http://perma.cc/WEW7-2HWS (listing numerous cloud applications available to lawyers).

reviewed the issue to date have found cloud computing ethical if lawyers "take reasonable steps to ensure that their law firm's confidential data is protected from unauthorized third party access."[151]

[68] For example, Iowa Ethics Opinion 11-01, which addressed issues of confidentiality in the cloud, concluded that

> A lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. 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.[152]

---

[150] *See Cloud Ethics Opinions Around the U.S.*, ABA, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html, *archived at* http://perma.cc/TJU8-JQF2 (last visited Jan. 5, 2015).

[151] Nicole Black, *The Ethics of Cloud Computing for Lawyers*, ABA (2012), *available at* http://www.americanbar.org/publications/gpsolo_ereport/2012/september_2012/ethics_cloud_computing_lawyers.html, *archived at* http://perma.cc/B285-7NAD; *see also* Thomas G. Wilkinson Jr., *Ethics Digest*, 34 PA. LAW. 49, 49 (2012) (discussing Pennsylvania Bar Association Legal Ethics and Professional Responsibility Committee Formal Opinion 2011–200); Robert Ambrogi, *Cloud Ethics Opinions: A Full List (Maybe)*, LAW SITES BLOG (May 23, 2014), http://www.lawsitesblog.com/2014/05/cloud-ethics-opinions-full-list.html, *archived at* http://perma.cc/5SLB-W8WR.

[152] Letter from Nick Critelli, Comm. Chair, Iowa State Bar Ass'n Ethics & Practice Guidelines Comm., to Dwight Dinkla, Exec Dir. Iowa State Bar Ass'n (Sept. 9, 2011) (quoting Iowa R. of Prof'l Conduct 32:1.6), *available at* http://www.wicsec.org/wp-content/uploads/2011%20WICSEC%20Conference%20Materials/M-6%20Iowa%20Bar%20Ethics%20Opinion%209911%20-%20Worley,%20Peiper.pdf, *archived at* http://perma.cc/NTS7-5CAH; Black, *supra* note 151 (analyzing Iowa State Bar Association's opinion).

[69] Opinion 842 of the New York State Bar Association Committee on Professional Ethics similarly addressed the ethical propriety of cloud computing.[153] Opinion 842 concluded that use of online systems to store confidential information implicated Rule 1.6's confidentiality requirement, but found that a lawyer can use a cloud service to store client files "provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained."[154]

[70] Opinion 842 found that necessary "[r]easonable care . . . may include consideration" of four issues:

> (1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
> (2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
> (3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or
> (4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.[155]

[153] *See* New York State Bar Comm. on Prof'l Ethics, Op. 842 (2010), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&ContentID=140010&template=/CM/ContentDisplay.cfm, *archived at* http://perma.cc/P6P8-CJKR (using outside online storage provider to store client confidential information).

[154] *Id.*

[155] *Id.*

[71] Opinion 842 cautioned that "[t]echnology and security of stored data are changing rapidly" and that "the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology."[156] The lawyer also has the duty, if he or she learns that security measures are ineffective, to "investigate whether there has been any breach of his or her clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated."[157] Lawyers must also monitor the law relating to technology, which "is changing rapidly," to see "when using technology may waive an otherwise applicable privilege."[158]

[72] New York Opinion 842 echoes the approach to technology taken in California Ethics Opinion 2010-179.[159] Although the California opinion dealt with the propriety of a lawyer using public and home wireless technology, its conclusion that lawyers must be cognizant of the effect of changing technology and security threats is equally applicable to cloud computing. As Opinion 2010-179 states, "[t]he greater the sensitivity of the information, the less risk the attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent."[160] Moreover, "if a particular technology lacks essential security features, use

[156] *Id.*

[157] *Id.*

[158] *Id.* (citing City of Ontario v. Quon, 560 U.S. 746, 762–63 (2010) (dealing with expectations of privacy in mobile technology as an example of changes that may affect privilege)).

[159] *See* Trope & Hughes, *supra* note 110, at 192–93.

[160] State Bar of California Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836, *archived at* http://perma.cc/4BKQ-HL3Z.

of such a technology could be deemed to have waived [attorney-client] protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considering in determining waiver."[161]

B. Security Risks of Lawyers' Use of Public Cloud Computing Services

[73] Although the California, Iowa and New York ethics opinions require lawyers to assess—and continue to assess—the security features of cloud computing providers, lawyers may have difficulties in fulfilling this obligation with major public cloud providers. As with e-mail, the standard policies of many public cloud providers—including Amazon and Google—make it challenging for lawyers to determine whether these services have the security measures required by ethics opinions.

[74] For example, Google's TOS states that Google provides its services "using a commercially reasonable level of skill and care."[162] Notwithstanding this commitment, Google's TOS states (in all capital letters) "NEITHER GOOGLE NOR ITS SUPPLIERS OR DISTRIBUTORS MAKE ANY SPECIFIC PROMISES ABOUT THE SERVICES. FOR EXAMPLE, WE DON'T MAKE ANY COMMITMENTS ABOUT THE CONTENT WITHIN THE SERVICES, THE SPECIFIC FUNCTIONS OF THE SERVICES, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICES 'AS IS.'"[163] Google also excludes all warranties and further states (again in all capital letters) "WHEN PERMITTED BY LAW, GOOGLE AND GOOGLE'S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA, FINANCIAL LOSSES OR INDIRECT, SPECIAL CONSEQUENTIAL, EXEMPLARY, OR

[161] *Id.*; *see also* Trope & Hughes, *supra* note 110, at 192–93 (discussing the applicability of ethical opinions to cloud computing).

[162] *Google Terms of Service*, *supra* note 108.

[163] *Id.*

PUNITIVE DAMAGES."[164]

[75] Under the heading "Business uses of our Services," Google's TOS states that a "business accepts these terms" and

> [W]ill hold harmless and indemnify Google and its affiliates, officers, agents, and employees from any claim, suit or action arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, suits judgments, litigation costs and attorneys' fees.[165]

[76] Google's TOS also incorporates the company's privacy policy,[166] which includes a section on "information security" stating that, generally, "[w]e work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold."[167] Google's privacy policy also states that it encrypts certain services using Secure Sockets Layer (SSL), offers two step verification and a safe browsing feature in Google Chrome, and reviews its "information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems."[168] Finally, Google restricts "access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations."[169]

[164] *Id.*

[165] *Id.*

[166] *Id.*

[167] *Privacy Policy*, *supra* note 127.

[168] *Id.*

[169] *Id.*

[77] Google's TOS and Privacy Policy do not provide any means for an attorney using Google's services to measure or assess the company's protection of confidential information stored or processed through the services. Not only does Google expressly decline to make any specific promises about its services—including the security of information stored on Google servers—it also requires business users to indemnify Google for any lawsuits "arising from or related to the use of the Services."[170]

[78] Google's Privacy Policy also makes no commitments regarding security of customers' information. Indeed, whatever restrictions the privacy policy places on dissemination of information are restricted to "personal information,"[171] which is a considerably narrower category than information that lawyers may consider to be confidential. Google's "license" to the content of documents stored on its servers and its right to make "derivative works" are also troublesome from the point of view of maintaining client confidentiality for information stored on Google's services.[172]

[79] Amazon similarly limits its liability for its "cloud drive," which provides remote storage for documents, by stating that

> (a) in no event will our or our software licensors' total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) arising

[170] *Google Terms of Service*, *supra* note 108.

[171] *See Key Terms*, *supra* note 128 (defining "personal information" as "information which you provide to us which personally identifies you, such as your name, e[-]mail address or billing information, or other data which can be reasonably linked to such information by Google.").

[172] *See* Trope & Hughes, *supra* note 110, at 248–50 ("There are probably few, if any, clients that would be willing to agree to grant a cloud vendor a right to any content that the client may generate or that its attorneys may generate through the use of a cloud-based, word-processing program such as Google Docs. A lawyer or law firm would certainly also be unwilling to agree to grant such a license.").

> out of or related to your use or inability to use the Software exceed the amount of fifty dollars ($50.00);
> (b) in no event will our total liability to you for all damages arising from your use of the Service or information, materials or products included on or otherwise made available to you through the Service (excluding the Software), exceed the amount you paid for the Service related to your claim for damages; and
> (c) we have no liability for any loss, damage or misappropriation of Your Files under any circumstances or for any consequences related to changes, restrictions, suspensions or termination of the Service or the Agreement. These limitations will apply to you even if the remedies fail of their essential purpose.[173]

Cloud service providers like Google and Amazon also make it difficult for attorneys to assure that they will be informed by the providers of any breach of security in the system. Under Google and other providers' TOS, there is "no assurance that a customer would be given any explanation of faults in the system."[174] Moreover, most public cloud computing providers, like Amazon and Google, make no commitments regarding the preservation and retrieval of documents from their services nor do they affirmatively state that they will provide information to users about security compromises.[175] "It is, therefore, questionable whether a lawyer or law firm who relinquishes control over the storage of its data would be acting reasonably when it has little to no control over security breaches."[176] Because state data breach notification laws pertain only to personal data, there is no legal obligation for public cloud providers to

[173] *Amazon Cloud Drive Terms of Use*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?nodeId=201376540, *archived at* http://perma.cc/KJX3-GMVS (last updated Nov. 11, 2014).

[174] Trope & Hughes, *supra* note 110, at 201–02.

[175] *See id.* at 206–07 (noting that Amazon's agreement removed any such assurances).

[176] *Id.* at 220–21.

provide notice to users regarding compromise of non-personal data such as confidential documents stored on a service.[177]

[80] Cloud computing also entails more general security concerns. A 2010 article by Christopher Soghoian argues that security concerns are inherent to cloud computing and thus "render[] the cloud computing model fundamentally unfit for the practice of law."[178] These "inherent" risks include transmittal of user names and passwords to servers via unencrypted network connections, transmittal of data that "'can easily be snooped on by hackers'" and encryption that is restricted to initial login information.[179] The Cloud Security Alliance has also assembled a list of the top nine security risks to the cloud: "(1) [d]ata [b]reaches; (2) [d]ata [l]oss;" (3) account [or service traffic] hijacking; (4) insecure [interfaces and] APIs; "(5) [d]enial of [s]ervice; (6) [m]alicious [i]nsiders; (7) [a]buse of [c]loud [s]ervices; (8) [i]nsufficient [d]ue [d]iligence;" and "(9) [s]hared [t]echnology [i]ssues."[180] Although these threats are not unique to the cloud, they demonstrate that lawyers do not avoid security issues when using the cloud any more than they do with their own in-house computing services.

VII. LAWYERS' USE OF E-MAIL, CLOUD COMPUTING, AND TECHNOLOGY

[81] Given the security challenges to confidential information sent through e-mails or stored with public cloud providers, lawyers should exercise greater care using these technologies than they have done in the

[177] *See id.* at 219–21.

[178] Bostick, *supra* note 140, at 1380.

[179] *Id.* at 1395–96 (citing Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 372 (2010)).

[180] CLOUD SECURITY ALLIANCE, THE NOTORIOUS NINE: CLOUD COMPUTING TOP THREATS IN 2013 6–7 (2013), *available at* https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf, *archived at* https://perma.cc/KBX2-A7R4.

past. Although ethics bodies have approved the use of both e-mail and cloud computing, they have done so with the important proviso that lawyers must reassess the propriety of using the technologies as both the technology and security risks continue to evolve. What may have been "reasonable" security in the past may no longer be adequate. Given risks of exposure of confidential documents and e-mails—as exemplified by the SPE breach—lawyers should consider whether it is appropriate to entrust highly confidential client information to unencrypted e-mail and cloud services.

[82] Although encryption is increasingly inexpensive and is used in many businesses, it is not yet widely used by lawyers.[181] But as lawyers come to understand the inherent security risks in e-mail and in cloud computing, they should consider using encryption, particularly for e-mails and documents containing sensitive information, such as client confidential documents and protected health information under HIPAA.[182]

[83] Like their clients, lawyers must put their own houses in order by implementing security measures and incident responses plans for security incidents and their aftermath.[183] A key aspect of security preparedness is training law firm personnel, including lawyers themselves. Even senior partners are not immune to phishing attacks and misuse of public document sharing sites—such as Dropbox or Box—which are "built to handle consumer data, with no true security safeguards, no ability to audit,

[181] *See Law Firm File Sharing in 2014*, *supra* note 147, at 1 (indicating that 89% of firms reported using e-mail and 74% use it on a daily basis, but that lawyers generally do not use encryption and instead use confidentiality statements in the e-mails); Scott Aurnou, *Lawyers and Email: Ethical & Security Considerations*, SECURITY ADVOCATE (July 8, 2014), http://www.thesecurityadvocate.com/2014/07/08/lawyers-and-email-ethical-security-considerations/, *archived at* http://perma.cc/9A5T-4RU3 (noting that confidentiality statements "essentially do[] nothing to protect firm or client data from any nefarious actors who view it . . . .").

[182] *See* Aurnou, *supra* note 181.

[183] *See id.* (discussing the need of lawyers and law firms to put in place security response plans).

and no redundancy or backups."[184]

[84] Law firms should also assess whether they need to put into place policies and procedures prohibiting certain practices that increase the danger of dissemination of confidential information. These policies may encompass topics such as using public cloud providers or file sharing services for sharing documents, the use of web-based e-mail services, and use of public cloud computing providers for sensitive documents. Instead of using public cloud services, lawyers might use "enterprise-grade file sharing services that focus on the security and protections designed with law firms in mind."[185] As earlier noted, if lawyers do use public storage or file sharing services, they should consider using encryption for confidential or proprietary documents.[186]

[85] Given recent ethical opinions, it is clear that lawyers must also continue to keep abreast of security risks posed by technology to fulfill their duties of competence and confidentiality. Although not every lawyer must be a specialist in technology, the days when some in the profession could afford to be technophobes are over. Like their clients, lawyers share the burden of preserving sensitive and proprietary data against attacks and unauthorized exposure.

[184] Bobby Kuzma, *Security in Era of Mobile Devices and Cloud Computing, in* 14 PRACTICE INNOVATIONS 15 (2013), *available at* https://info.legalsolutions.thomsonreuters.com/signup/newsletters/practice-innovations/2013-jan/Jan13_PracticeInnovations.pdf, *archived at* https://perma.cc/Q5UK-6GD5.

[185] *See Law Firm File Sharing in 2014*, *supra* note 147, at 9 (finding that 64.9% of firms do not provide an enterprise-grade filing service.).

[186] *See* Aurnou, *supra* note 181 (noting that DropBox and Google Drive are not suitable options for lawyers).