13

Intellectual Property Issues Raised by E-mail

Michael B. Smith  
Lupkin & Associates PLLC  
New York, New York

Sara Anne Hook  
Indiana University School of Informatics and Computing  
Indianapolis, Indiana

Aly Dossa  
Osha Liang LLP  
Houston, Texas

I. Introduction .................................. ........................ ..
   A. History of Electronic Messages ........................ .
   B. Technical Overview ........................................... .
   C. Future of Electronic Communication ............. .

II. Issues Arising Out of Permissible Use of E-mail...  
   A. Privacy/Confidentiality.................................
      1. Work vs. Home ............................................ ..
   B. Discovery..................................................
      1. Attorney-Client Privilege ............................. .
      2. Possession/Custody/Control ........................... .
   C. Cross-Border Issues..................................

III. Issues Arising Out of Impermissible Use of E-mail... 
   A. Spam ..................................................

Main Volume  Supplement
-------------  ------------
703  ----
703  ----
703  ----
704  ----
704  365
704  365
706  375
709  384
712  389
712  393
717  401
720  404
722  410
722  410
II. ISSUES ARISING OUT OF PERMISSIBLE USE OF E-MAIL

A. Privacy/Confidentiality

[Add the following text at the end of the section.]

Several bills introduced in Congress over the last few years reflect the public’s continued concerns over what should be considered permissible with respect to accessing a person’s e-mail and other electronic
information. H.R. 537, the Social Networking Online Protection Act,\(^1\) reminiscent of legislation with the same title that was proposed in 2012, responds to the growing trend of employer requests for information that would allow access to personal social media or private e-mail accounts, including as part of the hiring process or as a basis for adverse action if an employee or applicant refuses to provide this information.\(^2\) The bill summary notes that the Act

\[\text{[p]}\text{prohibits employers from: (1) requiring or requesting that an employee or applicant for employment provide a user name, password, or any other means for accessing a private e-mail account or personal account on a social networking Web site; or (2) discharging, disciplining, discriminating against, denying employment or promotion to, or threatening to take any such action against any employee or applicant who refuses to provide such information, files a compliant [sic] or institutes a proceeding under this Act, or testifies in any such proceeding.}\(^3\)

An additional provision in the proposed legislation would amend the Higher Education Act of 1965 and the Elementary and Secondary Education Act of 1965 "to prohibit certain institutions of higher education and local educational agencies from requesting such password or account information from students or potential students."\(^4\) The bill also forbids a variety of retaliatory actions against employees, applicants, students and potential students who refuse to provide the information or who seek redress through filing a complaint, instituting a proceeding, or testifying in a proceeding.\(^5\) Both civil penalties and injunctive relief would be available.\(^6\)

Another piece of legislation, introduced in May 2013, responds directly to the privacy concerns with e-mail communications that are provided through or stored by third-party and cloud computing service providers. H.R. 1852, the E-mail Privacy Act,\(^7\) would "amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes."\(^8\) Among the various provisions in the proposed legislation are confidentiality of electronic communications,

\(^4\)Id.
\(^6\)Id. §2(b)(1), (b)(2).
elimination of the 180-day rule, requirements for search warrants, required disclosure of customer records, delay of notification, evaluation by the government accountability office and rules of construction. Clearly a response to the recent events surrounding the disclosures from Edward Snowden about NSA surveillance, H.R. 2399 Limiting Internet and Blanket Electronic Review of Telecommunications and E-mail Act, or LIBERT-E Act, was introduced on June 17, 2013. The bill is intended to "prevent the mass collection of records of innocent Americans under section 501 of the Foreign Intelligence Surveillance Act of 1978, as amended by §215 of the USA PATRIOT Act, and to provide for greater accountability and transparency in the implementation of the USA PATRIOT Act and the Foreign Intelligence Surveillance Act of 1978." Among the many provisions outlined in the legislation are: amending Section 501 of the Foreign Intelligence Surveillance Act of 1978 with respect to access to certain business records for foreign intelligence and international terrorism investigations; amending Section 601 of the Foreign Intelligence Surveillance Act of 1978 to provide additional disclosures to Congress and the public; requiring a report on the impact on the privacy of people located in the United States by provisions related to certain business records and targeting of non-United States persons outside of the United States; and a new paragraph added to Section 702(1) of the Foreign Intelligence Surveillance Act of 1978 on the forms of assessments and reviews.

The Personal Data Privacy and Security Act of 2014 is a far-reaching bill that enhances penalties for identity theft and other violations of data privacy and security, sets requirements for business entities engaging in interstate commerce related to the privacy and security of personally identifiable information, and provides for compliance of the budgetary effects of the Act with the Statutory Pay-As-You-Go Act. In addition, this legislation defines "sensitive personally identifiable information" to include:

(1) specified combinations of data elements in electronic or digital form, such as an individual's name, home address or telephone number, mother's maiden name, and date of birth; (2) a non-truncated social security

---

9 Id.
13 Id. §1871.
14 Id. §1881a.
15 Id. It will be especially interesting to monitor these three pieces of legislation as they move forward and to consider the extent to which e-mail continues to be a major method of communication for employees, companies, law firms, students and citizens and is thus worthy of vigilance in security and privacy practices.
number, driver's license number, passport number, or government-issued unique identification number; (3) unique biometric data; (4) a unique account identifier; and (5) any security code, access code, password, or secure code that could be used to generate such codes or passwords.\(^9\)

Although e-mail is not mentioned specifically in the definition of "sensitive personally identifiable information," it is discussed in the provisions of the legislation that address the requirements for notification in the event of a breach:

Sec. 213. METHODS OF NOTICE.

An agency or business entity shall be in compliance with section 211 if it provides the following:

(1) Individual notice.—Notice to individuals by one of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the agency or business entity.

(B) Telephone notice to the individual personally.

(C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).\(^10\)

A bill with similar provisions that was introduced in February 2014 is S. 1995, the Personal Data Protection Act and Breach Accountability Act of 2014.\(^20\) In addition to the contents of H.R. 3990 and S. 1897, the bill adds Title III, Access to and Use of Commercial Data. Among the interesting provisions of this bill are a number of requirements for federal agencies that could serve as best practices when dealing with contractors, third-party business entities, and data brokers:

Requires federal agencies to: (1) evaluate and audit the information security practices of contractors or third party business entities that support the information systems or operations of such agencies involving sensitive personally identifiable information, and (2) ensure remedial action to address any significant deficiencies.

---


Requires federal agencies to conduct a privacy impact assessment before purchasing or subscribing to personally identifiable information from a data broker. Requires the Comptroller General to report on federal agency adherence to key privacy principles in using data brokers of commercial databases containing sensitive personally identifiable information.21

A more narrowly tailored bill, H.R. 4157, the Farmer Identity Protection Act,22 indicates that a wide variety of citizens have specific concerns about privacy, including the privacy of their e-mail addresses. The Act, introduced in March 2014, would prohibit:

the Environmental Protection Agency (EPA), or any EPA contractor or cooperator, from disclosing the information of any owner, operator, or employee of a livestock operation provided to EPA by a livestock producer or a state agency in accordance with the Federal Water Pollution Control Act (commonly known as the Clean Water Act) or any other law, including: (1) names; (2) telephone numbers; (3) e-mail addresses; (4) physical addresses; (5) global positioning system coordinates; or (6) other information regarding the location of the owner, operator, livestock, or employee.23

Privacy continued to be a concern of Congress during 2015 in the aftermath of the Edward Snowden revelations and with the expiration of various provisions of the USA PATRIOT Act. With respect to privacy issues related specifically to e-mail, several bills were proposed during the 114th Congress (2015-2016). For example, H.R. 1704, the Personal Data Notification and Protection Act of 2015 “[r]equires certain businesses that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information about more than 10,000 individuals during any 12-month period to notify individuals whose information is believed to have been accessed or acquired through a discovered security breach.”24 In terms of e-mail, the bill “[d]irects businesses, within 30 days after discovery of a breach, to notify: (1) affected individuals by mail, telephone, or e-mail; and (2) major media outlets if the number of affected residents of a state exceeds 5,000.”25

Another bill more specifically dealing with e-mail is intended to avoid the issues when federal government employees and agencies use personal e-mail to conduct official government business. Thus, H.R. 1152, the IRS Email Transparency Act, “[p]rohibits any officer or employee of the Internal Revenue Service from using a personal e-mail account to conduct official business.”26 This same restriction on the use of personal e-mail

21 Id.
25 Id.
accounts was included in a previous bill, H.R. 3520, the Exempt Organization Simplification and Taxpayers Protection Act of 2013.\(^{27}\)

The proposed legislation that most specifically targets privacy issues with e-mail is H.R. 699, the Email Privacy Act.\(^{28}\) Among its most important provisions are:

Amends the Electronic Communications Privacy Act of 1986 to prohibit a provider of remote computing service or electronic communication service to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions.

Revises provisions under which the government may require a provider to disclose the contents of such communications. Elimination of the different requirements applicable under current law, depending on whether such communications were: (1) stored for fewer than, or more than, 180 days by an electronic communication service or (2) held by an electronic communication service as opposed to a remote computing service.

Requires the government to obtain a warrant from a court before requiring providers to disclose the content of such communications regardless of how long the communication has been held in electronic storage by an electronic communication service or whether the information is sought from an electronic communication service or a remote computing service.\(^{29}\)

Related bills include H.R. 283, the Electronic Communications Privacy Act Amendments Act of 2015\(^{30}\) and S. 356, the Electronic Communications Privacy Act Amendments Act of 2015.\(^{31}\)

In their article, Hadjipetrova and Poteat discuss why the absence of a baseline federal privacy law is resulting in states becoming primary legislative and policing authorities in the area of privacy and data security.\(^{32}\) They provide an overview of recent state legislative actions, with special emphasis on the so-called “California effect,” especially its impact on the Internet.\(^{33}\) They also describe the activities of state attorneys general as chief privacy officers and enforcers as well as their cooperation with the FTC and across state borders.\(^{34}\) In his article, Curb reveals how e-mail is often the first step of a social engineering attack that is designed to give the victim a false sense of security so that he or she trusts the sender

---


\(^{29}\) Id.


\(^{32}\) Ganka Hadjipetrova & Hannah G. Poteat, States Are Coming to the Fore of Privacy in the Digital Era, LANDSLIDE 12-17, 71 (July/Aug. 2014).

\(^{33}\) Id. at 14-16.

\(^{34}\) Id. at 16-17.
enough to be willing to click on a link that is infected with malware that will install a virus.\textsuperscript{35}

Two helpful articles address how to keep data secure, including data that is transmitted via e-mail. First, Nelson and Simek provide a helpful discussion of some of the risks with the most commonly used e-mail systems, Gmail and Microsoft Exchange Server, as well as wireless communications, smartphones, tablets, cloud services, and documents.\textsuperscript{36} Their primary recommendation, which is especially useful for e-mail, is to use encryption.\textsuperscript{37} Similarly, Bilinsky discusses the importance of encryption for e-mail as well as the options for secure client portals and third-party secure services and risks related to Wi-Fi and mobile computing.\textsuperscript{38}

Dryer offers a comprehensive summary of the revisions to Rules 1.1 and 1.6 and the potential ethical issues that are created, specifically as they relate to communicating with clients, electronically stored information, social media, and data management.\textsuperscript{39} He discusses particular issues concerning the security and confidentiality of e-mail, including the risks of “reply all,” “blind copy,” and “autofill” and notes that although some encryption services will protect the contents of e-mail, they may still leave a trail of metadata as the e-mail is routed through a third-party server.\textsuperscript{40}

Congress and the administration have continued to grapple with issues related to e-mail during 2015–2016. As reported by Moyer in March 2016,

Congressional support for the modernization legislation called the Email Privacy Act has grown since its introduction several years ago. More than 300 House members today are co-sponsors of the measure, a number greater than any other bill pending in the House of Representatives and a reflection of the breadth of bipartisan support for privacy protection.

Introduced in the House by Rep. Kevin Yoder (R-Kan.) and in the Senate by Patrick Leahy (R-Vt.), the Email Privacy Act (H.R. 699 and S. 356) would change the framework for law enforcement access to email (and texts and other electronic content) housed with Internet service providers, like Google and Yahoo, and bring the statute in line with the Sixth Circuit’s opinion in \textit{United States v. Warshak}, 631 F.3d 266 (6th Cir. 2010), which requires the government to obtain a warrant to access emails, regardless of their age.\textsuperscript{41}

The author notes that the last time Congress updated e-mail privacy laws was in 1986 when it established the Electronic Communications

\textsuperscript{35}Tommy Curb, \textit{Defend Against Social Engineering Attacks}, PEER TO PEER 6–7 (Winter 2014).
\textsuperscript{37}Id. at 2–3.
\textsuperscript{40}Id. at 14–15.
Privacy Act (ECPA), which was intended to protect wire, oral, and electronic communications when those communications were being made, were in transit, and when stored on computers and includes e-mail, telephone conversations and data stored electronically. However, he observes that these distinctions and the motivation for the ECPA "have been outpaced by technology." As an example, he indicates that the ECPA permits the government to access e-mail messages without a warrant if they are stored by the service provider for more than 180 days, but a court-imposed warrant must be secured for e-mail messages that are stored for fewer than 180 days, a distinction that is quite outdated.

Another significant piece of legislation that impacts privacy protection is the Federal Cybersecurity Information Sharing Act (CISA), signed into law on December 15, 2015, as part of the December 2015 omnibus legislation. Per the authors:

To address privacy and civil liberty concerns, CISA requires that the federal government retain, use, and disseminate cyber threat information in a way that protects any personally identifiable information contained within cyber threat indicators from unauthorized use or disclosure. Further, CISA restricts the government's disclosure, retention, and use of cyber threat information to certain enumerated purposes. Use of cyber threat information will also be subject to forthcoming policies, procedures, and guidelines governing the sharing of cyber threat information. These requirements will incorporate security controls intended to protect against unauthorized access to or acquisition of the cyber threat information.

The new legislation also has requirements for businesses, the U.S. Attorney General, and the Secretary of Homeland Security.

Among the federal administration's efforts on cybersecurity in 2015 and its plans for 2016 were raising the level of cybersecurity in both the public and private sector, disrupting and deterring malicious activity in cyberspace, and improving incident response and resilience.
Two other interesting pieces of legislation have been proposed since the 2015 Supplement that specifically address issues with e-mail and privacy. First, H.R. 3743 Securing Every Relevant and Vital Electronic Record Act of 2015 (the SERVER Act) would prohibit the Secretary of a cabinet-level executive department from maintaining a private email server to conduct official government business. The Inspector General of each such department shall ensure compliance with such prohibition. A Secretary who violates such prohibition is subject to a fine and/or prison term and shall forfeit his or her office and be disqualified from holding any U.S. government office.\(^50\)

A second bill is H.R. 4709, the Unsubscribe From All Act of 2016. Per the Summary,

This bill amends the CAN-SPAM Act of 2003 to require commercial email messages to contain an "unsubscribe from all" option that recipients may select, with not more than one additional action required by the recipient, to send a reply requesting not to receive future emails from the sender.

A commercial email message must remain capable of receiving such unsubscribe replies for at least 30 days after the transmission of the original message.\(^51\)

Concerns with security in law firms continue to be reflected in the ABA 2015 Legal Technology Survey Report, as distilled into a concise summary by David Ries.\(^52\) As he reports in his introduction, "[L]aw firm data breaches are continuing. It was recently reported that at least 80% of the largest 100 law firms, by revenue, have been hacked since 2011." In terms of the 2015 Survey, data security is addressed most directly in Volume I, Technology Basics, but also in Volume IV, Web and Communications Technology, and Volume VI, Mobile Lawyers.\(^53\) After discussing the lawyer's duties for information security under ABA Model Rules 1.1 and 1.6, particularly Comment 18 to Rule 1.6, the author notes that according to the 2015 Survey, "about 15% of respondents overall reported that their firms had experienced a security breach at some point," which includes lost or stolen computers or smartphones, hackers, break-ins or exploitation of the Web site. As he observes, "[T]he most serious consequence of a data breach for a law firm would most likely be unauthorized access to sensitive client data" which the statistics indicate fortunately appears to be low.\(^54\) How-


\(^{53}\) Id. at 1.

\(^{54}\) Id. at 1-2.

\(^{55}\) Id.
ever, the author cautions that this is likely because a high percentage of respondents do not even know whether their law firm has experienced a data breach.\textsuperscript{57} As he notes, the other consequences of data breaches are significant and reported in 20–30% of incidents. These consequences include downtime/loss of billable hours, the expense of replacing hardware and software, consulting fees for repair, destruction or loss of files, and expenses to notify clients of a breach.\textsuperscript{58} Ries devotes the remainder of his summary to report the findings of the 2015 Survey on security programs and policies, cyber insurance coverage, authentication and access control, encryption, use of basic security tools, and disaster recovery/business continuity.\textsuperscript{59}

With respect to cyber insurance, Nelson and Simek have recently published an important article indicating that there has been a rapid evolution in these types of policies and urging law firms to think about costs and coverage.\textsuperscript{60} The article includes a list of questions that a prospective insurer may ask about the law firm and its security practices and offers advice on what kind of coverage to look for.\textsuperscript{61} The authors conclude the article with a discussion of how insurers will try to avoid being liable for a cybersecurity incident.\textsuperscript{62} As they indicate, insurers are starting to cover only data theft, not negligence. For example, if an employee loses an unencrypted laptop with sensitive data, some policies will not cover the breach.\textsuperscript{63} This is especially important because statistics suggest that one of the most common cybersecurity incidents is the theft or loss of portable devices.

Fortunately, resources continue to be made available to help law firms manage their own security as well as provide guidance to clients. For example, after providing statistics on why law firms are attractive targets for cybercriminals, Hernandez\textsuperscript{64} describes spear phishing, ransomware, fake apps, and malicious social network links as some of the potential threats that law firms can face.\textsuperscript{65} Among the specific security measures he recommends that law firms take to protect themselves online are creating a strong password policy, conducting due diligence with cloud computing vendors, developing a Bring Your Own Device (BYOD) policy (see Section II.A.1 below), enacting policies for dealing with lost or stolen devices, and making staff aware of social engineering.\textsuperscript{66} Additional information on how to recognize and guard against social engineering is provided

\textsuperscript{57} Id.
\textsuperscript{58} Id. at 2–3.
\textsuperscript{59} Id. at 3–7.
\textsuperscript{61} Id. at 4–6.
\textsuperscript{62} Id. at 6.
\textsuperscript{63} Id.
\textsuperscript{65} Id. at 45–48.
\textsuperscript{66} Id. at 48–50.
by Ho, with suggestions that include using complex passwords that are not based on actual words, using obscure knowledge-based authentication questions and answers, hovering over before clicking on hyperlinks, thinking before posting on public social networks, and asking the caller if he/she can be called back.\footnote{Bill Ho, \textit{Have You Been Socially Engineered?}, \textsc{Peer to Peer} 32–33 (Winter 2015).}

Because e-mail continues to be the most common method of communicating in the business world, Nelson and Simek provide a comprehensive and practical article on encryption of e-mail.\footnote{Sharon D. Nelson & John W. Simek, \textit{E-mail Encryption}, \textsc{Sensei Enterprises} (2015), http://senseient.com/wp-content/uploads/E-mail-Encryption-for-Fee-Simple.pdf (last visited June 28, 2016).} Additional guidance on privacy and information security for lawyers is provided by The Sedona Conference, which has been a leader in issuing principles and best practices in a variety of complex areas of the law, including electronic discovery, intellectual property rights, and antitrust. In November 2015, it issued its \textit{Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers}.\footnote{The Sedona Conference, \textit{Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers} (Nov. 2015), https://thesedonaconference.org/publication/sedona-conference-commentary-privacy-and-information-security-principles-and-guidelines (last visited June 28, 2016).} Among the topics covered are the sources of the duty to protect private and confidential information, conducting a risk assessment, and guidelines for policies and practices that address privacy and information security, along with appendices for privacy and security in the health care and financial services industries. Within the section for policies and practices are six steps: identifying the types and sources of information that must be protected, determining who needs access, information security policies and practices, processes for timely disposition of records and information, implementing a training program, and preparing for a significant security incident.

Although security in law firms may seem daunting and the statistics may be discouraging, it has resulted in some positive news in an otherwise difficult legal job market. Among the most promising alternative legal careers are legal technology, risk management, compliance, and data protection.\footnote{Richard L. Hermann, \textit{10 Hottest Alternative Legal Careers}, \textsc{The National Jurist} 12–13 (Winter 2016).}

1. \textit{Work vs. Home}

[Add the following text at the end of the section.]

A number of recent articles should heighten an attorney's awareness of the significant risks to information security and confidentiality posed by the use of mobile devices, which are typically the means by which e-mail is exchanged. Often, the issue is not the technology itself, but human behavior that causes mobile devices to be lost or stolen at alarming rates. Law firms are only beginning to grapple with some of these issues. Nelson and Simek, who are experts in information security and privacy matters, provide a number of helpful recommendations for security when using smartphones, with a reminder that attorneys have an ethical obligation to protect confidential client information. They also advise attorneys to be aware of the changes to the ABA Model Rules of Professional Conduct because under the revisions to the Rules (as part of the Ethics 20/20 project), attorneys are now required to use technology competently and to assess the risks of any particular technology and the sensitivity of the data being handled as it relates to the measures being taken to secure the data. An article by Nelson and Simek covers how to securely delete data from mobile devices. One of the preferred ways to ensure the security and confidentiality of e-mail is to use proper encryption methods. A recent article by Ries and Simek discusses how encryption works and provides suggestions for securing laptops and portable media, smartphones and tablets, wireless networks and e-mail.

Where the line is really beginning to blur between work and home is the growing trend towards employees using their personal devices (smartphone, tablets, laptops) for employment-related activities, which is now referred to as Bring Your Own Device (BYOD). BYOD is not really a new concept, because many organizations have allowed employees to work from home for years, providing them with remote access to whatever software and systems were needed, including e-mail. The new twist is that employees are now connecting through tablets and iPhones, many of which are owned by the employees. Some commentators have suggested that this phenomenon should be referred to as BYOT—Bring Your Own Technology—because employees also are choosing the outside software and apps that they want to download onto their devices, not all of which provide sufficient security features. Whether referred to as BYOD or BYOT, this trend presents a number of risks to lawyers and law firms as well as to the clients that they represent.

---

74 Id. at 4.
Issues related to BYOD are expected to multiply, especially if employers begin to require their employees to pay for their own devices and for the technology to support them. Certainly, this saves the employer from the expense of purchasing the devices as well as the cost of robust, centralized IT support. If the employer provides a stipend to purchase devices or network services, this further complicates the issue of who owns or controls the device, how it is used, and its contents (see below). In fact, recent commentators suggest that in the future, more employers may choose to provide employees with a stipend towards the purchase of these devices and for network services.

Allowing or mandating that employees use personal devices means that business and personal data are now jumbled together and raises the question of who owns the information. Although most commentators urge the development of a BYOD policy, Tighe cautions that "[a] comprehensive BYOD policy does not guarantee that an employer can effectively control corporate data that has been commingled with personal records on devices that the company does not truly control." Believing that "BYOD policies have little practical effect" and may even hamper the discovery process, she suggests that the best policy for the employer may be to prohibit the use of personal devices for work purposes and to inform employees that they will be personally liable if company policies are violated or corporate data stored on a personal device is lost, suppressed or misused.

BYOD raises concerns about privacy rights over personal information, especially for employees in the public sector. Heaton notes that while public-sector employees do not have a right to disclose confidential government information, "an agency has to be extremely careful to segregate private and public information on a device" so that only government data is monitored. Among the solutions offered for employers are to allow employees to review but not store government data on their devices; to draft carefully worded policies that address privacy and First Amendment issues; to segregate data; to use search-access agreements and financial disclaimers about purchasing, upgrading or paying for access services; and to require employees to use passwords on personal devices and provide those passwords to the employer.

As an example of the pervasiveness of these issues, and the myriad ways in which they can be addressed, H.R. 3520, the Exempt Organization Simplification and Taxpayer Protection Act of 2013—primarily intended to streamline and clarify the process for entities to apply

---

78 Id. at 7.
79 Id. at 8.
81 Id.
to operate as tax-exempt social welfare organizations—contains the requirement that “[n]o officer or employee of the Internal Revenue Service may use a personal e-mail account to conduct any official business of the Government.”

Murphy discusses the impact of the increasing use of mobile devices by lawyers and law firm employees. He describes how this blurring of personal and business computing is creating special challenges for law firms and their IT departments, including security as an afterthought, data contamination, mobile malware, phishing attacks that can bypass network defenses, lost devices, and risky file sharing. He advocates using a security file-sharing solution which can shield confidential data from unauthorized access and from malware that may have infected other files on the device.

Beck notes that the data being stored on mobile devices continues to grow because of e-mail messages and attachments, text messages and other instant messaging services, app data, multimedia files and metadata. He notes that proper mobile device management (MDM) begins with information governance, including policies and standards. Essential MDM technical controls covered in his article include asset management, configuration management, encryption and remote secure wipe.

Not only are mobile devices prone to being lost or stolen, but people also continue to fall victim to the tactics of social engineering, which Carlson and Wolf define as manipulating people into disclosing information or performing tasks. Social engineering can present risks to the security of e-mail if people can be inveigled to reveal confidential information, such as user identification and passwords. Statistics indicate that people who use their smartphones for work have inconsistent security habits, including not protecting their phones with passwords, using unsecure Wi-Fi networks, and not disabling Bluetooth discoverable modes.

The fact that the device being used is a personal rather than an employer-provided device may mean that people are less vigilant about potential threats and more casual about observing and using proper security protocols and tools.

---

84 Coleman Murphy, Contain Yourself: Top Five Ways to Protect Mobile Data, PEER TO PEER 16–19 (Mar. 2013).
85 Id. at 17–19.
86 Id. at 19.
88 Id. at 81.
89 Id. at 81–82. See also Paula Skokowski, Stop, Thief: Protecting Legal Documents in a Mobile World, PEER TO PEER 84–88 (Sept. 2012); Charles Magliato, Making BYOD Work for Legal, PEER TO PEER 20–24 (Sept. 2012).
Nelson and Simek report that not only are law firms often the victims of security breaches, but that often lawyers in those law firms are not even aware that there has been a breach. They cite a survey conducted by the ABA’s Legal Technology Resource Center that found that “15 percent of survey respondents had experienced a security breach, and respondents of mid-size firms (10–99 attorneys) were most likely to know about the breach.” The authors relate that “[t]he survey highlighted the increased risks from bring-your-own-device policies which allow attorneys to access firm networks through their smartphones, tablets or other devices. As indicated by Nelson and Simek, the report found that ‘34 percent of respondents reported that their firms allowed them to connect their personal mobile devices to the network without restrictions.”

Carlson and Wolf’s article discusses the importance of training lawyers and their staff members about information security threats which can be helpful for clients as well. In terms of keeping mobile employees and their data safe, Nabavi provides a number of best practices for keeping IT secure, whether it is mobile or stationary and DeSot recommends building a "culture of security." Hilal provides a number of practical suggestions for implementing and managing BYOD that are valuable for both law firms and their clients. He identifies the two basic models of corporate-owned and employee-owned BYOD and variations of each of these models and notes that an organization must understand its needs and provide clarity to its employees in order to ensure that a BYOD program is successful.

Although there may be cost savings to the employer, Hilal suggests that companies also need to consider device costs to employees as well as costs for voice and data, an IT helpdesk, mobile development, and mobile management. Employers also must be vigilant to ensure an enterprise-wide security strategy that takes into account access through multiple platforms and limited control of applications that may include malicious software.

---

92Sharon Nelson & John Simek, 70% of Large Firm Lawyers Don’t Know If Their Firm Has Been Breached, LEGAL BY THE BAY (Mar. 4, 2014), http://blog.sfbar.org/2014/03/04/70-of-large-firm-lawyers-dont-know-if-their-firm-has-been-breached/ (last visited June 18, 2014).
93Id.
94Id.
95Id.
96Reza Nabavi, Keep Mobile Workers and Their Data Safe, PEER TO PEER 26–27 (Sept. 2012).
97Tom DeSot, Build a “Culture of Security,” PEER TO PEER 28 (Sept. 2012).
99Id. at 16–17.
100Id. at 17–18.
101Id. at 18.
Likewise, Brown offers a number of suggestions for developing a BYOD strategy. Among his recommendations are adopting a standardized roster of acceptable devices, avoiding devices that are "jailbroken" (i.e., "modified to remove the controls set by the original manufacture"), establishing control through password or pin code policies, adopting some level of encryption, regulating the apps installed by users (especially apps for personal use), and implementing acceptable use policies, Mobile Device Management (MDM) technologies, and strong security controls on the devices. He also reports that productivity is a key concern, especially among the corporate and law firm customers that are members of his company's strategic advisory board.

Special considerations are needed with respect to electronic discovery, not only for the law firm's employees who are working on a case, but particularly related to the lawyer's responsibilities in overseeing the client so that proper collection and preservation procedures and litigation holds are communicated to the client's constituents and are being followed. One issue that is likely to have significant implications is the ESI (Electronically Stored Information) that is available on personal devices and that was communicated through personal e-mail accounts. For example, in Puerto Rico Telephone Co. v. San Juan Cable LLC, the court determined that the duty to preserve extended to the personal e-mail accounts of a company's former officers, although the court declined a request for sanctions based on an absence of bad faith and failure to show prejudice. Cornwell outlines a number of reasons for the risks of spoliation when using a BYOD strategy. Among the risks he identifies are the movement of data from a company's network to personal devices, especially from smaller companies that do not have a high level of security and controls; angry former or terminated employees who may take company data with them; and overtime related to BYOD, resulting in wage and hour claims, if employees are expected to check and respond to e-mail outside of normal work hours. Among the strategies he suggests to mitigate these risks are allowing "read only" access outside of the company's firewall, the ability to wipe company data from devices remotely, setting up BYOD policies, and establishing a model for handling electronic discovery in the event of litigation.

The issue of BYOD continues to be an important topic. In response to a question about allowing personal mobile devices to be used to access the law firm's network, 50 percent of the firms permit it, but with
restrictions or preapproval, 31 percent permit BYOD without restrictions (down from 34 percent in 2013), and 14 percent do not allow BYOD access at all (up from 12 percent in 2013).103

Nelson and Simek discuss the risks with BYOD in two articles on law firm technology, stating, for example, that "[t]here is no cost to forbidding employees by policy from connecting to the law firm network with personal devices. Who knows what malware may exist on those devices? Large firms may choose to use sophisticated techniques to manage personal devices, but smaller firms are better off simply forbidding them to connect to the network." They continue to advocate against BYOD in their second article:

In all aspects of your tech planning and review, consider security. Want to allow employees to bring their own devices and connect to your network? Bad idea. They may be carrying malware and infect your network. Is BYOD cheaper? NEVER if you have a data breach. We’ve heard folks argue that mobile device management solves the problem. Maybe, but the price of that management has soared in the past several years—far beyond the reach of small law firms. Buying and issuing work devices makes the management of their security far easier—and employees have nothing to say about how you choose to manage them.111

In her article about how to create a unified approach to information security, Fischer also expresses her concerns with the trend toward allowing the use of personal devices.112 Although she recognizes the benefits of BYOD, such as increased productivity, employee satisfaction, and lower costs, she notes that the capabilities of most mobile devices far exceed the current technology to secure them.113 Predicting that the majority of security breaches in the future will be caused by hackers who are able to bypass authentication methods on mobile devices, she advocates the use of application-level encryption and segregating enterprise data from the rest of the device.114

McLellan, Sherer, and Fedeles provide a comprehensive review of the privacy risks and legal issues with BYOD from an international perspective.115 Among the challenges they identify are costs, employee behavior,

---

105 Id.
106 Id. at 48.
107 Laurie Fischer, Dream the Impossible Dream: A Unified Approach to Information Security, PEER TO PEER 44–49 (Fall 2014).
108 Id. at 48.
109 Id.
110 Id.
111 Id.
and device security management versus employee personal data. They also examine existing statutory law in the United States, such as the Electronic Communications Privacy Act, the Stored Communications Act, and the Computer Fraud and Abuse Act as well as electronic discovery issues and guidance from the Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST). Finally, the authors cover BYOD programs in France, Germany, Spain, and the United Kingdom. In their conclusion, they provide a number of helpful questions to consider when implementing or enhancing a BYOD program. There are also particular issues with BYOD programs related to unionized employees.

The issues related to Hillary Clinton's use of personal e-mail and her own server while conducting government business as Secretary of State raises a number of important considerations with respect to electronic discovery. Among the questions posed for lawyers to contemplate are: who is in charge of pulling data from the client's or the opposing party's electronic sources; where is the data located; how secure is data on servers, phones, computers, and laptops; where are the servers located; can data be deleted; and does the client have a data retention and destruction policy.

The ABA 2015 Legal Technology Survey Report highlights the increasing number of lawyers using iPhones and iPads. As indicated in the survey, "[f]or those nine out of every ten attorneys who are using smartphones, 75.7% reported in 2015 that they were using a personally owned smartphone, and 26.4% used a smartphone permanently assigned by their law firm." The author notes that those numbers have not changed much since 2014. Per the survey, almost all lawyers are using their smartphones to make phone calls and handle e-mail, in addition to calendars, contacts, Internet access and text messaging, with less popular uses being GPS/maps, taking photographs, and using mobiles-specific research apps. The author observes that although the survey shows that lawyers are continuing to think more about security, only 92% of those who use security measures are using a password to lock their smartphones.
Likewise, lawyers are using their iPads and other tablets for similar activities, including Internet access, e-mail, and calendars. Another article based on the 2015 Survey highlights the increasing lawyer mobility because of mobile technology, including 20% of lawyers working from home and a corresponding decrease in the number of lawyers who work in traditional office space that is leased or owned exclusively by their law firms. As indicated in the article,

> With that mobility comes an inevitable increase in the use of mobile devices, and respondents to the survey were asked if they have a policy governing the use of laptops, tablets and smartphones outside of the primary workplace. While 85% of respondents from firms of 500 or more lawyers reported that their firm has a mobile phone policy, the overall figure was 39%, with the figure dropping in accordance with the number of practitioners.

As these statistics suggest, the trend continues to be towards a liberal view of BYOD in law firms in spite of the security risks.

Fortunately, a number of excellent articles have been published to help lawyers minimize security risks in an increasingly BYOD work environment. For example, after identifying some of the dangers posed by BYOD, Leckie and Prosser discuss the policies that should be in place. Among their recommendations are doing a risk analysis to see what information devices are accessing and what should be sanctioned by the law firm, including language in the BYOD policy that requires immediate reporting of lost or stolen devices, incorporating BYOD into the firm's Acceptable Use Policy, ensuring that any access to data requires a strong passcode, and that accessing the device will require authentication. The authors provide a suggested checklist of BYOD policies and procedures. Likewise, because of the increased blurring between work versus home because of BYOD, Pall describes four steps to a better BYOD policy that are useful for any kind of entity, with these steps covering access, planning, implementation and iteration, which includes auditing, considering new technologies, and reviewing and updating the policies as needed. Additional guidance on BYOD is provided by Waterfill that can be helpful for law firms as well as their clients.

---

126 Id.
128 Id.
130 Id. at 11–12.
131 Id. at 12.
132 Vikas Pall, From Blurred to Secured: Four Steps to a Better BYOD Policy, Peer to Peer 18–20 (Fall 2015).
Organizations should create a BYOD plan based on their company’s needs and goals. This policy should be clear and precise. Employers should then have their employees sign off on the policies. Lastly, organizations should continue to monitor court decisions with regard to BYOD employee privacy expectations in the workplace and continuously update BYOD policies with the ever-changing state of technology and communication devices.134

Nelson and Simek are especially blunt about the risks that employees pose in the workplace, especially in a BYOD environment, including the danger of compromising an electronic discovery process.135

Employees are by nature rogues. In every study that’s been made, they will ignore policies (assuming they exist) in order to do what they want to do. This often means they bring their own devices (BYOD) which may be infected when they connected to your network. They may also bring their own network (BYON) or bring their own cloud (BYOC). Certainly your policies should disallow these practices (in our judgment) or at least manage the risks by controlling what it is done by a combination of polices and technology.

Oh, and they steal your data or leave it on flash drives, their home devices, etc. This means you have “dark data”—data you don’t know about and over which you have no control. This means you may miss data required in discovery because you don’t know it exists. Your data may not be protected in compliance with federal or state laws and regulations. And you have no way to manage the data because you don’t know it is there. Once again, a combination of policies and technology should be in place to prevent these issues.136

2. Document Retention Policies

A recent article by Nelson and Simek outlines a number of polices and plans that firms should have in place to deal with the vast amount of electronic information that is being generated by employees using a variety of devices and social media sites.137 These same suggestions seem appropriate for any corporation or organization and the authors also note the importance of annual training as a way to reinforce these policies and plans. Among the policies that the authors advocate for law firms that encompass e-mail and other popular forms of electronic communication and that pose risks to client confidentiality are an electronic communications and Internet use policy, a social media policy, a document retention policy, a secure password policy, an equipment disposal policy, and policies for mobile security.

134 Id. at 26.
136 Id. at 1–2.
The technology plans that Nelson and Simek consider essential for law firms are an incident response plan, a disaster recovery plan, and a litigation hold plan. The authors note that “[t]hese policies and plans are an integral part of risk management and ensuring business continuity, two things near and dear to the heart of all lawyers.”

Drawing on the work of Nelson and Simek, Kerschberg also discusses why companies should have robust social media policies and a secure and reliable method for archiving information generated through social media, especially since it is discoverable in litigation.139

One of the most important ways to help clients is to make sure that they have a comprehensive document retention policy that is being used on a regular and consistent basis. On the flip side, one of the worst things that a client can do is to suddenly begin using a document retention policy, especially when it appears that certain electronically stored information that might be relevant to impending litigation has been selectively targeted for disposal. Such was the behavior exhibited by Rambus, resulting in a finding of bad faith and with an appropriate sanction being to declare that the patents-in-suit were unenforceable against Micron.140 Among the four main categories of facts that supported the finding of bad faith were:

1) facts that show that the plaintiff’s document retention policy was adopted only as a weapon for litigation; 2) facts that show that the plaintiff’s document retention policy was selectively executed, with suspicious documents discarded; 3) facts that show that the plaintiff knew of the impropriety of the document retention policy, minimizing discussion thereof via e-mail, and; 4) plaintiff’s litigation misconduct, and misrepresentations in depositions about the number of “shred days.”

In a similar case involving Rambus and SK Hynix, the court found that Rambus had committed spoliation, but adjusted the royalty rate as its sanction.141 In a more recent case, the court awarded a monetary sanction of $250,000,000, which would be applied as a credit against Rambus’s

---

138 Id. at 5.
more than $300 million judgment against SK Hynix, Inc. The ongoing litigation between Rambus and its competitors not only provides considerable insight into various steps in the electronic discovery process and the substantial penalties that can be assessed for spoliation, but also points to the importance of having and properly using document retention policies.

Scentsy, Inc. v. B.R. Chase, LLC addresses both inadequate document retention policies and concerns with the litigation hold process, including using oral rather than written litigation holds and inconsistency in handling and storing e-mail and other ESI. Another recent case involving improper handling of e-mail during an electronic discovery process is Carrillo v. Schneider Logistics, Inc. In this case, the court ordered monetary sanctions and that an outside vendor be hired after determining that the defendant had failed to comply with its discovery obligations. Among the deficiencies identified were: 1) failing to conduct a “reasonably diligent search,” 2) improperly withholding responsive documents, and 3) failing to take “adequate steps to preserve documents.” With the trend towards a Bring Your Own Device (BYOD) policy, companies will need to be even more thoughtful about how e-mail is handled in all phases of an electronic discovery process as well as policies, procedures and tools for preservation, storage, archiving and destruction of e-mail and other ESI that will now reside on devices that are not directly purchased by or under the control of the employer.

Several recent electronic discovery cases emphasize not only the importance of working with clients to develop and implement an effective records retention policy, but also of ensuring that clients cease their established processes for destroying or otherwise making inaccessible

---

146 Id. at *3.
147 Id. at *5.

In Herrmann v. Rain Link, Inc.,\footnote{No. 10-0541, 2013 WL 6159177 (S.D. Cal. Nov. 25, 2013).} however, the court declined to sanction the defendants for failing to suspend their routine document retention procedures, even though it resulted in the destruction of documents and ESI, because the plaintiff had not demonstrated that it was prejudiced, or that the defendants acted in bad faith. The court characterized the defendants' failure to suspend their routine practices as negligent as opposed to being done with intent to deprive the plaintiff of evidence.\footnote{Id. at 497 (footnotes omitted).}

In a third case, Sekisui American Corp. v. Hart,\footnote{Id. at *3.} Judge Shira A. Scheindlin (author of the Zubulake opinions) reversed an earlier order from the Magistrate Judge wherein he declined to impose spoliation sanctions for the plaintiffs' deletion of ESI that belonged to two important custodians in the case. In her Opinion and Order, she states:

A decade ago, I issued a series of opinions regarding the scope of a litigant's duty to preserve electronic documents and the consequences of a failure to preserve such documents falling within the scope of that duty. At its simplest, that duty requires a party anticipating litigation to refrain from deleting electronically stored information ("ESI") that may be relevant to that litigation. Such obligation should, at this point, be quite clear—especially to the party planning to sue. Here, I consider the appropriate penalty for a party that—with full knowledge of the likelihood of litigation—intentionally and permanently destroyed the e-mail files of several key players in this action.\footnote{945 F. Supp. 2d 494 (S.D.N.Y. 2013).}

Among the deficiencies in Sekisui's e-discovery process were many months of delay in imposing a litigation hold and in advising the vendor in charge of managing its information technology systems of the hold as well as orders to permanently delete ESI in the form of e-mails and e-mail folders of two key figures in the company, including one of the
defendants. In addition to granting the defendants’ request for an adverse inference jury instruction, Judge Scheindlin awarded them reasonable costs, including attorneys’ fees, which were associated with bringing their motion.

Even the Internal Revenue Service is facing the consequences from questionable document retention policies and the failure to stop destruction processes when it seemed likely that there would be an investigation of the handing of applications for tax-exempt status by the director of the IRS’s Exempt Organization Unit. A recent article reported that among the problems were “seven hard drive crashes, the lack of a centralized archive, a practice of erasing and reusing backup tapes every six months, and an IRS policy of allowing employees to decide for themselves which e-mails constitute an official agency record.” The article notes that the IRS system had an e-mail limit of 150 megabytes per mailbox (about 1,800 e-mails), that some employees used a “print and save” approach, and that many times e-mail attachments were not saved at all.

In his summary of the security sections of the ABA 2014 Legal Technology Survey Report, Ries reviews the information security risks that law firms have faced as well as measures that law firms have taken to protect themselves, including security programs and policies, authentication and access control, and encryption and backup. Among the positive findings are that 56 percent of respondents reported that their law firms have a document or records management and retention policy, 46 percent reported that their firms have a computer acceptable-use policy, 47 percent have a policy for Internet use, 42 percent have a policy for e-mail retention, and 34 percent have a policy on employee privacy, with all of these percentages up slightly from 2013.

A search of the K&L Gates and Kroll Ontrack databases (K&L Gates, E-Discovery Case Database, http://www.ediscoverylaw.com/e-discovery-case-database/ and Kroll Ontrack, ediscovery.com, http://www.ediscovery.com/pulse/case-law/) for cases related to electronic discovery resulted in just a few cases that were specific to issues with e-mail. Several cases discuss the interrelationship of document retention policies and the duty to preserve, especially when parties either fail to impose effective litigation holds or to stop routine destruction policies such as overwritten.

---

150 Id. at 499-501.
151 Id. at 509-10.
153 Id.
155 Id. at 3.
In an especially interesting case, *United Corp. v. Tutu Park Ltd.*, the court addressed the issue of the length of time a corporation may be expected to retain records, the methods it uses to store its records, and the difficulties when a large corporation's information technology changes over time as well as the impact of mergers and reorganizations.

Kmart has identified a number of reasonable explanations for the scope of its production under the subpoena. Most notably, Kmart claims that its record retention policy does not provide for the retention of records before the year 2005. The year 2005 was over nine years ago, and as a practical matter, a corporation may be justified if it chooses not to retain records that are over nine years old. Kmart has also alleged that internal changes in sales reporting prohibited it from estimating pre-tax income for certain items. Moreover, Kmart emerged from Chapter 11 bankruptcy protection in May of 2003, and merged with Sears, Roebuck and Co. in 2005. It is reasonable to believe that the disruption caused by bankruptcy and the integration of two companies impacted Kmart's ability to access records. Finally, Kmart has explained that certain data cannot be recreated due to software and database conversions, among other changes in recordkeeping. Having considered these reasons, the Court believes that Kmart has made a diligent attempt to comply in a reasonable manner with the Court's March 22, 2013 Order.

Several electronic discovery cases in 2015-2016 located through searching the K&L Gates and Kroll Ontrack databases deal with disputes over the adequacy of a party's document retention policies, including policies and procedures that cover e-mail accounts and the disposition of e-mail messages, and failure to preserve this data once litigation is reasonably anticipated. Among these cases are *Moore v. Lowe's Home Centers, LLC*, *Official Committee of Unsecured Creditors of Exeter Holdings Ltd. v. Haltman*, *Stinson v. City of New York*, *Grove City Veterinary Services, LLC v. Charter Practices International, LLC*, *Kan-Di-Ki, LLC v. Sue*, and *Burd v. Ford Motor Company*.

**B. Discovery**

[Add the following text at the end of the section.]

A search of the K&L Gates Electronic Discovery Case Database and the Kroll Ontrack database for cases since June 2013 indicates that discovery of e-mail continues to be a serious matter for clients and their

---

164 Id. at *4.
lawyers, resulting in claims of spoliation and lack of cooperation, motions for sanctions, motions to compel, and disputes about the adequacy of search, identification or collection methods and over the format of production, privilege and metadata. These cases concern employment discrimination and/or hostile work environment, breach of contract and trade secret misappropriation, product liability, copyright and trademark infringement and unfair competition, a variety of federal and state laws, patent infringement, and breach of contract and conversion. Additional cases concern insurance disputes, lack of specificity in discovery requests, and whether a deposition request about search methodology was unduly burdensome. Interestingly, the discoverability of e-mail messages and their use as documentary evidence are the subjects of two related pieces of legislation introduced in Congress over the past year. First, S. 1013, the Patent Abuse Reduction Act of 2013, provides a long list of criteria that qualify as "core documentary evidence." However, this definition excludes "any computer code or electronic communication, such as e-mail, text messages, instant messaging, and other forms of electronic communication, unless the court finds good cause." In what appears to be a more expansive version for purposes of discovery, H.R. 3309, the Innovation Act, [p]rovides for discovery of electronic communications (including e-mails, text messages, or instant messages) only if the parties determine that it is appropriate under procedures that address whether such discovery is to occur after

---


183 Id.

the parties have exchanged initial disclosures and core documentary evidence.\textsuperscript{188}

A bill related to patent infringement has been proposed as part of the 114th session of Congress. Similar to S. 1013 and H.R. 3309, H.R. 9, Innovation Act, also covers the discoverability of e-mail and "[r]equires the Judicial Conference to consider proposals to delay determinations as to whether discovery of e-mails, text messages, or instant messages is appropriate until after the parties have exchanged initial disclosures and core documentary evidence."\textsuperscript{189}

Several cases from mid-2014 to mid-2015 discuss the continued difficulties with discovery of e-mail, including the sufficiency of production, archival systems, and working with custodians. These cases concern employment termination (\textit{Gladue v. Saint Francis Medical Center}\textsuperscript{187}), breach of contract and various business torts (\textit{Novick v. AXA Network, LLC}\textsuperscript{188}), securities fraud (\textit{Freedman v. Weatherford International Ltd.}\textsuperscript{189}) and patent infringement (\textit{Finjan, Inc. v. Blue Coat Systems, Inc.}\textsuperscript{190}). In \textit{Finjan}, the court provided commentary on the question of custodial e-mails and archiving systems:

Where Blue Coat has been less than fair is with respect to archival e-mail for its eight custodians. Blue Coat may largely be in the right that it should not have to dig through legacy systems when Finjan is unable to the same for its custodians. But one party's discovery shortcomings are rarely enough to justify another's. And here, at least with respect to documents mentioning Finjan—the one specific category of documents Finjan could identify that it needed from archived e-mail—Finjan's request is reasonable.\textsuperscript{191}

For additional assistance with a broad range of issues related to electronic discovery, the International Legal Technology Association (ILTA) released a White Paper in May 2015 that provides considerable guidance, including practical advice on e-discovery in Asia and the European Union and measuring e-discovery metrics.\textsuperscript{192}
One of the most important developments since the publication of the 2015 Supplement is the amendments to the Federal Rules of Civil Procedure (FRCP), which became effective on December 1, 2015. Amendments were made to Rules 1, 4, 16, 26, 34, 37, 55, and 84. However, the most significant changes concern proportionality and a uniform standard for when sanctions are available for spoliation of evidence. However, the amended Rule 1 of FRCP is interesting in that it requires everyone, not just lawyers, to cooperate in the litigation process:


Other revisions should encourage cooperation between lawyers, including Rules 4(m), 16, 26(d)(2) and 34(b)(2)(a), which reduce the time periods for various activities to happen. In addition, Rule 34 has been revised in ways that encourage cooperation and reduce the opportunity for dilatory tactics:

Rule 34: Boilerplate objections are prohibited and objections must "state with specificity the grounds for objecting" and "whether any responsive materials are being withheld." The Committee notes: "An objection may state that a request is overbroad, but ... should state the scope that is not over­broad." An objection that "states the limits that have controlled the search for responsive and relevant materials"—which might include the date range or the scope of sources or search terms used—"qualifies as a statement that the materials have been 'withheld.'" Furthermore, this Rule includes a new provision that "[t]he production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response." This new provision appears to limit the parties' ability to engage in unconstrained rolling productions.\footnote{Id. (emphasis in original) (footnote omitted). \footnote{Id. (footnote omitted).}}

In terms of Rule 26(b)(1)'s focus on proportionality, the Advisory Committee on Rules of Civil Procedure noted that "a party may not 'refuse discovery simply by making a boilerplate objection that it is not proportional.'"\footnote{Id. See United States Courts, Redline of Civil Procedure Rules Text and Committee Notes, http://www.uscourts.gov/rules-policies/current-rules-practice-procedure.} As part of the revisions to Rule 37(e) on sanctions, the Committee noted that the "rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection."\footnote{Id. (footnote omitted).}

As reported by Brown, the five things that are most important to know about the amendments are:
1. Proportionality in discovery is now part of the rules.
2. Much-needed improvements are made to Rule 34(b)(2) regarding responses to document requests.
3. Rule 37(e) has been completely rewritten to standardize sanctions for failure to preserve ESI.
4. Document requests can be served 22 days after the complaint and summons are served, before any party has answered.
5. Rule 26 expressly authorizes an option of shifting expenses as part of a protective order.\(^{197}\)

A search of the K&L Gates and Kroll Ontrack databases reveals a number of interesting cases from 2015-2016 that deal with e-mail as potentially relevant ESI. Many of these cases specifically consider spoliation and sanctions and illustrate how courts are applying the recently amended FRCP Rule 37(e). Among these cases are FiTeq Inc. v. Venture Corp.,\(^{198}\) Matthew Enterprise, Inc. v. Chrysler Group, LLC,\(^{199}\) Cat3, LLC v. Black Lineage, Inc.,\(^{200}\) and NuVasive, Inc. v. Madsen Medical, Inc.\(^{201}\)

1. Attorney-Client Privilege

Since July 2011, a number of cases have addressed the issue of privilege for e-mail that was requested as part of the discovery process. These cases suggest that courts are becoming more comfortable within the realm of electronic discovery and the responsibilities of clients and counsel for preservation and production of electronically stored information and less patient when the appropriate steps and safeguards are not in place, especially with respect to privilege.

Another theme of some of the cases is the failure of the party or its counsel to address inadvertent disclosure in a timely manner. For example, in Ceglia v. Zuckerberg,\(^{202}\) the court held that the attorney-client privilege was waived when an e-mail was inadvertently produced by an information technology expert. The court found that the plaintiff and counsel did not take reasonable steps to prevent disclosure of the e-mail nor did they act promptly to address this lapse once it was discovered,

---


waiting nearly two months after the material was disseminated to request that it be returned or destroyed. In *Williams v. District of Columbia*, the court denied the defendant’s motion to exclude an inadvertently produced e-mail because the defendant failed to satisfy the burden of establishing that reasonable steps were taken to prevent disclosure and did not promptly take steps to rectify the error.

Courts are also finding that privilege has been waived when parties do not take reasonable steps to preserve confidentiality. For example, in *Pacific Coast Steel, Inc. v. Leany*, the plaintiff had purchased the assets of several companies in which the defendant had an ownership interest and became a high-level employee. He was later terminated and his computer was seized. PCS claimed that Leany had been previously informed that the computer was the property of PCS, that all documents would be merged into a single PCS server, and that PCS reserved the right to monitor the use of the computer system. Nevertheless, he made no effort to remove any confidential or privileged information during an e-mail migration or upon being terminated. In particular, the court noted that Leany could not have had any expectation of privacy in the e-mails. This case points to the dangers of waiving privilege for otherwise confidential information when using an employer-provided computer to communicate with accountants, spouses, or attorneys if the employer has reserved the right to monitor usage and has an Acceptable Use Policy for e-mail and other electronic communications systems.

The ABA’s Formal Opinion 11-459, August 4, 2011, Duty to Protect the Confidentiality of E-Mail Communications with One’s Client, addresses the danger of third-party access to client communications. The opinion discusses two common examples of how the attorney-client privilege can be put at risk: employer-provided e-mail, where the employer has indicated that it has the right to monitor e-mails (and the party

---


communications with counsel via the e-mail account, and where a family member can access an e-mail account (and the party is involved in a matrimonial dispute). The opinion, which echoes a number of recent cases, suggests the need to educate the client about this risk and obtain consent to how he/she would like to be communicated with.

An article by Stagg and Anderson\(^\text{209}\) highlights this issue in the context of attorney-client privilege in Tennessee, first reviewing cases from New York, New Jersey, and California as well as the ABA's Formal Opinion 11-459, and then describing the decision in a recent Tennessee trial court case, *Forrest v. Lewis*.\(^\text{210}\) The court in *Forrest v. Lewis* held that the plaintiff had "no reasonable expectation that his communications to his attorney using company e-mail were private" and that the e-mails conveyed through a company e-mail system did not fall within the attorney-client privilege.\(^\text{211}\)

A quick search of the K&L Gates database\(^\text{212}\) of electronic discovery cases related to e-mail in 2012 illuminates a number of common themes, including: spoliation and sanctions;\(^\text{213}\) privilege and waiver;\(^\text{214}\) forensic examination of e-mail accounts;\(^\text{215}\) cost shifting for processing e-mail accounts;\(^\text{216}\) and motions for a protective order over e-mail records, e-mails, text messages, and other related information from Yahoo! and Verizon.\(^\text{217}\)

There have been predictions that use of e-mail would by now be passé and would be bypassed in favor of texting, tweeting, and social media, at least within popular culture. However, from these cases it is clear that e-mail continues to be a major means of communication within the business community, so it still should be a matter of concern in the context of electronic discovery, as well as for overall information management.

Care needs to be taken throughout the electronic discovery process when handling e-mail as electronically stored information (ESI). Given the sheer volume of e-mail that might be generated by even a small company or individual client, inadvertent production may pose a special risk

---


because courts may deem that this results in a waiver of the attorney-client privilege. For example, in *Inhalation Plastics, Inc. v. Medex Cardio-Pulmonary, Inc.* the court held that privilege had been waived for 347 pages of e-mail which had been inadvertently produced, out of a batch of 7,500 pages that had been produced as hard copy without marking anything as confidential, finding that the defendant had failed to establish that it had taken reasonable precautions to prevent the disclosure and then failed to take adequate measures to rectify or mitigate the damage from the disclosure.

In its analysis of whether privilege had been waived, the court discussed the three-factor analysis from Federal Rule of Evidence 502(b) and a five-factor test that is generally used to determine whether a party’s documents should be returned. The court was also persuaded by the sheer number of documents that were inadvertently disclosed (4.6 percent), the lack of a privilege log at the time of the disclosure, the relevance of the documents to the dispute, and whether several layers of attorneys had participated in the review.

One facet of the attorney-client privilege that is receiving attention in 2013 is how the attorney-client privilege is applied to in-house counsel. In *United States ex rel. Baklid-Kunz v. Halifax Hospital Medical Center,* a federal magistrate judge took a rather narrow approach in applying a rule that communications between a client and a corporate attorney about business matters or business advice are not privileged unless they “solicit or predominantly deliver legal advice.” In so doing, he held that hundreds of documents and communications, including audit and review materials and e-mails that were sent between the finance and legal department involving Halifax Hospital’s inside counsel, were not privileged and granted the privilege narrowly only to documents that sought or reflected legal advice. First, the judge provided an analysis of assertions of privilege over e-mail communications in the corporate setting and adopted the rule that each e-mail in an e-mail string must be listed separately on a privilege log. Then the judge addressed each of the seven categories where a determination of privilege was requested. The opinion includes detailed charts of his rulings with respect to specific documents, such as Category 3 related to documents or communications that relate to internal audits and reviews and Category 6 covering e-mail strings. Interestingly, a significant majority of the rulings listed

---

220 Id.
221 Id.
223 Id. at *11–15.
224 Id. at *17–37.
225 Id. at *25–27.
226 Id. at *21–24.
on the charts indicate that the material was deemed not privileged, often because either no legal advice was sought or received or because of no attorney “to” or “from.”

In a short article analyzing this case, Kim notes that “[t]he Halifax decision reflects the growing scrutiny that courts are applying to businesses asserting attorney-client privilege over documents involving in-house counsel.” The author notes that although this is not a new issue, the increased scrutiny can be attributed to the expanded role of in-house counsel in providing business advice as well as legal advice, due to their experience in the commercial setting, and that courts have been inconsistent in how they have evaluated attorney-client privilege claims. She concludes that:

Courts have recognized certain practices—such as addressing the in-house attorney in the “to” line as opposed to the “cc” line in e-mails, structuring important compliance audits to be conducted under the direction of in-house attorneys, and limiting the number of people included in a communication—to trigger attorney-client privilege. To gain more certainty in retaining confidentiality in documents and communications, in-house counsel for healthcare institutions will need to be more explicit and deliberate in applying these recognized practices in the future to ensure that institutional documents and communications remain protected under the attorney-client privilege.

An article by Judish and Assay provides additional insight into the case and also includes a list of best practices for communications with general counsel, with the observation that this case and others discussed in their article serve as “important cautions to organizations that assume the inclusion of general counsel in discussions automatically confers privilege on such discussions.”

There is often an assumption, especially among clients, that including in-house lawyers as recipients of a communication or copying them in e-mail circulation will mean that the document is protected by privilege. Desoer, Lambert, and Wites provide a thoughtful analysis of this situation, emphasizing that the determination of whether the privilege has been asserted properly may require more detailed information.

An article by DeLisi addresses the issue of protecting attorney-client privilege in an era where many, if not most, employers have Acceptable


228 Id.

229 Id. at 188.


231 Michele Desoer, Lawrence B. Lambert & Marc A. Wites, Does Copying an In-House Lawyer on Corporate Correspondence Render It Privileged?, THE FEDERAL LAWYER (Mar. 2014), at 60–63, 70.
Use policies governing e-mail, Internet, social media and other technology and which include the right to monitor employee communications through this technology.\textsuperscript{232} He advocates a three-pronged approach:

First, lawyers should seek to prevent nonconfidential communications from occurring by discussing the degree of confidentiality of their client's workplace systems and how the lack of confidentiality might undermine attorney-client privilege. Second, if employers monitor attorney-client communications, employers should attempt to avoid reading them so that, even though they were technically nonconfidential, courts may still consider them privileged. Third, courts should allow the privilege to attach when the employee believed that her communications with her attorney were confidential.\textsuperscript{233}

A recent article by Favro provides an excellent discussion of the impact of new technologies on the attorney-client privilege for in-house counsel and includes some suggested practices to enhance the defensibility of in-house counsel's privilege claims.\textsuperscript{234}

Recent ethics opinions address the risks associated with communicating by e-mail. One of the issues is whether lawyers should respond to e-mails with the "Reply All" option.\textsuperscript{235} Another issue focuses on confidential written communications between the opposing party and his or her counsel are sent by a nonparty, but where the receiving lawyer believes that the circumstances may suggest that the crime-fraud exception applies to the attorney-client privilege.\textsuperscript{236}

An article on e-mail etiquette also covers important issues with respect to maintaining the confidentiality of client information.\textsuperscript{237} The author's recommendations for e-mail correspondence that intersect with client confidentiality and attorney-client privilege include whether e-mail should be sent at all because of the potential for it being discoverable; confining an e-mail message to a single or related group or subjects; clarifying the status of drafts and revisions sent via e-mail; writing with the presumption that the client will forward the e-mail even if warned not to; security concerns with wireless devices, unsecure networks, hacking and

\textsuperscript{232}Alex DeLisi, Note: Employer Monitoring of Employee Email: Attorney-Client Privilege Should Attach to Communications That the Client Believed Were Confidential, 81 FORDHAM L. REV. 3521 (May 2013).

\textsuperscript{233}Id. at 3524.


\textsuperscript{237}George W. Kuney, Legal Form, Style, and Etiquette for Email, 15 TRANSACTIONS 59 (Fall 2013).
An interesting discussion of the attorney-client privilege and how claims of this privilege can be abused is presented in Brown v. Tellermate Holdings, a case involving employment discrimination. In this case, not only did the defendant decide to classify approximately 50,000 pages of documents as privileged, but the defendant also allegedly marked 99 percent of documents as “Attorneys’ Eyes Only.” In terms of the claims of privilege, the court stated that:

Finally, if Tellermate intended to withhold these documents on privilege grounds, it had a duty to raise that claim on a timely basis. It failed to so here both with respect to the Rule 408 privilege claim and, more egregiously, with respect to the attorney-client privilege claim. See, e.g., Pulsecard, Inc. v. Discover Card Servs., Inc., 168 F.R.D. 295, 302 (D. Kan. 1996) (finding that objections raised by defendants in response to plaintiff’s motion to compel discovery were untimely, where defendants failed to raise such objections in response to plaintiff’s initial requests for discovery). The actions of Tellermate and its counsel with respect to the Mecka documents again impaired the Browns’ ability to pursue this discovery in a timely and cost-efficient manner.

The court also expressed its displeasure with the extreme over-use of the “Attorneys’ Eyes Only” designation on nearly all of the defendant’s documents.

The issue of the “Attorneys’ Eyes Only” designation represents the final chapter in this saga. The protective order permitted this designation to be made only when counsel held a good faith belief that such material constituted or revealed a trade secret or other confidential research, development, or proprietary business information, and that such material was entitled to a higher level of protection than otherwise provided in the protective order. As the producing party, Tellermate had the burden of demonstrating entitlement to the designation. See Procter & Gamble Co. v. Nabisco Brands, Inc., 111 F.R.D. 326, 328 (D. Del. 1986). Although Tellermate and its counsel claim that the designation was warranted because the Browns are Tellermate’s competitors, this unsupported argument does not satisfy their burden of demonstrating that the documents at issue were entitled to the higher level of protection. See THK Am., Inc. v. NSK Co., Ltd., 157 F.R.D. 637, 646 (N.D. Ill. 1993). The alleged burden imposed by a high volume production does not provide the producing party or its counsel free reign to choose a given designation and ignore the Court’s order pertaining to that designation. See, e.g., Minter v. Wells Fargo Bank, N.A., 2010 U.S. Dist. LEXIS 136006, 2010 WL 5418910, *2 (D. Md. Dec. 23, 2010) (finding that “defendants act at their own peril in continued unexamined and quite apparent over-designation” of documents).
There continue to be concerns about maintaining the attorney-client privilege not only because of the surveillance activities of the NSA but also as e-mail and other forms of communications cross international borders.\(^{243}\) As stated by Macpherson and Stevenson, "[i]ncreased globalization of legal advice brings greater risks to law firms and clients alike, especially when it comes to maintaining privilege of communications."\(^{244}\) They observe that "[p]rivilege protections for in-house and outside counsel communication vary widely across the globe, and, as a result, privileged communications in one jurisdiction may be discoverable in another."\(^{245}\) They state that

\[
\text{[i]n light of these and other developments, it is important for multinational companies and attorneys serving them to understand and be able to predict the scope of privilege and confidentiality that applies to communications between their employees and attorneys. The problem is that a company is at risk for being involved in a litigation matter or investigation in any country in which it does business, and the laws of the forum country tend to be used to evaluate claims of privilege regardless of where the legal advice was rendered.}^{246}\]

The authors include a non-exhaustive table that provides a simplified summary of the current state of attorney-client privilege in a number of jurisdictions as well as commentary about specific countries. The table shows countries that do and do not recognize attorney-client privilege in some form, whether by statute or common law, and then to whom the confidentiality or privilege laws apply (in-house counsel, outside counsel, foreign attorneys).\(^{247}\)

Another interesting issue with e-mail communications between the attorney and the client is "online legal marketplaces," third-party Web sites that specialize in the delivery of legal services and that act as intermediaries between lawyers and those who want to obtain legal services.\(^{248}\) One of the questions posed by the authors is whether the third-party Web site facilitates preserving the confidentiality of information, which they examine from the point of view of both the potential client and the attorney. In terms of questions for the client:

\[
\text{[d]oes the site explain to the potential client before the client transmits the information that information transmitted over the Internet may not be entitled to a client-lawyer privilege? Depending on how data is handled by the site, there is a risk that information the client considers confidential may not, in fact, be kept confidential or entitled to privilege.}^{249}\]


\(^{244}\) Nina Macpherson & Theodore Stevenson III, Attorney-Client Privilege in an Interconnected World, 29 ANTITRUST ABA 28 (Spr. 2015).

\(^{245}\) Id. at 28.

\(^{246}\) Id.

\(^{247}\) Id. at 29–31.


\(^{249}\) Id. (emphasis in original).
From the attorney's point of view:

Lawyers must exercise reasonable care to prevent those whose services they are using from revealing client confidences or secrets. Presumably, this includes an online legal marketplace. Request from the site an account of the encryption and other protections it has in place and examine the information flow to assure that the site is exercising reasonable care to safeguard information.250

Per the summary from K&L Gates electronic discovery case database regarding inadvertent production of ESI in product liability cases and privilege,

In four cases involving the same inadvertently produced document, which was included on a privilege log by description and bates number, the court found in a detailed analysis of case law that the document was privileged and that the defendant did not waive the privilege as the result of a vendor’s processing error that caused the privilege designation to be stripped from the document. The court analyzed five factors under FRE 502(b) to determine if the defendant took reasonable steps to prevent disclosure and concluded that the defendant was entitled to clawback of the document.251

2. Possession/Custody/Control

[Add the following text at the end of the section.]

In 2012, the American Bar Association Commission on Ethics 20/20 circulated drafts of amendments to rules and comments that reflect the modern realities of the practice of law, particularly issues that relate to the increasing use of technology to manage law firms and to deliver legal services more efficiently and economically. A number of materials were filed with the ABA House of Delegates on May 7, 2012, for consideration at the ABA’s annual meeting in Chicago in August 2012. Among the filings were resolutions and reports on technology and confidentiality, technology and client development, and outsourcing that could encompass e-mail and other electronic means of communication within law firms, with clients, and with third parties and which may depend on the services of third-party and Cloud computing vendors.252

On August 6, 2012, the ABA House of Delegates voted to approve changes to the ABA Model Rules of Professional Conduct “to provide guidance regarding lawyers’ use of technology and confidentiality as follows....”253 Resolution 105A makes several changes regarding e-mail:

250 Id.
Model Rule 1.0 Terminology: In Section (n), “e-mail” is amended to “electronic communications”;

Model Rule 1.0, Comment [9] (Screened): Screening includes avoiding contact with or denying access to “information, including information in electronic form,” which relates to the matter;

Model Rule 1.1 Competence, Comment [6] (Maintaining Competence): Rule 1.1’s admonition that a lawyer should maintain “ requisite knowledge and skill” by keeping “ abreast of changes in the law and its practice” now includes in such practice “the benefits and risks associated with relevant technology”;

Model Rule 1.6 Confidentiality of Information: Section (c) is added whereby “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.” The expectations are illuminated in the amendments to Comment [16] (Acting Competently to Preserve Confidentiality);

Model Rule 4.4 Respect for Rights of Third Persons: Section (b) now adds “electronically stored information” as material whose inadvertent receipt requires a prompt notification to the sender;

Model Rule 4.4, Comment [2] describes how a document or electronically stored information is inadvertently sent when it is accidentally transmitted, for example, as when an e-mail or letter is misaddressed.254

Lawyers are urged to review these proposed revisions to the Rules as well as to read the report that accompanies these revisions to fully understand what their ethical responsibilities may be, given that many, if not most, states are likely to adopt the same or similar revisions. In addition, lawyers will want to review the revisions in Resolution 105B dealing with technology and client development to see the extent to which it impacts advertising and solicitation using e-mail or other electronic means as well as the multijurisdictional practice of law.255

The impact of the Stored Communications Act and whether this protects electronically stored information has been a continuing theme in the development of electronic discovery processes. In Optiver Australia Pty. Ltd. & Anor v. Tibra Trading Pty. Ltd. & Ors,256 the court addressed what qualifies as “content” so that disclosure by service providers would be prohibited under the SCA.257 The plaintiff had issued a subpoena to Google

254Id.


requesting e-mails, e-mail attachments and Google Talk messages sent by the employee's defendants, including metadata related to messages containing certain search terms and the subject lines of those messages and others which met criteria, such as time frame or recipients. Most of this information was deemed to be "content" protected under the SLA. As stated by the court,

[the SCA prohibits any knowing disclosure by service providers of the content of electronic communications, no matter how insignificant. The search proposed by Optiver would necessarily reveal that the e-mails identified contain the terms "PGP" or "Optiver," which are words contained in the body of the communications. These terms constitute content, or information concerning the "substance, purport, or meaning" of the communications. However trivial, this is exactly the sort of information the SCA sought to protect.]

The court did allow the plaintiff to receive non-content metadata.

On the other hand, in Garcia v. City of Laredo, the Fifth Circuit affirmed the district court's interpretation of the Stored Communications Act, concluding that it does not apply to data stored on a personal cell phone because a cell phone is not an SCA-protected "facility."

The interpretation of the Stored Communications Act and whether it protects electronically stored information (ESI) continues to evolve in electronic discovery case law. For example, in Cheng v. Romo, the court was asked to determine whether Web-based e-mails are "electronic storage" as defined by the Stored Communications Act. After discussing case law and commentary identifying imperfections in the Act's statutory language and reviewing the definition of "electronic storage" found at 18 U.S.C. §2510(17)(B), the court found that the SCA did apply because the Web-based server continued to store copies of the e-mails that had been transmitted to both the plaintiff's and the defendant's Web browsers.

Information Governance (IG) is becoming an increasingly important topic among corporate leaders as well as security experts. According to an article by Hulse and Quick, information governance is predicted to be one of the growth areas in legal technology hiring.

An excellent resource on information governance for attorneys is provided in an April 2015 White Paper from the International Legal

---

258 Optiver Australia, 2013 WL 2566771, at *1.
259 Id. at *2 (emphasis added).
260 Id. at *3.
261 702 F.3d 788 (5th Cir. 2012).
262 See id. at 790 ("We conclude that the Stored Communications Act... does not apply to data stored in a personal cell phone.").
265 Kristen Uhl Hulse & Diane Quick, 2015 Hiring Predictions: E-Discovery and More, PEER TO PEER (Spr. 2015), at 44-45.
Technology Association (ILTA). This publication includes articles on legal ethics and information governance, outside counsel's role in information governance, management and disposal of client information, and the evolution of records and information management.

A particularly interesting case is presented in *Brown Jordan International, Inc. v. Carmicle* with a dispute over custody and control over devices and which caused the court to use the newly amended FRCP Rule 37(e).

As summarized in Kroll's electronic discovery case law database,

> In this wrongful termination case, the defendant employee sought the return of his personal laptop from the company plaintiffs, who refused to release the laptop unless the plaintiff could prove he paid for it with his own money. The defendant then remotely locked a company laptop he had in his possession, and refused to provide a password to unlock it throughout the case proceedings, rendering it inaccessible. The defendant also claimed to have lost a personal tablet and other devices containing screenshots of emails and other data "despite the near certainty of impending litigation." The plaintiffs filed a motion for sanctions under the newly amended Rule 37(e) for spoliation of evidence. The court determined that litigation was reasonably anticipated when the defendant destroyed or withheld data, and that he knew or should have known of his duty to preserve based on his background. Therefore, the court held that the defendant had acted with intent to deprive information from the plaintiffs, and accordingly ordered an adverse inference instruction for the jury.

As reported in a short summary of the same case by K&L Gates, the defendant's behavior included accessing 2.4 million files on his personal laptop, thus changing the metadata prior to forensic examination.

Another case involving control of personal e-mails of employees and data maintained by a third-party provider for purposes of discovery was *Matthew Enterprise, Inc. v. Chrysler Group, LLC.*

### C. Cross-Border Issues

[Add the following text at the end of the section.]

Outsourcing of many of the functions of a law firm may raise cross-border issues with respect to e-mail and other electronic communications. As part of its work, the ABA Commission on Ethics 20/20 recently

---


CH. 13.II.C.  ISSUES RAISED BY EMAILING

released its resolution and report dealing with outsourcing. Among the revisions approved by the ABA House of Delegates in August 2012 are the following changes:

- Model Rule 1.1 Competence, Comments [6] & [7] (Retaining or Contracting With Other Lawyers): These two new Comments illuminate the ethical responsibilities for retaining or contracting with other lawyers. One aspect of this related to cross-border issues is the possibility that these lawyers may be located in other countries, thus necessitating the need to communicate via e-mail and other electronic means which may not necessarily be protected by laws and regulations in those counties, as well as making sure that lawyers in those countries are properly apprised of their responsibilities for handling confidential materials in a secure manner.

- Model Rule 5.3 Responsibilities Regarding Nonlawyer Assistance: In the title, a subtle but significant change is made from "Assistants" to "Assistance." New Comments [3] & [4] address the use of nonlawyers outside the firm and provide as examples the hiring of a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. Comment [3] makes it clear the lawyer must make reasonable efforts to make sure that services that are outsourced to nonlawyers are provided in a manner that is compatible with the lawyer's professional obligations. This Comment also references several of the other rules, including Rule 1.1 Competence, Rule 1.6 Confidentiality, and Rule 5.5(a) Authorized Practice Of Law.

Cross-border issues with respect to e-mail are already receiving considerable attention due to the recent disclosures about NSA surveillance. One bill, H.R. 2399, the Limiting Internet and Blanket Electronic Review of Telecommunications and E-mail Act, or LIBERT-E Act, was introduced on June 17, 2013. The bill addresses and attempts to limit and provide oversight for surveillance of many types of electronic communication, including e-mail.

As more information is released about the scope of the activities of Edward Snowden, the extent of the NSA's surveillance programs is being revealed. Among the surveillance systems in place are not only those that collect information about e-mail activity, including both domestic

---

and cross-border e-mail, but also those systems that can search the content of e-mail messages. Out of concern for the protection of client confidentiality and the duties of lawyers under Model Rules 1.1 and 1.6, especially as it relates to the appropriate use of technology for rendering legal services, the American Bar Association issued its Resolution 118 on cybersecurity at its House of Delegates Meeting in August 2013.

The resolution states that the American Bar Association "condemns unauthorized, illegal governmental, organizational and individual intrusions into the computer systems and networks utilized by lawyers and law firms" and also "opposes governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, the confidential lawyer-client relationship, or traditional state court and bar regulation and oversight of lawyers and the legal profession." The resolution also encourages lawyers and law firms to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice, and also comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity.

Nelson and Simek continue to provide practical and timely information about the security risks to law firms. A short article published in January 2014 raised questions about the NSA's XKeyscore program, noting that the program allows NSA to gather phone numbers, e-mail addresses, and metadata as well as see e-mail content, browser history, and an IP address without obtaining a warrant and that this information can be stored for later analysis. The authors state that "while the NSA's purported mission is to target foreigners, the NSA sometimes retains the written content of e-mails sent between citizens with [sic] the U.S."

---


275 Id. at 1.

276 Id.


278 Id. at 3.
The authors offer advice related to law firm use of cloud computing, of encryption, of allowing Bring Your Own Device (BYOD) only with a Mobile Device Management (MDM) solution implemented, of moving data out of the United States in favor of having it stored in the United States with companies that pledge not to cooperate with the government, of passwords, of security audits, and of training. Our preference is to use encryption and recommend that lawyers consult an article by Holahan and Hussain on the basics of encryption.

A more expansive article by Nelson and Simek from March 2014 discusses Edward Snowden's revelations about the NSA's activities, including access to the Google and Yahoo! accounts of Americans, the XKeyscore program, harvesting of e-mails and instant messaging contact lists, searching e-mail content, tracking and mapping the location of cell phones, and tapping into Google and Yahoo data centers. The article raises specific concerns for lawyers about how they communicate and access information using e-mail and other technologies. It relates a story from the New York Times from February 2014 wherein a top-secret document demonstrated that an American law firm was monitored while representing a foreign government in trade disputes with the United States. The government of Indonesia had retained the law firm for help in trade talks, according to the February 2013 document. It reports that the NSA's Australian counterpart, the Australian Signals Directorate, notified the NSA that it was conducting surveillance of the talks, including communications between Indonesian officials and the American law firm, and offered to share the information.

Nelson and Simek report that ABA President James R. Silkenat asked the NSA's Director for an explanation of what policies and practices the NSA has in place to protect confidential attorney-client privilege that may be received or intercepted as well as whether these policies and practices were followed in the alleged law firm incident. The authors relate that while there is considerable discussion about keeping sensitive information out of e-mail messages, telephone conversations, and video conferencing systems, this also supports the need for using encryption to protect confidential client data and communications. They suggest that perhaps distrust of state-sponsored surveillance may result in a return to the past practice of face-to-face communications that are free from cameras or audio surveillance systems.

---

270 Id. at 3–5.
282 Id. at 5.
283 Id. at 6.
284 Id. at 8.
285 Id.
An extensive article by van Hoboken and Rubinstein discusses some of the important considerations for cloud computing in light of transnational surveillance. The authors observe that "at the technical and organizational level, industry players are responding with the deployment of encryption measures to safeguard their customers' data and there is an increased emphasis on the use of privacy enhancing technologies and innovative architectures for securing their services." Among the concerns they address are e-mail communications and the extent to which technology solutions such as encryption will be able to protect the security and confidentiality of information transmitted via e-mail. In terms of the scope and reach of the Stored Communications Act, a magistrate judge ruled and the District Court of the Southern District of New York affirmed that an SCA warrant obligated a U.S. provider to produce e-mails that were stored on a foreign server.

A key development related to cross-border issues in 2015-2016 was the "Schrems" case. On October 6, 2015, the European Court of Justice (ECJ) ruled in the Schrems case that the U.S.-EU Safe Harbor framework on the transfer of personal data from Europe to the United States was invalid. A subsequent posting on the K&L Gates Web site indicated that "[f]ollowing the ECJ's decision in the 'Schrems' case which has invalidated the Safe Harbor framework, multinational corporations may now face profound privacy law related compliance issues in a multitude of jurisdictions." As the authors explain, "[i]n Germany, the transfer of employees' personal data to U.S. group companies had already been a highly problematic and recurring issue in the past. After the ECJ's decision, the magnitude of this issue has significantly increased." The article goes on to provide advice on how U.S. entities can ensure an adequate level of data protection themselves.

An article by Leopold offers insight into how cloud computing vendors are planning to respond to the EU Safe Harbor ruling so that they

---

287 Id. at 496.
288 Recent Case: District Court Holds that SCA Warrant Obligates U.S. Provider to Produce E-mails Stored on Foreign Servers, In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), 128 HARV. L. REV. 1019 (Jan. 2015).
291 Id.
292 Id.
can meet stricter data protection requirements. Likewise, Clark observes that "[t]he ruling renders data transfers relying solely on Safe Harbor self-certification illegal, upending the status quo at the more than 5,000 companies that have self-certified under the agreement." Among the basic practices that can help companies avoid the regulatory pitfalls created by the removal of the Safe Harbor, she suggests employing good information governance practices, applying targeted collection methodologies, utilizing data culling techniques, establishing and enforcing strict data security measures, and partnering with companies that have the ability to host European data in the EU.

In terms of what the Schrems decision means for the legal profession and its clients, McFarlane and Rix provide valuable insights. They note that companies need to move quickly if the Safe Harbor was the primary basis on which they were transferring data and to consider alternative means of protection, such as using model clauses in contracts which have been negotiated and then agreed upon and signed off on by the European Commission. As the authors caution, even if a law firm is not multinational, the decision could still have an impact if that law firm outsources work or provides services outside its own country. Moreover, many law firms use client relationship management or enterprise resource planning systems that are based overseas or in the cloud. Although a grace period was available immediately after the decision that extended until January 31, 2016, the authors encourage law firms and other organizations to begin taking at least some action to prepare.

More recently, the vote by the United Kingdom to leave the European Union may have even more far-reaching implications for cross-border communications via e-mail and other technologies. On June 23, 2016, the referendum called "Brexit" was approved by a narrow margin after a bitter campaign, with one of the first actions being the resignation of Prime Minister Cameron. Because the United Kingdom is a major economic and political power in Europe as well as a major trading partner and long-time ally of the United States, it is too soon to tell the depth and breadth that the aftermath of the vote will have in many aspects of international relations, not the least of which is the transfer of data between the United States and the United Kingdom. It will take months for the United Kingdom to actually leave the EU and many regulations will

---

295 Id.
297 Id. at 50.
298 Id. at 51.
299 Id.
300 Id.
have to be rewritten. Another question is whether Brexit will be the first of several countries to leave the EU. Readers may recall that one option contemplated by Greece in the face of its significant economic issues and the imposition of strict austerity measures by the EU in exchange for providing a financial safety net was withdrawing from the European Union, a move known as “Grexit.”

III. ISSUES ARISING OUT OF IMPERMISSIBLE USE OF E-MAIL

A. Spam

2. The CAN-SPAM Act

a. What Is Covered

ii. “Transactional or Relationship Content”

[Add the following text at the end of the section.]

At least one court has held that “opting in” (i.e., providing consent to receive e-mails) does not constitute a prior relationship or transaction such that it would take those e-mails to which consent was given outside the definition of “commercial electronic mail” message.301

iii. “Hybrid” Messages

301[Replace the MySpace citation in footnote 93 with the following.] 2007 WL 1686966 (C.D. Cal. 2007).

v. “Initiating Transmission”

[Add the following text at the end of the section.]

The question of what constitutes “initiat[ing] the transmission” of covered e-mails arose recently in the context of social media messaging in Facebook, Inc. v. Power Ventures, Inc.302 Defendant Power Ventures, Inc. offered users the ability to access multiple social networking accounts through a single, integrated Web site at www.power.com. As a promotion of its Web site, Power offered users the chance to win $100 if they successfully invited and signed up new Power.com users. Power used participants’ Facebook login credentials to obtain a list of their Facebook friends, and asked the participants to select which of those friends should receive an

---

301 United States v. Rad, 559 F. App’x 148 (3d Cir. 2014).
Intellectual Property Law in Cyberspace

Second Edition

2016 Cumulative Supplement

G. Peter Albert, Jr.

and

American Intellectual Property Law Association

AIPLA

Bloomberg BNA

American Intellectual Property Law Association

Arlington, VA

Bloomberg BNA, Arlington, VA