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 .................................................. 703
   A. History of Electronic Messages ..................... 703
   B. Technical Overview .................................. 703
   C. Future of Electronic Communication ............... 704

II. Issues Arising Out of Permissible Use of E-mail .... 704
   A. Privacy/Confidentiality .................................. 704
      1. Work vs. Home ......................................... 706
      2. Document Retention Policies ....................... 709
   B. Discovery .................................................. 712
      1. Attorney-Client Privilege ............................. 712
      2. Possession/Custody/Control ......................... 717
   C. Cross-Border Issues .................................... 720

III. Issues Arising Out of Impermissible Use of E-mail 722
   A. Spam ...................................................... 722
      1. Legislative Efforts to Regulate Spam ............... 723
      2. The CAN-SPAM Act .................................... 724

13-1
B. Phishing
   1. Overview
   2. Technical Overview
   3. Impact on E-Commerce
   4. Legal Remedies
      a. Lanham Act
      b. Anticybersquatting Consumer Protection Act
      c. Uniform Domain Name Dispute Resolution Policy
      d. Computer Fraud and Abuse Act
      e. CAN-SPAM Act
      f. State Causes of Action

C. Spoofing
   1. Overview
   2. Communication Protocol Spoofing
   3. E-mail Spoofing
   4. Web Site Spoofing
   5. Legal Remedies
      a. Lanham Act
      b. Anticybersquatting Consumer Protection Act
      c. Uniform Domain Name Dispute Resolution Policy
      d. Computer Fraud and Abuse Act
      e. CAN-SPAM Act
      f. Telephone Consumer Protection Act

II. ISSUES ARISING OUT OF PERMISSIBLE USE OF E-MAIL

A. Privacy/Confidentiality

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

Several bills introduced in Congress over the last two 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. 587, 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. The bill summary notes that the Act

[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.]

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." 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. Both civil penalties and injunctive relief would be available.

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, 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." Among the various provisions in the proposed legislation are confidentiality of electronic communications, 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

---

6Summary: H.R. 537, supra note 1.
7Id.
9Id. §2(b)(1), (b)(2).
12Id.
Act, or LIBERT-E Act,\textsuperscript{10} 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.”\textsuperscript{11} Among the many provisions outlined in the legislation are: amending §501 of the Foreign Intelligence Surveillance Act of 1978\textsuperscript{12} with respect to access to certain business records for foreign intelligence and international terrorism investigations; amending §601 of the Foreign Intelligence Surveillance Act of 1978\textsuperscript{13} 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 §702(l) of the Foreign Intelligence Surveillance Act of 1978\textsuperscript{14} on the forms of assessments and reviews.\textsuperscript{15}

The Personal Data Privacy and Security Act of 2014\textsuperscript{16} 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.\textsuperscript{17} 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 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.\textsuperscript{18}

Although e-mail is not mentioned specifically in the definition of “sensitive personally identifiable information,” it is discussed in the

\textsuperscript{12}50 U.S.C. §1861.
\textsuperscript{13}Id. §1871.
\textsuperscript{14}Id. §1881a.
\textsuperscript{15}Id. It will be especially interesting to monitor these three pieces of legislation as they move forward to consider the extent to which email 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.
\textsuperscript{17}See Pub. L. No. 111-139, 124 Stat. 8 (Feb. 12, 2010).
\textsuperscript{18}Summary: H.R. 3990, supra note 16.
provisions of the legislation that address the requirements for notification in the event of a breach:

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

(I) 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).\(^\text{19}\)

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.\(^\text{20}\) 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.\(^\text{21}\)

A more narrowly tailored bill, H.R. 4157, the Farmer Identity Protection Act,\(^\text{22}\) 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:

---


\(^{21}\) Id.

the Environmental Protection Agency (EPA), or any EPA contractor or co-
operator, from disclosing the information of any owner, operator, or em-
ployee 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 regard-
ing the location of the owner, operator, livestock, or employee.\textsuperscript{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 is-
sues 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 “requires 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.”\textsuperscript{24}
In terms of e-mail, the bill “[d]irects businesses, within 30 days after dis-
covering 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.”\textsuperscript{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
E-mail Transparency Act, “[p]rohibits any officer or employee of the In-
ternal Revenue Service from using a personal e-mail account to conduct
official business.”\textsuperscript{26} This same restriction on the use of personal e-mail
accounts was included in a previous bill, H.R. 3520, the Exempt Organi-
zation Simplification and Taxpayers Protection Act of 2013.\textsuperscript{27}

The proposed legislation that most specifically targets privacy issues
with e-mail is H.R. 699, the E-mail Privacy Act.\textsuperscript{28} Among its most impor-
tant 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

\textsuperscript{23}Id.; see also Farmer Identity Protection Act, Summary: S. 1343, 113th Congress
\textsuperscript{25}Id.
bill/114th-congress/house-bill/1152/.
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.

Id.


In their article, Hadjipetova and Poteat discuss why the absence of a baseline federal privacy law is resulting in states becoming primarily legislative and policing authorities in the area of privacy and data security. They provide an overview of recent state legislative actions, with special emphasis on the so-called “California effect,” especially its impact on the Internet. 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. 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 enough to be willing to click on a link that is infected with malware that will install a virus.

Two helpful articles address how to keep data secure, including data that is transmitted via e-mail. First, Nelson and Sineck 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. Their

---

30Id. at 14–16.
31Id. at 16–17.
32Tommy Curb, Defend Against Social Engineering Attacks, PEER TO PEER 6–7 (Winter 2014).
primary recommendation, which is especially useful for e-mail, is to use encryption.\textsuperscript{34} 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{35}

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{36} 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{37}

1. Work vs. Home

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

A new book by Nelson, Ries, and Simek provides a chapter on e-mail security, along with substantial information on securing all types of devices.\textsuperscript{38}

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.\textsuperscript{39} 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.\textsuperscript{40} 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

\textsuperscript{34}Id. at 2–3.
\textsuperscript{36}Randy L. Dryer, Litigation, Technology & Ethics: Teaching Old Dogs New Tricks or Legal Luddites Are No Longer Welcome in Utah, 28 Utah Bar J. 12 (May/June 2015).
\textsuperscript{37}Id. at 14–15.
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.

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, Tigue 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 polices have little practical effect" and may even hamper the dis-

---

11 Id. at 4.
15 Id. at 7.
covery 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.\textsuperscript{48}

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.\textsuperscript{49} 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.\textsuperscript{50}

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\textsuperscript{51}—primarily intended to streamline and clarify the process for entities to apply 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."\textsuperscript{52}

Murphy discusses the impact of the increasing use of mobile devices by lawyers and law firm employees.\textsuperscript{53} 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.\textsuperscript{54} 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.\textsuperscript{55}

Beck notes that the data being stored on mobile devices continues to grow because of e-mail messages and attachments, text messages and

\begin{footnotes}
\footnotetext{48}{Id. at 8.}
\footnotetext{50}{Id.}
\footnotetext{53}{Coleman Murphy, Contain Yourself: Top Five Ways to Protect Mobile Data, PEEK TO PEER 16–19 (Mar. 2013).}
\footnotetext{54}{Id. at 17–19.}
\footnotetext{55}{Id. at 19.}
\end{footnotes}
other instant messaging services, app data, multimedia files and metadata.\textsuperscript{54} He notes that proper mobile device management (MDM) begins with information governance, including policies and standards.\textsuperscript{55} Essential MDM technical controls covered in his article include asset management, configuration management, encryption and remote secure wipe.\textsuperscript{56}

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.\textsuperscript{57}

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.\textsuperscript{58}

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.\textsuperscript{59} Nelson and Simek also reveal that these firms often fail to notify clients of a breach.\textsuperscript{60} 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.”\textsuperscript{61} 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. 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.’”\textsuperscript{62}

\textsuperscript{55}\textit{Id.} at 81.
\textsuperscript{58}Adam Carlson & Matt Wolf, \textit{Train to Strengthen Security’s “Weakest Link,”} \textit{Peer to Peer} 52–56 (Sept. 2012).
\textsuperscript{59}Sharon Nelson & John Simek, \textit{70% of Large Firm Lawyers Don’t Know If Their Firm Has Been Breached}, \textit{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).
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.

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.

---

63Reza Nabavi, _Keep Mobile Workers and Their Data Safe, Peer to Peer_ 26–27 (Sept. 2012).
64Tom DeSot, _Build a "Culture of Security," Peer to Peer_ 28 (Sept. 2012).
66Id. at 16–17.
67Id. at 17–18.
68Id. at 18.
70Id.
71Id.
(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 (Bring Your Own Device) 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). Nelson and Simek discuss the risks with BYOD in two articles on law firm technology, stating, for example, that "there 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 (Bring Your Own Device) 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—

---

74Id.
75Id.
76Id.
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.\footnote{Sharon D. Nelson & John W. Simek, How Lawyers Can Manage Their Technology Well, SENSEI ENTERPRISES (2015), http://www.senseient.com/news-press-articles/2015/1/5/tyukthxfvppg5izvcf3xmiwp2c80ad (last visited June 4, 2015).}

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.\footnote{Laurie Fischer, Dream the Impossible Dream: A Unified Approach to Information Security, P2P TO P2P 44–49 (Fall 2014).} 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.\footnote{Id. at 48.} 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.\footnote{Id.}

McLellan, Sherer, and Fedele provide a comprehensive review of the privacy risks and legal issues with BYOD from an international perspective.\footnote{Melinda L. McLellan, James A. Sherer & Emily R. Fedele, Wherever You Go, There You Are (With Your Mobile Device): Privacy Risks and Legal Complexities Associated With International “Bring Your Own Device” Programs, 21 RICH. J.L. & TECH. 1 (2015).} Among the challenges they identify are costs, employee behavior, and device security management versus employee personal data.\footnote{Id. at 10–21.} 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).\footnote{Id. at 20–34.} Finally, the authors cover BYOD programs in France, Germany, Spain, and the United Kingdom.\footnote{Id. at 35–44.} In their conclusion, they provide a number of helpful questions to consider when implementing or enhancing a BYOD program.\footnote{Id. at 44–50.}

There are also particular issues with BYOD programs related to unionized employees.\footnote{Patrick J. Beisell, Something Old and Something New: Balancing “Bring Your Own Device” to Work Programs With the Requirements of the National Labor Relations Act, 14 U. I.L.L. J. TECH. & POL’Y 497 (Fall 2014); see also Maria Greco Danaher, NLRA Supports Use of Employer’s E-mail System for Non-Work Purposes, 17 LAWYER’S J. 5 (2015).}

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
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.

2. **Document Retention Policies**

Add the following at the end of the section.

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. 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.

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 attorneys.” 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.

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.

---


82 Id. at 5.

of bad faith and with an appropriate sanction being to declare that the
patents-in-suit were unenforceable against Micron. 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 doc-
ument discarded; 3) facts that show that the plaintiff knew of the improp-
riety 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. In a more recent case, the court awarded a monetary san-
ton of $250,000,000, which would be applied as a credit against Ram-
bus’s more than $300 million judgment against SK Hynix, Inc. The on-
going 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 reten-
tion policies.

_**Scentsy, Inc. v. B.R. Chase, LLC**,_96 addresses both inadequate document
retention policies and concerns with the litigation hold process, including
using oral rather than written litigation holds and inconsistency in han-
dling and storing e-mail and other ESI.97 Another recent case involving

---

Remand, Court Finds Rambus’ Spoliation was in Bad Faith and Resulted in Prejudice,
com/2013/01/articles/case-summaries/on-remand-court-finds-rambus-spoliation-
was-in-bad-faith-and-resulted-in-prejudice-holds-patents-in-suit-unenforceable-against-

97Court Elaborates on the Standard for Bad Faith Spoliation in Patent Infringement Case,
http://www.krollontrack.com/resource-library/case-law?caseid=26475 (Kroll
Ontrack) (last visited June 21, 2013).

May 8, 2013). See Case Update: For Spoliation, Court Orders $250,000,000 “to be applied
as a credit against Rambus’s [$349 million] judgment against SK Hynix,” http://www.
ediscoverylaw.com/2013/05/articles/case-summaries/case-update-for-spoliation-court-
orders-250000000-to-be-applied-as-a-credit-against-rambus-349-million-judgment-


90See Concluding Litigation Hold and Document Retention Policies are “Clearly
Unacceptable,” Court Allows Depositions to Determine if Spoliation Occurred, http://
www.ediscoverylaw.com/2012/10/articles/case-summaries/concluding-litigation-hold-
and-document-retention-policies-are-clearly-unacceptable-court-allows-depositions-to-
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 BYOD, 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 potentially relevant evidence once litigation can be reasonably anticipated. For example, in response to failure to issue a litigation hold and to monitor preservation, the court in *Zest IP Holdings, LLC v. Implant Direct Mfg., LLC* awarded monetary sanctions and an adverse inference instruction against the defendants.

In *Herrmann v. Rain Link, Inc.*, 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

---

*No. CV 11-8557-CAS (DTBx), 2012 WL 4791614 (C.D. Cal. Oct. 5, 2012).*

*Id. at *3.*

*Id. at *5.*


the defendants' failure to suspend their routine practices as negligent as opposed to being done with intent to deprive the plaintiff of evidence.\textsuperscript{105}

In a third case, \emph{Sekisui American Corp. v. Hart},\textsuperscript{106} Judge Shira A. Scheindlin (author of the \textit{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.\textsuperscript{107}

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.\textsuperscript{108} In addition to granting the defendants' request for an adverse inference jury instruction, Judge Scheindlin awarded them reasonable costs, including attorney’s fees, that were associated with bringing their motion.\textsuperscript{109}

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 handling 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.”\textsuperscript{110} 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.\textsuperscript{111}

\textsuperscript{105} \textit{Id.} at *3.

\textsuperscript{106}945 F. Supp. 2d 494 (S.D.N.Y. 2013).

\textsuperscript{107} \textit{Id.} at 497 (footnotes omitted).

\textsuperscript{108} \textit{Id.} at 499–501.

\textsuperscript{109} \textit{Id.} at 509–10.


\textsuperscript{111} \textit{Id.}. 
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 overwriting. 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.

---


113 Id. at 3.


116 Id. at *4.
B. Discovery

[Add the following to the end of the section.]

A search of the K&L Gates Electronic Discovery Case Database and the Kroll Ontrack database[117] for cases since June 2013 indicates that discovery of e-mail continues to be a serious matter for clients and their 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,[118] breach of contract and trade secret misappropriation,[119] product liability,[120] copyright and trademark infringement and unfair competition,[121] a variety of federal and state laws,[122] patent infringement,[123] and breach of contract and conversion.[124] Additional cases concern insurance disputes,[125] lack of specificity in discovery requests,[126] and whether a deposition request about search methodology was unduly burdensome.[127] 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,[128] 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.”[129] In what

[129]Id.
appears to be a more expansive version for purposes of discovery, H.R. 3309, the Innovation Act, \textsuperscript{130} "[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 the parties have exchanged initial disclosures and core documentary evidence." \textsuperscript{131}

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{132}


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{133}

\textit{Id. at 2.}

For additional assistance with a broad range of issues related to electronic discovery, the International Legal Technology Association (ILTA)

I. **Attorney-Client Privilege**

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

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*,\footnote{135}{Id. See Electronic Discovery Law, Expert's Inadvertent Production Results in Waiver of Privilege Absent Sufficient Supervision by Counsel or Prompt Steps to Rectify Disclosure, http://www.ediscoverylaw.com/2012/05/articles/case-summaries/experts-inadvertent-production-results-in-waiver-of-privilege-absent-sufficient-supervision-by-counsel-or-prompt-steps-to-rectify-disclosure/ (K&L Gates May 24, 2012) (last visited June 28, 2012).} 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.\footnote{136}{806 F. Supp. 2d 44 (D.D.C. 2011). See Electronic Discovery Law, Court Denies Motion to Exclude Inadvertently Produced Email, Rejects Argument that 26(b)(5)(B) Request for the Email's Return Satisfied FRE 502(b)(3) Obligation, http://www.ediscoverylaw.com/2011/09/articles/case-summaries/court-denies-motion-to-exclude-inadvertently-produced-email-rejects-argument-that-26b5b-request-for-the-emails-return-satisfied-fre-502b3-obligation/print.html (K&L Gates Sept. 5, 2011) (last visited June 28, 2012).} In *Williams v. District of Columbia*,\footnote{137}{See Court Denies Motion to Exclude Inadvertently Produced Email, Rejects Argument that 26(b)(5)(B) Request for the Email's Return Satisfied FRE 502(b)(3) Obligation, http://www.ediscoverylaw.com/2011/09/articles/case-summaries/court-denies-motion-to-exclude-inadvertently-produced-email-rejects-argument-that-26b5b-request-for-the-emails-return-satisfied-fre-502b3-obligation/print.html (last visited June 28, 2012).} 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.\footnote{138}{Id. See Electronic Discovery Law, Expert's Inadvertent Production Results in Waiver of Privilege Absent Sufficient Supervision by Counsel or Prompt Steps to Rectify Disclosure, http://www.ediscoverylaw.com/2012/05/articles/case-summaries/experts-inadvertent-production-results-in-waiver-of-privilege-absent-sufficient-supervision-by-counsel-or-prompt-steps-to-rectify-disclosure/ (K&L Gates May 24, 2012) (last visited June 28, 2012).}
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 communicates 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 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*. 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.

---

140 Id. at ¶7-8, ¶11, 2011 U.S. Dist. LEXIS 113849, at ¶24.
A quick search of the K&L Gates database\textsuperscript{145} of electronic discovery cases related to e-mail in 2012 illuminates a number of common themes, including: spoliation and sanctions;\textsuperscript{146} privilege and waiver;\textsuperscript{147} forensic examination of e-mail accounts;\textsuperscript{148} cost shifting for processing e-mail accounts;\textsuperscript{149} and motions for a protective order over e-mail records, e-mails, text messages, and other related information from Yahoo! and Verizon.\textsuperscript{150}

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.,\textsuperscript{151} the court held that privilege had been waived for 347 pages of e-mail which had been inadvertently produced, out of a batch of 7500 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.\textsuperscript{152} 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

\textsuperscript{152}Id.
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 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:

153 Id.
154 Id.
156 Id. at *11–15.
157 Id. at *17–37.
158 Id. at *25–27.
159 Id. at *21–24.
161 Id.
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.162

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.”163

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.164

An article by DeLisi addresses the issue of protecting attorney-client privilege in an era where many, if not most, employers have Acceptable Use policies governing e-mail, Internet, social media and other technology and which include the right to monitor employee communications through this technology.165 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.166

162 Id. at 188.
164 Michele Desoer, Lawrence B. Lambert & Marc A. Wites, Does Copying an In-House Lawyer on Corporate Correspondence Render It Privileged?, THE FEDERAL LAWYER (May. 2014), at 60-63, 70.
165 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).
166 Id. at 3524.
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. 167

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. 168 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. 169

An article on e-mail etiquette also covers important issues with respect to maintaining the confidentiality of client information. 170 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 eavesdropping; guarding against emotional outbursts in e-mail; verifying receipt; and checking e-mail attachments before sending. 171

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. 172 In this case, not only did the defendant decide to classify approximately 50,000 pages of documents as privileged, but the defendant also marked 99 percent of documents as "Attorneys' Eyes Only." 173 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.

170George W. Kuney, Legal Form, Style, and Etiquette for Email, 15 TRANSACTIONS 59 (Fall 2013).
171Id.
failed to do 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., Pulsedcard, 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.171

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. 926, 928 (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. 1996). 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 156006, 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).175

There continue to be concerns about maintaining the attorney-client privilege as not only because of the surveillance activities of the NSA but also as e-mail and other forms of communications cross international borders.176 As stated by Macpherson and Stevenson, “increased globalization of legal advice brings greater risks to law firms and clients alike, especially when it comes to maintaining privilege of communications.”177 They observe that “privilege 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.”178 They state that

171Id. at 21.
172Id. at 22.
174Nina Macpherson & Theodore Stevenson III, Attorney-Client Privilege in an Interconnected World, 29 ANTITRUST ABA 28 (Spr. 2015).
175Id. at 28.
In 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.\textsuperscript{179}

The authors include a nonexhaustive 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).\textsuperscript{180}

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.\textsuperscript{181} 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:

[d]oes the site explain to the potential client \textit{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.\textsuperscript{182}

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.\textsuperscript{183}

2. \textit{Possession/Custody/Control}

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

\textsuperscript{179} Id.
\textsuperscript{180} Id. at 29–31.
\textsuperscript{182} Id.
\textsuperscript{183} Id.
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.  

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....” Resolution 105A makes several changes regarding e-mail:

- 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 accidently transmitted, for example, as when an e-mail or letter is misaddressed.

---

186 Id.
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 multi-jurisdictional practice of law.\textsuperscript{167}

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 \textit{Optiver Australia Pty. Ltd. \& Anor v. Tibra Trading Pty. Ltd. \& Ors},\textsuperscript{180} the court addressed what qualifies as “content” so that disclosure by service providers would be prohibited under the SCA.\textsuperscript{180} The plaintiff had issued a subpoena to Google 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.\textsuperscript{180} Most of this information was deemed to be “content” protected under the SLA. As stated by the court,

\begin{quote}
[i]he SCA prohibits \textit{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.\textsuperscript{181}
\end{quote}

The court did allow the plaintiff to receive non-content metadata.\textsuperscript{182} On the other hand, in \textit{Garcia v. City of Laredo},\textsuperscript{183} 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.”\textsuperscript{184}

\textsuperscript{170}Optiver Australia, 2013 WL 256771, at *1.
\textsuperscript{171}Id. at *2 (emphasis added).
\textsuperscript{172}Id. at *3.
\textsuperscript{173}No. 11-41118, 2012 WL 6176479 (5th Cir. Dec. 12, 2012).
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 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.

C. Cross-Border Issues

[Add the following 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 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

---

190Id.; see also Opening Web-based Emails Are “Electronic Storage” as Defined by the Stored Communications Act, ediscovery.com, http://www.ediscovery.com/pulse/case-law/detail/26541/#VFjAQ8t0yp (Kroll Ontrack) (last visited June 18, 2014).
191Kristen Uhl Hulse & Diane Quick, 2015 Hiring Predictions: E-Discovery and More, Peer to Peer (Sp. 2015), at 44–45.
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.200

- 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, 2013.201 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.202 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." The authors offer advice related to law firm use of cloud computing, of encryption, of allowing BYOD only with a Mobile Device Management (MDM) solution implemented, of moving data out of the U.S. 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.

---

204Id. at 1.
205Id.
207Id. at 3.
208Id. at 3–5.
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 that 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.

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.”

---

211Id. at 5.
212Id. at 6.
213Id. at 8.
214Id.
216Id. at 496.
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.\textsuperscript{217}

### 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 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.\textsuperscript{218}

      iii. "Hybrid" Messages

      \textsuperscript{18}[Replace the MySpace citation in footnote 93 with the following.] 2007 WL 1686966 (C.D. Cal. 2007).

   v. "Initiating Transmission"

   [Add the following 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 \textit{Facebook, Inc. v. Power Ventures, Inc.}\textsuperscript{219} 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

\textsuperscript{217}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).

\textsuperscript{218}United States v. Rad, 559 Fed. App’x 148 (3d Cir. 2014).

Intellectual Property Law in Cyberspace

Second Edition

2015 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
Hi Sara Anne – yes, you have permission to post your section of Chapter 13 on your faculty’s digital database. Please make sure to include copyright information (© Bloomberg BNA 2015, reprinted with permission) and a link to ordering the book, www.bna.com/bnabooks/lps. I’ve attached the final Word file, or I can send a PDF of your chapter if you like.

Happy New Year.

From: Hook, Sara Anne [mailto:sahook@iupui.edu]
Sent: Monday, January 04, 2016 2:00 PM
To: Turqman, Elizabeth <eturqman@bna.com>
Subject: 2015 Supplement

Dear Elizabeth:

I just received my copies of the 2015 Supplement to IP Law in Cyberspace, 2nd ed. Do I have permission to post my section of Chapter 13 (which is Section II) to our faculty’s digital scholarship database, IUPUI ScholarWorks? I’ve been doing this every year – it is a great resource.

Thank you so much!

Sara Anne Hook, M.B.A. (Finance), J.D.
Professor of Informatics and Program Director, Informatics Core
Professor, University College, IUPUI
Adjunct Professor of Law, Center for Intellectual Property Law and Innovation
Adjunct Professor of American Studies
Indiana University School of Informatics and Computing
535 W. Michigan Street, IT 589
Indianapolis, Indiana 46202
317-278-7690, 317-278-7669 (fax)