13

INTELLECTUAL PROPERTY ISSUES RAISED BY EMAIL

Michael B. Smith
Gibson Dunn, LLP
Palo Alto, California

Sara Anne Hook
Indiana University School of Informatics
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 Email ................................................... 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 Email ............................................... 722
    A. Spam .............................................................................................................. 722

701
1. Legislative Efforts to Regulate Spam ........................................... 723
2. The CAN-SPAM Act .................................................................. 724
   a. What is Covered .................................................................. 724
      i. "Exclusively Commercial" ........................................... 724
      ii. "Transactional or Relationship Content" .................. 724
      iii. "Hybrid" Messages .................................................. 725
      iv. "Electronic Mail Messages" ....................................... 726
      v. "Initiating Transmission"............................................. 727
   b. Requirements of CAN-SPAM Act...................................... 728
      i. Requirements for All Categories of Email..................... 728
         a) Headers................................................................. 728
         b) No False Header Information ............................... 730
         c) "Promotion" Liability ............................................ 730
      ii. Requirements for "Commercial" Email ....................... 731
         a) Deceptive Subject Lines ......................................... 732
         b) Opt-Out Provisions................................................. 732
            i) Opt-Out Must be Available for at Least
               30 Days ................................................................ 732
            ii) No Transmission of Commercial Emails
                After Opt-out ..................................................... 732
            iii) No Sharing of Opted-Out Email Address ............. 733
            iv) Subsequent Affirmative Consent ......................... 733
         c) Sending Behavior .................................................. 733
            i) Address Harvesting and Dictionary Attacks ......... 733
            ii) Automatic Creation of Email Addresses ............. 733
            iii) Open Relays/Proxies ......................................... 734
            iv) Aggravated Violations ....................................... 734
      iii. Sexually Explicit Email ............................................... 734
      iv. Enforcement ................................................................ 735
         a) Federal ................................................................. 735
         b) State ................................................................. 735
         c) Private Right of Action ......................................... 736
         d) Backlash: Opportunistic Plaintiffs ......................... 737

3. State Statutes ......................................................................... 738

B. Phishing .............................................................................. 740
1. Overview............................................................................... 740
2. Technical Overview ........................................................... 740
3. Impact on E-Commerce ..................................................... 740
4. Legal Remedies ................................................................. 741
   a. Lanham Act .................................................................. 741
   b. Anticybersquatting Consumer Protection Act ............ 741
   c. Uniform Domain Name Dispute Resolution Policy ....... 741
   d. Computer Fraud and Abuse Act ................................. 741
   e. CAN-SPAM Act .......................................................... 742
   f. State Causes of Action ................................................. 742

C. Spoofing.............................................................................. 742
1. Overview............................................................................... 742
2. Communication Protocol Spoofing ................................. 743
3. Email Spoofing ........................................ 743
4. Website Spoofing ..................................... 744
5. Legal Remedies ....................................... 744
   a. Lanham Act ....................................... 744
   b. Anti-Cybersquatting Consumer Protection Act .... 744
   c. Uniform Domain Name Dispute Resolution Policy ...... 745
   d. Computer Fraud and Abuse Act ........................ 746
   e. CAN-SPAM Act .................................... 746
   f. Telephone Consumer Protection Act .................... 747

I. INTRODUCTION

A. History of Electronic Messages

The first electronic mail message (email) was sent by Ray Tomlinson in late 1971 over ARPANET. With that first email message, Tomlinson also established the following address-naming convention: [name][@][host], which has since evolved into [name][@][domain name].

Initially, email was accessible only to individuals affiliated with governmental and educational institutions. However, starting in the early 1980s, a number of companies took steps towards making email generally available to the public via dial-up connections. These companies provided customers with the ability to send and receive personal email.

Today, of course, access to the Internet is ubiquitous, and so is access to email. The ubiquity of email gives anyone with an Internet connection the ability to communicate instantaneously with someone almost anywhere else in the world.

B. Technical Overview

The path of an email usually begins and ends with an email “client”—the program through which a user accesses his or her email account. An email client can be software-installed on an individual’s computer (common examples are Microsoft Outlook and Apple’s Mail.app), a Web-based interface such as those provided by Google, Yahoo, Microsoft and AOL for access to their free, Web-based email accounts, or software installed on a hand-held device or tablet, like RIM’s BlackBerry or Apple’s iPad. Typically, all of these clients provide users with an interface through which they can access their email account, which is maintained on a remote server along with other accounts associated with the same corporate network, organization, email service, Internet service provider, etc.

Once an email is composed, the email client connects to the sender’s email server using a series of data exchanges governed by the Simple Mail Transfer Protocol (SMTP). Once the sender’s email server authenticates the sender (that is, recognizes the sender as someone authorized to use that account), the sender’s email server then uses the information provided by the sender (specifically, the
email address entered into the "To:" line to locate the recipient's mail server. Once the recipient's server is located, the message is transmitted, again through a series of data exchanges governed by SMTP. Assuming the incoming email satisfies the requirements of the recipient's server, the email is accepted by that server, and routed to the recipient's email account. The next time the recipient accesses his or her mail server through a client, that email will be available to be viewed, downloaded, forwarded, etc.

The above (simplified) description involves four computers (or devices): The sending client, the sending server, the receiving server, and the receiving client. Depending on a number of factors, including how each client and server network is set up, and how the message data ultimately get routed over the Internet, many other computers may be involved in routing the email from the sender's client to the recipient's client. As will be discussed further below, each computer involved in routing the email usually will append some data to the header of the email, like a customs official stamping a passport. Also, depending on the configurations of the clients, servers, and other computers that may be involved in the transmission and routing of the email, multiple copies of the email may be generated and stored on different computers along the way. As discussed herein, this can have a profound effect on issues of privacy, confidentiality, and discovery.

C. Future of Electronic Communication

While email is perhaps the most ubiquitous form of electronic communication, other forms of electronic communication are becoming increasingly prevalent. In particular, instant messaging (IM), text messaging, and communication within social networks have become widely used means of electronic communication.

Considering that at the turn of this century, Facebook and Twitter did not exist, it is almost impossible to predict what services people will use to communicate with each other in the next five years. However, what is clear is that users will continue to communicate using increasingly more personally identifiable and targeted forms of electronic communication. This widespread adoption of electronic communication by users has not gone unnoticed by companies, which now aggressively use electronic communication to interact with both existing and potential future customers. Within this new and rapidly evolving communication ecosystem there are complex legal issues that need to be addressed. In this chapter, we discuss the current legal issues surrounding electronic communication and the solutions that the legislative and judicial branches have devised to address them.

II. Issues Arising Out of Permissible Use of Email

A. Privacy/Confidentiality

One question that continues to confront those who use Internet resources, such as email systems, social media sites, and virtual worlds, is where to draw
the line with respect to ownership of any material that is created through, posted on, or communicated through these technologies. Likewise, a related question is the privacy of any information that is uploaded or transmitted by a user, as well as control over that information. Some high-profile examples in the social media context have caused users to begin thinking about the privacy of the information they provide to these services and the extent to which they lose control over what is done with this information in the future, depending on the account setting they have selected. Many users are now calling for the default settings of these services to be set at the maximum privacy level, with the user having to affirmatively select less private settings versus needing to instead change a profile to be more secure.

The same questions are also posed with email messages. For example, in United States v. Warshak,¹ the U.S. Court of Appeals for the Sixth Circuit considered whether the account holder had an expectation of privacy regarding the content of email messages. The court held that “a subscriber enjoys a reasonable expectation of privacy in the contents of his emails ‘that are stored with, or sent or received through, a commercial ISP’” and that “the government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause.” In another case, the court found that personal emails that were stored in a public school’s email system were not subject to that state’s Freedom of Information Act. In Howell Educational Association MEA/NEA v. Howell Board of Education,² the court noted that:

> It appears that the system is intended to retain and store emails relating to official function, but that it is simply easier technologically to capture all the emails on the system rather than have some mechanism to distinguish them. We do not think that because the technological net used to capture public record emails also automatically captures other emails we must conclude that the other emails are public records. To rule as defendants request would essentially render all personal emails sent by governmental employees while at work subject to public release upon request. We conclude that this was not the intent of the Legislature when it passed FOIA.³

Nelson, Isom and Simek report a number of issues related to email among employers generally, but including law firms. These issues include lack of confidentiality, authenticity, integrity, non-repudiation, misdirection or forwarding, informality, permanence, malicious codes, and instant responses which may be inappropriate.⁴

An article by Micalyn S. Harris provides an overview of the risks of email in the workplace and provides some helpful suggestions of steps that the employer can take to reduce these risks.⁵ These risks include that email is available to system administrators and third-party and commercial ISPs, where obligations of confidentiality are less clear, hacking, infection from computer viruses, and

---

¹2010 WL 5071766 (6th Cir. 2010).
³Id at 539.
⁵Micalyn S. Harris, Online Activities & Their Impact on the Legal Profession: Is Email Privacy an Oxymoron? Meeting the Challenges of Formulating a Company Email Policy, 16 St. John’s J.L. Comm. 553, 556–58 (2002).
human relations issues, such as harassment, libel, and the creation of a hostile work environment. On the other hand, she notes that overly aggressive monitoring of email and Internet usage may have an adverse impact on employee morale and productivity, especially when personal tasks that the employee could easily handle quickly via the company’s computer system and email now require time away from the office.

An interesting situation with the confidentiality of email was presented with Google’s Gmail system, which scans the content of email messages to generate targeted advertising. This caused significant concerns with privacy advocates, but also has implications for attorneys and other professionals who have a duty of confidentiality. The New York State Bar considered whether Google’s practice of scanning the text of email messages to generate targeted advertising would breach an attorney’s duty of confidentiality, and in Opinion 820 concluded that it would not, as long as the information was not reviewed by humans. This is a significant issue for attorneys, given the popularity of Gmail, particularly among clients who may use it to communicate with their attorneys. Another feature of Google’s scanning process that argued against finding a breach of the duty of confidentiality was that the information that is retrieved from email messages is not revealed to third parties, including the advertisers for whom this process generates income. One author concludes that Opinion 820 has several implications for the activities of attorneys and the general acceptance of technology by the legal community, including that Gmail’s marketing purpose has no realistic impact on confidentiality and that, as new business models are developed to provide targeted advertising, these models will not threaten confidentiality as long as humans are not exposed to the information used to generate the advertisements.

1. Work vs. Home

One of the major difficulties in terms of the privacy and confidentiality of email regards home computers that are used for employment purposes. The issue goes beyond the traditional desktop computer, but should also encompass any mobile devices that the employee might use for both business and personal email communications. Although not email per se, many employees now communicate through texting and various social media sites. The opportunity to work from home or from anywhere outside the office has resulted in a workforce that may be available on a nearly 24-hour basis. In these situations the lines can be blurred between what is truly private and personal to the employee and what can legitimately be accessed by the employer, including information that the employer regards as proprietary.

Another aspect of the work-versus-home dichotomy is particularly apparent in intellectual property law. Many employees, but especially people in the IT and

---

6Kevin Raudebaugh, Trusting the Machines: New York State Bar Ethics Opinion Allows Attorneys to Use Gmail, 6 WASH. J.L. TECH. & ARTS 83 (2010).
7Id. at 84.
8Id. at 86.
9Id. at 91–92.
creative fields, engage in outside consulting and freelance work. The difficulty becomes how to separate what is truly work which the employee is doing for the company, versus what might be personal, freelance, or consulting work, as well as where to draw the line over the rights to inventive or creative work. In addition, where the employee uses email for both work-related and personal communications, there may be conflicts between the need to ensure that meaningful analysis is conducted during an electronic discovery process and guarding the employee’s right to privacy.

One area that is ripe for difficulties is the propensity for families to share the same computer, which also includes, perhaps, sharing user IDs, passwords, and email access. This can present a significant problem, not only in revealing confidential or proprietary information of the employer, but also in waiving the attorney-client privilege. For example, in *Willis v. Willis*, the court noted that the plaintiff waived the attorney-client privilege by using an account to communicate with her attorneys, to which her children had access for their own email. The court noted: “Under these circumstances, it cannot be said that the plaintiff had a ‘reasonable expectation of confidentiality’ in the email communications between herself and her attorneys, which communications were freely accessible by third parties.”

An opposite situation occurs when the employee uses the employer’s computer, network, or email system for personal matters. This has already become a significant issue where the employee is participating in social media, such as Facebook or YouTube, through an employer’s computer system, but is using that technology to criticize the company or reveal confidential or proprietary information. Likewise, there are dangers when the employee uses a company’s system for personal email, particularly if the employee is on notice that the employer has reserved the right to monitor that usage. Such behavior can also waive the attorney-client privilege. For example, in *Holmes v. Petrovich*, the plaintiff used the company’s computer to communicate with her attorney, even though she knew that company policy prohibited such use because she had read and signed the company’s policies related to the use of technology resources. The court stated that:

> As we will explain, an attorney-client communication “does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.” (Evid. Code, §907, subd. (b).) However, the emails sent via company computer under the circumstances of this case were akin to consulting her lawyer in her employer’s conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him.

The court distinguished this case from *Stengart v. Loving Care Agency, Inc.*, where the employee communicated with her attorney using her personal,

---

11Id. at 245.
132010 WL 1189458 (N.J. 2010).
Web-based email account, accessed from the employer’s computer, which was not covered by the employer’s policies.\textsuperscript{14} This is not a settled issue, however. In \textit{DeGeer v. Gillis},\textsuperscript{15} the court considered whether there was a waiver of privilege where the company email account and laptop were used to communicate with counsel. In that case, the court summarized a five-factor test to determine whether information stored on an employer’s computer waives the attorney-client privilege:

1. does the company employer maintain a policy banning personal use of emails;
2. does the employer monitor the use of its computer or email;
3. does the employer have access to the computer or emails;
4. did the employer notify the employee about these policies, and
5. how did the employer interpret its computer usage policy?

Likewise, there may be times when a family member’s access to a client’s email will be a legitimate part of the representation, as in the case of \textit{Green v. Beer},\textsuperscript{16} where plaintiffs’ lack of technological proficiency meant that they had to rely on their son in order to receive their emails. Although given a more modern spin, this is parallel to the exception that is recognized when family members or others act as agents of the client in order to facilitate the matter, such as with an elderly client or a client with a disability. More recently, the American Bar Association issued a new Formal Opinion on the duty to protect the confidentiality of e-mail communications with one’s client (Formal Opinion 11-459, August 4, 2011). This opinion recommends that the attorney warn the client about communications via email or other electronic means when there is there is significant risk that a third party may gain access. The situations discussed in the Opinion include a client’s use of email or a business device or system where there is risk that the communications will be read by the employer or another third party; by using a public computer at a library or hotel; by using a borrowed computer, or by using a home computer where other household members may have access.

An article by Meir S. Hornung discusses the complex issue of email privacy in the workplace.\textsuperscript{17} The article covers the right to privacy in the workplace, employer monitoring of employees, federal and common law electronic privacy protection, and what various courts have decided when considering the issue of an employer’s liability for privacy violations, including monitoring of personal email accounts, and state approaches to email privacy. As stated in the conclusion:

Employees in the private workforce currently enjoy no privacy in their electronic mail communications. Even though legal doctrines exist that would seem to recognize a right to privacy for employees, courts have been wary to extend that right very far into the workplace. As such, private employees have been subjected to

\textsuperscript{14}See also \textit{In re Oil Spill by the Oil Rig “Deepwater Horizon”} in the Gulf of Mexico, April 20, 2010, N. MDL 2179, 2011 WL 1193030 (E.D. La. 2011); and \textit{In re Royce Homes, LP}, No. 09-32467-H4-7, 2011 WL 873428 (Bmkcr S.D. Tex. 2011).

\textsuperscript{15}2010 WL 3732132 (N.D. Ill. 2010).

\textsuperscript{16}2010 WL 3422723 (S.D.N.Y. 2010).

\textsuperscript{17}Meir S. Hornung, \textit{Think Before You Type: A Look at Email Privacy in the Workplace}, 11 FORDHAM J. CORP. & FIN. L. 115 (2005).
monitoring of their email communications in the workplace, and will continue to be subject to such monitoring. Employers believe monitoring of employee email will stem liability for abuses such as corporate espionage and fostering a hostile work environment. At the same time, monitoring hurts the employees because it erodes employee privacy, and creates stress that has a direct negative impact on the emotional and physical health of employees.\textsuperscript{18}

2. Document Retention Policies

An important feature of the Federal Rules of Civil Procedure is Rule 37(e), known as the safe harbor provision. Rule 37(e) states that:

Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

However, in order to claim the safe harbor outlined under Rule 37(e), the party must have a document-retention policy in place and be able to demonstrate that the party had been following the necessary procedures and dates outlined for the timely and regular destruction of information. In other words, just having a policy is not enough, and even worse is to begin using the policy once the party becomes aware that there is impending litigation. Having a document-retention policy in place is especially important because the duty to preserve electronically stored information begins when litigation is reasonably anticipated, not when the actual suit is filed or when official notice of a lawsuit is received. Because there could be a dispute over when the duty to preserve started, it is advantageous to be able to show that there were routine procedures in place and that any gap between when a preservation order was issued and when the processes were halted was not due to bad faith or a deliberate intent to alter or destroy electronically stored information.

Commentary suggests that many large corporations see information as a strategic asset and are interested in managing it on an enterprise-wide basis. At the same time, many vendors are beginning to offer solutions to information management that include tools that integrate litigation preparedness. In addition, there is a growing appreciation for the lifecycle of digital information, from the time of its creation to the point at which it is no longer necessary and can be comfortably destroyed. Other phases in the lifecycle of information have been outlined in various decisions, most famously in Zubulake v. UBS Warburg,\textsuperscript{19} and might include designations such as active or online, near online, stored or archived, with each phase tending to mean that the data moves from being accessible to inaccessible in terms of an electronic discovery process. This not only has advantages in terms of saving costs on storage and maintenance, but also puts a limitation on the point at which that information would need to be produced in litigation, thus reducing its potential risk in the future. Any document-retention policy and procedures must be carefully crafted in order to reflect the unique nature of the corporation or organization. There may be valid business and legal

\textsuperscript{18}Id. at 160.

\textsuperscript{19}217 F.R.D. 309 (S.D.N.Y. 2003).
reasons to keep some information longer, and many entities will also be bound by federal and state regulations that dictate the time at which information can be disposed of. Health records and tax records are two categories of information that may have such requirements about retention. In addition, employees should be fully apprised of the document-retention policy, including monitoring procedures and adverse consequences of noncompliance, to ensure that there is compliance with the policy.

Email presents some special challenges related to document retention and destruction. At the moment, many corporations and organizations allow employees to manage their own email and to make independent decisions about how and when email messages should be deleted, filed, and archived. Moreover, email messages often provide coveted bits of information that can be used to prove culpability in cases ranging from employment discrimination to misappropriation of trade secrets. Perhaps it is in the area of intellectual property law where email messages sent by employees and others can be the most damaging, particularly if that information were to reveal confidential information about a company’s marketing strategy, research and development efforts, or upcoming product launch.

There are a number of sources of law related to the privacy of email messages in the United States. These include common law and the balance between the employee’s expectation of privacy and the employer’s business purpose for reviewing email, and the Electronic Communications Privacy Act, including the Wiretap Act and the Stored Communications Act. One author has noted that in the case of the Wiretap Act, there is confusion whether a message may be “intercepted” from electronic storage, and that exceptions include consent and the ordinary course of business. In terms of the Stored Communications Act, exceptions include conduct that is authorized by the electronic communication service provider or consent from the user to read communications. Remedies include actual and statutory damages and criminal penalties.

Another important facet of the management of email is to have an Acceptable Use Policy in place for employees, or anyone who might have access to, or be granted, email privileges. Under U.S. law, employers are allowed to monitor the use of the Internet, email, telephone service, and other devices. However, best practices would dictate that employees should be clearly informed of the policy and be required to sign a document indicating that they agree to be bound by the provisions of the policy. A company operating globally will want to be certain that it understands the laws and regulations related to workplace privacy in each country in which it has employees. Not only do statistics show that employees waste a significant amount of time sending personal emails, surfing the Web, and accessing social media sites, but that this behavior can also present risks to the employer as a whole. While it may be tempting to adopt a harsh policy that prohibits any kind of personal use of the Internet, email, telephones, and photo-

---

21 id. at 460.
22 id.
23 id.
24 id.
copiers, the likelihood is that this would not only be impossible to monitor, but it would also have a detrimental effect on morale. A better plan would be to make it clear in the policy what kinds of behavior would result in sanctions—such as visiting inappropriate Web sites, sending harassing email to colleagues, using any kind of technology to reveal confidential or proprietary information or to make disparaging statements about the company or its management—and then to invoke those sanctions for violations of the policy. For example, note the language in the Appropriate Use of Information Technology Resources from Indiana University:  

Incidental Personal Use "is the use of information technology resources by members of the Indiana University community in support of activities that do not relate to their university employment or studies or to other activities involving and approved by the university. Examples include use of email to send personal messages to friends, family, or colleagues, including messages relating to one-time minimal sales or purchase transactions, and use of the personal home page service to provide information about personal hobbies or interests. If personal use adversely affects or conflicts with university operations or activities, the user will be asked to cease those activities. All direct costs (for example, printer or copier paper and other supplies) attributed to personal incidental use must be assumed by the user."  

Nelson, Isom, and Simek provide a number of specific provisions for Acceptable Use Policies in law firms. They also note that the policy should explain the consequences for violations, including possible termination, suspension, and revocation of technology use privileges, and that it should be integrated into or coordinated with other policies related to records management and information security and should include monitoring and enforcement.  

Employees should also be cautioned about dangerous practices, such as sharing their computers with others and not keeping their access codes and passwords confidential. Another element of risk management for computer security is training employees to be watchful for strategies that would allow someone to gain access to the company’s computer systems. This not only includes "phishing" (the act of sending an email to a user in which the sender falsely claims to be a legitimate enterprise, in an attempt to get the user to surrender private information that will be used for identity theft) and similar high-tech tactics, but also through social engineering techniques. It is a natural tendency for people to want to be helpful, but employees should be routinely reminded that care should be exercised when responding to any requests for information that might reveal either personal information or information sufficient to gain access to the employee’s email, computer, or computer network. Suspicious behavior should be reported immediately to the appropriate supervisor, and all employees should receive sufficient training about computer and physical security measures that need to be taken to safeguard a company’s information. Often, it is the frontline staff who may be the first to recognize a potential threat, rather than IT personnel.

26NELSON ET AL., supra note 4, at 133–35.
27Id. at 135–39.
In her article on email in the workplace, Micalyn Harris provides a checklist for organizing and establishing an email policy, as well as a checklist for email users. The items on the checklist include:

- Understand how the email/computer system of the organization works.
- Establish and publicize a written policy with standards for creating email messages.
- Explain to employees that use of certain kinds of facilities may create problems for the organization, and therefore that the company prohibits or places limitations on certain uses, and limitations on sending and receiving certain kinds of messages.
- Establish procedures for storing and retrieving email documents, including that backup copies are handled appropriately. Explain that these procedures are designed to maximize ease of use while minimizing the risks associated with that use, and deserve to be (and will be) enforced. Establish procedures for overseeing implementation and ongoing enforcement.
- Educate clients, customers and suppliers about the organization’s email system with a view to reducing inadvertent abuse and assisting them in exercising good judgment regarding when and how, and for what purposes, it is appropriate to use email and when, if at all, arrangements for using encryption, a secure socket, or another method of communication are advisable.
- Consider the advantages of encryption and of making it easily available, either by using a public-private key or other encryption scheme, or by using secure sockets for privileged and confidential communications.
- Consider the advantages of installing a dedicated server for email, and of having a separate, dedicated server for the organization’s web site.

As technology becomes more robust, it is anticipated that more corporations will invest in centralized management and archiving solutions for handling email. Thus, the decision about when and how to save email messages may be taken out of the hands of individual employees, and instead coordinated at corporate headquarters by an automatic process.

B. Discovery

I. Attorney-Client Privilege

Email messages have proven to be a rich repository of evidence that can be relevant in litigation. Even before the revisions to the Federal Rules of Civil Procedure in 2006, a variety of decisions made it clear that email messages were fully discoverable, absent some sort of privilege or other protection. Moreover, the phrase “electronically stored information” or ESI was intended to encompass a variety of communication technologies, including email messages. The sheer amount of email that is exchanged presents that danger that email messages that

---

21Harris, supra note 5, at 562–65.
could have, and should have, been protected under the attorney-client privilege or as attorney work-product are inadvertently produced to the opposing party, thus waiving any protection they would have been granted.

The kinds of situations in which the attorney-client privilege can be waived for email messages are numerous and may often happen without any awareness of the risks. According to Matthew S. Cornick, email security can be breached in many ways, including “leaving confidential emails open on a computer screen for others to read over your shoulder, leaving your office for lunch or for a break while signed into your email program, printing emails that others can find, such as on a network computer, and using a password such as ‘password’ or names of family members that would be easy for others to guess.” Other security risks are creating a file on the computer called “passwords” or leaving passwords readily available, such as posted by the computer or in an unlocked desk drawer.

Although they were intended for the user’s convenience, some of the features of email can put confidential information at risk. For example, the careless use of such a common feature of email software such as Reply All may mean that the email message goes beyond the intended exchange between attorney and client. For example, in *Charm v. Kohn*, the court granted a motion to strike a privileged communication that was inadvertently sent to opposing counsel using the “Reply All” function. Although finding this a “close” question and weighing a number of factors, the court concluded that the defendant had met its burden of showing that reasonable steps were taken to preserve confidentiality and cautioned against the use of email features such as “reply all” and “bcc”. Another feature of email that may put privileged or confidential information at risk is the “autofill” function. In this case, in attempting to respond to an email message from his attorney, the defendant inadvertently sent his email message to a third party because the autofill feature on his email supplied the address of the third party. The court in *Multiquip, Inc. v. Water Management Systems, LLC* analyzed the situation under Rule 502 of the Federal Rules of Evidence, finding that since all of elements of FRE 502 were satisfied, there was no waiver of the attorney-client privilege. Furthermore, footnote 6 in the case outlines some helpful steps for preventing misdirected email messages in the future, such as:

1. erasing the relevant third party’s address from the email program’s address book;
2. checking to see if the autofill program worked as expected;
3. sending email to just one attorney who would then forward it as necessary, and
4. creating a “group” to send certain emails rather than relying on the autofill process.

In addition to the revisions to the Federal Rules of Civil Procedure, many states are fashioning similar rules to guide attorneys in the electronic discovery process. Many state court decisions may also provide clarity about how to deal

---

302009 WL 4261214 (D. Idaho 2009).
with electronically stored information, including email messages. For example, as reported by Jill Yaziji, the Texas Supreme Court recently set some limitations on the ability to directly access an opposing party’s files and outlined a benefit-burden test.²² Some important aspects of this case are that the party did have a process in place for periodic deletion of emails, which were backed up on hard drives but were then retained for only 30 days. The defendant asserted that this rendered the email messages not reasonably available to require their production under Texas Rule of Civil Procedure. In response to the request to search employees’ hard drives, the defendant asserted “intrusiveness, loss of confidentiality, disruption of business and the ultimate feasibility of plaintiff’s proposed methodology to retrieve the deleted emails.”²³ The court continued:

In sum, this opinion discourages direct access to an opponent’s files. One seeking such access should be able to show: (1) the party resisting discovery defaulted in its obligation to search for the requested material, i.e. a more diligent search would likely yield the information requested; (2) the search can be done through qualified experts who can articulate a search methodology based on familiarity with the opponent’s filing method to assure the court’s concern that it is not just a fishing expedition; and (3) a close connection between the electronic storage device and the claim in controversy that warrants such an invasive method of discovery.²⁴

The technology itself may also be a cause for inadvertent production of privileged emails, such as in Datel Holdings, LTD v. Microsoft Corp.,²⁵ where a software glitch was the reason that privileged portions of emails were not identified prior to being produced. Including others on the email message, including experts, family members, other employees, and any parties who are not the client—or who do not fall into a narrow group of recognized participants who may be needed to assist in the matter, such as a client’s guardian or an accountant—can result in a waiver of the privilege. As discussed above, a particularly dangerous situation occurs when the email address is shared, for example, when children or family members can access each other’s email from a home computer.

Since clients can also inadvertently waive the attorney-client privilege, they should be fully apprised of the need for communications and materials about the representation to remain confidential. This should be addressed in the representation letter or even in a contract that clients are required to sign, wherein they indicate the method by which they would like to be contacted and that they clearly understand the prohibition on sharing information with others. As part of this process, clients should be cautioned that any information sent via email is not necessarily secure, and they should be offered the options of encryption or password-protection of documents. In addition, all email messages sent from the law firm should include a confidentiality statement. Although not required, many practitioners with expertise in the area of computer security are advocating the encryption of any sensitive or confidential client information as a best practice.

²²Jill Yaziji, Texas Supreme Court Denies Right to Search Opponent’s Emails and Sets Standards for E-Discovery, 47 Houst. L.AW. 33 (2010).
²³Id.
²⁴Id.
²⁵2011 U.S. Dist. LEXIS 30872 (N.D. Cal. 2011).
Social media, which is now starting to take the place of email communication, can also pose potential risks for inadvertent waiver of attorney-client privilege. Clients should also be warned not to share information about the representation through Facebook, LinkedIn, YouTube, Twitter or blogs, to name but a few. In fact, there are attorneys who require that clients cease any activities related to Web sites and social media as a condition of accepting the case.

The revisions to the Federal Rules of Civil Procedure do provide at least some redress if information that could have been protected by the attorney-client privilege is inadvertently produced, and many state courts have adopted these revisions or variations of them. FRCP 26(b)(5)(B) states that:

If information produced in discovery is subject to a claim of privilege or of protection as trial preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies of it; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determining of the claim. The producing party must preserve the information until the claim is resolved.

The issue of waiver and a process for handling inadvertently produced electronically stored information (ESI) should be discussed in a “meet and confer” conference. As part of this conference, attorneys should consider a clawback agreement. Likewise, Model Rule 4.4(b), Transactions With Persons Other Than Clients, addresses the ethical issues of handling information that has been sent inadvertently:

(b) A lawyer who receives a document relating to the representation of the lawyer’s client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.36

In addition to the FRCP and the Model Rules, attorneys should also note the Federal Rules of Evidence, Rule 502 on limitations of waivers of the attorney-client privilege and work product.

Attorneys need to be particularly careful about the handling of email messages. Not only does careless use of email features present the risk of waiver of the attorney-client privilege, but it also impacts the overarching ethical duties of the attorney. One of the most important ethical principles articulated in the ABA Model Rules of Professional Conduct is the duty of confidentiality. Rule 1.6, Confidentiality of Information, states:

• A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly

authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).\textsuperscript{37}

It is also important to note that attorneys are responsible for the conduct of everyone in the law firm, including junior attorneys as well as support staff such as paralegals, secretaries, file room personnel, IT staff and librarians, to name but a few. These duties are articulated under Model Rules 5.1, 5.2, and 5.3. Moreover, the effect of Model Rule 5.3 is that the attorney retains the responsibility for oversight of third-party vendors, which could include electronic discovery service providers, computer forensics experts, and any other outside consultants who may be working on a case. This duty may become more significant with the increasing use of cloud computing or Software as a Service (SaaS) vendors to maintain and store client information, as well as to manage email messaging and archiving systems. In other words, the attorney cannot avoid violations of the Rules by "hiring away" the ethical breaches through the use of third-party vendors. The attorney has ultimate responsibility for the integrity of the e-discovery process, including the preservation of email messages as outlined in the litigation hold. It is important for attorneys, clients and vendors to understand their roles in the e-discovery process and the importance of properly handling ESI at all stages of the process. Attorneys who are responsible for selecting and working with third-party vendors will find it helpful to review various state ethical opinions, as well as ABA Formal Opinion 08-451.\textsuperscript{38}

Email seems particularly susceptible to spoliation, whether intentionally or inadvertently, and thus can subject attorneys and their clients to sanctions. On the one hand, email is so pervasive and is generated with so little thought of its significance that people may not even think about the necessity to preserve it for litigation purposes. On the other hand, since email so often contains evidence of guilt or fault, it is not uncommon for those with at least some technology savvy to attempt to delete or destroy potentially incriminating email messages through a number of tactics. Digital evidence, including email, is fragile and to the extent that it easily can be tampered with, the attorney is under a duty to work with the client on an ongoing basis to make sure that litigation holds are being followed. Not only has this duty been articulated in a number of decisions, including Zubulake v. UBS Warburg LLC,\textsuperscript{39} but it is also encompassed under Model Rule 3.4:

A lawyer shall not:

- unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential


\textsuperscript{39}229 F.R.D. 422 (S.D.N.Y. 2003).
evidentiary value. A lawyer shall not counsel or assist another person to do any such act . . . .\(^{40}\)

Several recent cases discuss the difficulty with preserving and producing email messages, particularly in complex cases, which can lead to a charge of spoliation and sanctions. Among the recent cases related to how to handle email messages, and the extent to which sanctions may be imposed, are Siani v. State University of New York at Farmingdale,\(^{41}\) where the court declined to grant a motion for sanction because, even though the preservation of email messages was deemed at least negligent, the plaintiff failed to establish that the lost emails were relevant. On the other hand, the court in Passlogix, Inc. v. 2E Technologies\(^{42}\) was willing to impose monetary sanctions for what it considered gross negligence and intentional spoliation of electronically stored information, including email, text, and Skype messages. The behavior in this case included deletion of email messages when the defendants had a duty to preserve evidence, and the failure to implement a litigation hold was gross negligence. Sanctions in the case of Northington v. H&M International\(^{43}\) included an order that defense counsel search all of its client's electronic media and hard copy files after the defendant failed to preserve and produce the electronically stored information that had been requested, with the court finding that this failure amounted to conduct that was "recklessly and grossly negligent". Other issues with the preservation and production of email messages are: whether email messages that are archived are not reasonably accessible; whether the production is more burdensome than the value of the information to the other party; and whether the costs of the production should be shifted from the producing party to the requesting party. For example, in Starbucks Corp. v. ADT Security Services, Inc.,\(^{44}\) the court not only declined to find that the archived emails were not reasonably accessible, but it also indicated that good cause existed to order the production anyway. Because of differences in the courts in the kinds of conduct that have been held to warrant sanctions, and in the sanctions imposed, one author has advocated a comprehensive adverse inference instruction standard for spoliation.\(^{45}\)

2. Possession/Custody/Control

In an attempt to guide attorneys in the handling of technology, the International Legal Technical Standards Organization (ILTSO) has drafted and is circulating


\(^{41}\)2010 WL 3170664 (E.D.N.Y. 2010).

\(^{42}\)708 F. Supp. 2d 378 (S.D.N.Y. 2010).

\(^{43}\)No. 08-CV-6297, 2011 WL 663055 (N.D. Ill. 2011); No. 08 C 6297, 2011 WL 662727 (N.D. Ill. 2011).

\(^{44}\)2009 WL 4730798 (W.D. Wash. 2009).

for comment its 2011 Guidelines for Legal Professionals.46 Its many recommendations for best practices for law firm technology include email server security, including access controls; use of encryption for any client data communicated through the Internet; an engagement letter that clearly specifies how the attorney and client should communicate, especially when exchanging confidential or personally identifiable information; and steps for notifying clients in the event of a security breach. The draft standards also advocate that law firms define the ownership of information technology equipment, data and services, the standard of care, and privacy obligations and restrictions on installation of unauthorized software as part of an Acceptable Use Policy.

Likewise, Stephanie Kimbro provides helpful information on security for mobile devices, particularly when those devices are used to store and transmit confidential client information.47 One of her special areas of caution is the use of an unsecure or free Wi-Fi service that may be available through bookstores, coffee shops or other public places.48 Kimbro notes that unencrypted email and Web pages not using Secure Sockets Layer (SSL) technology can be completely visible to an eavesdropper monitoring the network49 and suggests that no matter how one is connected to the Internet, whether by landline, Wi-Fi, or AirCard, all confidential communication should be done over secure protocols such as SSL, from end to end, noting that “[e]ven if a connection is secure from the laptop to the Internet Service Provider (ISP), it is not guaranteed to be secure from the ISP to the end user without additional protection, such as end-to-end encryption.”50 California Ethics Opinion No. 2010-179 notes:

Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate:

(1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security;
(2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information;
(3) the degree of sensitivity of the information;
(4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product;
(5) the urgency of the situation, and
(6) the client’s instructions and circumstances, such as access by others to the client’s devices and communications.51

47STEPHANIE KIMBRO, VIRTUAL LAW PRACTICE: HOW TO DELIVER LEGAL SERVICES ONLINE (2010).
49Kimbro, supra at 96.
50Id. at 97.
51See supra note 46.
Likewise, the New York State Bar Association’s Opinion 842 on using an outside online storage provider to store confidential client information, dated September 10, 2010, states: “A lawyer may use an online data storage system to store and back up client confidential information, provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer’s obligations under Rule 1.6.” The opinion goes on to state: “A lawyer using an online storage provider should take reasonable care to protect confidential information, and should exercise reasonable care to prevent others whose services are being utilized by the lawyer from disclosing or using confidential information of a client.” The opinion also notes the need for the lawyer to stay abreast of technology advances to be sure that the vendor uses the most current practices and procedures for the security of client information, as well as to monitor the changing nature of decisions related to privilege and protected information.

Among the items on Kimbro’s checklist of daily best practices for the use of technology are using full disk encryption on all computers, creating strong passwords and changing them regularly, and educating and reminding clients who are communicating online about protecting themselves using their own hardware.

The American Bar Association has issued an opinion on the confidentiality of unencrypted email. In *Information Security for Lawyers & Law Firms*, Nelson, Isom, and Simek discuss the duty of confidentiality for client information sent by email, the consequences of breach, whether access to the email was unauthorized, and the benefits of doing more than the minimum to protect email security. In its Formal Opinion 10-457 on lawyer Web sites, the American Bar Association also cautioned attorneys about the content of websites, offering legal information to the public, duties to prospective clients, and the dangers of inadvertently creating an attorney-client relationship.

As more corporations, organizations, law firms, and individuals turn to cloud computing to provide software and storage services, the issues of custody, possession, and control can become less clear. This issue was anticipated in an extensive article on the complicated policy issues that arise when email messages are stored online by ISPs and other third-party vendors. The paper discusses the storage revolution, the current rules for government access, including the Electronic Communications Privacy Act (ECPA), civil subpoenas, deletion from storage, and next-of-kin requests when a relative has died.

---

52. New York State Bar Association Committee on Professional Ethics. Using an Outside Online Storage Provider to Store Client Confidential Information. Op. 842 (9/10/10).

53. Id.

54. Kimbro, supra at 97. See also id. at 202–05, which include ethics opinions related to electronic communications in general, including email.


In 2004, a study conducted by the Center for Democracy and Technology examined industry practices related to data storage and access. The authors collected information from providers' Web sites and from direct contact with ISPs and the chief privacy officer or legal counsel for the seven largest commercial email providers. The survey covered five issues: deletion without subscriber request, deletion upon request, next-of-kin access, civil subpoenas, and under what situations does the vendor read customer email. The authors concluded: "Given the dramatic changes in technology, especially the shift to Web-based email and the offering of huge amounts of online storage, changes are needed in several areas. In particular, protecting user privacy calls for a mix of user education, industry policies to protect stored electronic communications better, and revisions to ECPA and other pertinent privacy laws." The authors conclude their article by articulating several policy recommendations, especially with respect to government access to stored email messages.

C. Cross-Border Issues

As there are significant differences in the privacy protections given to citizens in other countries, cross-border issues must be considered when sending email internationally. As one author notes: "Inconsistencies in legal frameworks can pose serious dilemmas for organizations and make their security programs quite complex. The communications industry sector has faced increasing difficulties with subpoenas for customer records that are protected in the provider's jurisdiction but not in the jurisdiction of the court seeking the information." In addition, "[i]t is the cross-border transfer of information that can also be problematic if one jurisdiction protects that data and the other does not," especially since "[f]requently data moves through several locations in its life cycle." Therefore, she notes the importance of tracking the origin of the information in order to determine which privacy protections travel with the data.

Another difficulty with email messages when considering cross-border issues is data retention. In 2002, the European Union adopted its Electronic Communications Directive, which requires "communication providers to retain traffic and location data of all communications taking place over mobile and land telephones, faxes, emails, chat rooms, the Internet, or any other communications device" and which also means that any security programs will have to provide for secure retention of this data with sufficient privacy protection. Another example of the European Union's efforts to regulate collection and processing of personal information is its Directive on Information Privacy Protection. As one author put it, "[t]he basic purpose of the directive is to ensure that personal

---

59 Id. at 614.
60 JODY R. WESTBY, INTERNATIONAL GUIDE TO CYBER SECURITY 209 (2004).
61 Id. at 209–10.
62 Id. at 210.
63 Id.
64 Id.
data are processed appropriately and with informed consent,” and “it imposes some fundamental obligations on companies to ensure that personal information is being handled fairly and lawfully.” As indicated by this author, “[f]rom the standpoint of the United States, possibly the most important feature of the directive is that it prohibits the transfer of personal data to countries outside of the EU that do not generate an adequate level of protection.” Fortunately, the United States and the European Union were able to negotiate a safe harbor framework to allow personal data to be transmitted.

Cross-border issues with email and other communications technologies are particularly difficult for attorneys because of the overarching duty of confidentiality and the danger of waiving attorney-client privilege or attorney work-product protection or revealing proprietary or trade secret information. One of the principles articulated in the draft 2011 Guidelines for Legal Professionals, currently being circulated by the International Legal Technical Standards Organization (ILTSO) for input and feedback from the legal profession, is that “[c]hoice of law and other complicating factors must be thoroughly assessed whenever client data moves across an international border for any reason.”

The same concerns are echoed in ABA Formal Ethics Opinion 08-451 for dealing with third-party vendors. One of the key provisions of the Opinion states: “When the work will be outsourced to a foreign country, the outsourcing lawyer should also ascertain whether the legal training received in that country is comparable to that in the United States, whether legal professionals in that country share the same core ethical principles with lawyers in the United States, and whether there is an effective professional discipline system.” In addition to the training and ethical issues of using attorneys outside of the United States, the Opinion also comments on the issue of privacy laws in foreign countries when legal services are outsourced to third-party vendors:

Consideration also should be given to the legal landscape of the nation to which the services are being outsourced, particularly the extent that personal property, including documents, may be susceptible to seizure in judicial or administrative proceedings notwithstanding claims of client confidentiality. Similarly, the judicial system of the country in question should be evaluated to assess the risk of loss of client information or disruption of the project in the event that a dispute arises between the service provider and the lawyer and the courts do not provide prompt and effective remedies to avert prejudice to the client.

Electronic discovery presents some interesting issues with respect to electronically stored information, including email messages, that is held by parties

---

66Id.
67Id. at 479.
68Supra note 46.
70Id.
in other countries. Recently, the Seventh Circuit issued its decision in *Heraeus Kulzer, GmbH v. Biomet, Inc.*, a trade secret misappropriation case. The court held that a party in a lawsuit pending in Germany could be subjected to U.S. discovery rules—which it acknowledged are “far broader than in most (maybe all) foreign countries”—even though the Court assumed that the discovery sought would not be allowed by the German court in which the case was pending. The court recognized that the discovery requests might be excessive and present “a danger of swamping a foreign court with fruits of American discovery” and that a “discovery demand in our courts might yield a haul of 30 million emails, few of which would be admissible in evidence.”

Still, the court held that where the requirements of the federal statute are met, a litigant in a non-U.S. dispute is entitled to obtain discovery in accordance with the Federal Rules of Civil Procedure, including Rule 26. The court also discussed a number of potential abuses that would warrant denial of such broad discovery. For additional recent cases on electronic discovery and foreign parties, see also *In re Global Power Equipment Group, Inc.* and *Accessdata Corp. v. ALSTE Tech. GMBH*.

### III. Issues Arising Out of Impermissible Use of Email

#### A. Spam

There are few more highly charged words in the current common parlance than “spam.” Once used only in reference to the distinctive mark of a canned luncheon meat (“SPAM”), the term (uncapitalized, to distinguish it from Hormel’s trademark) now is perhaps more regularly associated with email—in particular, with email that is annoying, offensive, deceptive, unwanted, or simply voluminous. The term can be used as a noun (“My mailbox is full of spam”) or as a verb (“Stop spamming me with emails about selling your car.”).

The use of the term “spam” in the online context can be traced back to the early days of the Internet and to a rather unlikely inspiration: a sketch performed by the famous British comedy troupe, Monty Python. In that sketch, a couple are ordering breakfast off of a menu on which every item has SPAM in it. As the sketch proceeds, the word “SPAM” becomes increasingly prevalent, not only in the list of menu items but also in the rest of the dialogue, rendering each speaker increasingly incomprehensible. Eventually, the dialogue is drowned out by a chorus of Vikings singing “SPAM, SPAM, SPAM, SPAM . . . .” This “SPAMming”

---

71633 F.3d 591 (7th Cir. 2011).
72Id. at 594.
73Id.
752010 WL 318477 (D. Utah 2010).