2019

Technology in Legal Practice: Keeping Ethical Obligations in Mind

Teresa J. Verges

Christine Lazaro

PLI Current
The Journal of PLI Press

Vol. 3, No. 3, Summer 2019

Technology in Legal Practice: Keeping Ethical Obligations in Mind

Teresa J. Verges

University of Miami School of Law

Christine Lazaro

*St. John's University School of Law**

I. Introduction

The use of technology in the legal profession is ubiquitous, expanding, and ever changing. Lawyers connect with their clients, co-workers, and others through

* The authors would like to thank Giselle Sardinas ('20 University of Miami), Richard Mayer ('20 St. John's University), and David Marron ('20 St. John's University) for their research and contributions to this article.

email. Cloud computing has allowed lawyers to create virtual and mobile workspaces, providing them with accessibility to client files and resources anywhere in the world. Social media allows lawyers to showcase their expertise and build their practice. Technology has undoubtedly impacted *how* lawyers provide legal services to their clients. However, as lawyers, we remain subject to long-standing professional and ethical obligations that govern our practice. This article explores how commonly used technology in legal practice implicates these ethical obligations, in particular, the duties of competence and confidentiality, and takes into account the constantly evolving guidance on these very important issues.

II. Attorneys' Ethical Obligation to Be Technologically Competent

The duty to provide competent representation is the first rule of the ABA's Model Rules of Professional Conduct ("Model Rules") for a reason: it is the foundation for all other ethical obligations. Model Rule 1.1 provides:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[1]

"Competence" today requires lawyers to have a basic understanding of the electronic devices, computers, and applications they use to render legal services—file storage, email, wireless technology, security, and social media—or risk the inadvertent violation of other ethical obligations, such as the duty to maintain client information confidential. If a lawyer lacks the necessary competence to understand the security of the technology used in his or her practice, the lawyer must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.[2]

For example, lawyers must be proactive in preventing unauthorized disclosure of confidential client information—this includes protecting electronically stored information (ESI) from cyber attacks and inadvertent disclosure. If using third-party service providers or digital storage media, lawyers must ensure that there are proper safeguards in place to protect confidential client information.[3] When sending emails, lawyers should take precautions, particularly when working in less secure environments, such as airports and hotels using "free Wi-Fi."[4] If lawyers

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

lack a basic understanding of the systems, devices, and software they are using, those lawyers risk inadvertent disclosure of confidential information or violating other ethical obligations.

The ABA Commission on Ethics 20/20 conducted an extensive review of the Model Rules in the context of advances in technology and the global use of technology throughout the legal profession. In response to the Ethics 20/20 review and ensuing recommendations, in 2012, the ABA emphasized competence in

Lawyers who lack a basic understanding of the systems, devices, and software they are using risk inadvertent disclosure of confidential information or violating other ethical obligations.

technology as a central requirement to Model Rule 1.1, by adding new Comment 8, which provides that "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risk associated with relevant technology." With the adoption of Comment 8 to Model Rule 1.1, "lawyers can no longer claim ignorance of technology as a defense for not knowing or not doing something the court or the bar believe they should have known or done."[5]

As of June 2019, thirty-six states have adopted Comment 8 to Model Rule 1.1, making it clear that lawyers in those jurisdictions must stay abreast of the technology used in their practice as a central requirement of their duty to provide competent representation.[6] California, while not formally adopting the Model Rules, relied on Comment 8 of Model Rule 1.1 to establish that the "duty of competence requires a basic understanding the electronic protections afforded by the technology in the use of their practice."[7]

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

At least two jurisdictions have gone further, adding a technology component as part of their continuing legal education (CLE) requirements. On September 29, 2016, the Florida Supreme Court not only incorporated Comment 8 to its own Rule 4-1.1 of the Florida Rules of Professional Conduct, but it also amended Rule 6-10.3 Minimum Continuing Legal Education Standards (MCLE) to require an additional three CLE hours in an approved technology program.[8] North Carolina now requires that at least one hour of CLE training be devoted to technology training.[9]

Alternatively, many states, including those that have not adopted Comment 8 to Model Rule 1.1, have approved technology-related courses for CLE credit, recognizing that technology training is an important part of a lawyer's ability to adequately and competently represent their clients. The New York Bar Association's Committee on Technology and the Legal Profession actively promotes MCLE credit programs in "subjects concerning technology that will impact the delivery of legal services."[10] The State Bar of California provides a comprehensive list of approved MCLE programs addressing professional responsibility issues that arise in connection with the use of technology.[11] The Texas Bar Association features a list of online technology CLE packages, each satisfying a portion of the state's ethics CLE requirement.[12]

Competency with respect to technology is most directly relevant in the area of e-discovery, and specifically, the collection, preservation, and production of ESI. As e-discovery becomes more common in client representation in litigation settings, a lawyer must be able to meet ESI demands. For example, a case may have the following e-discovery needs:

> (i) assessing e-discovery needs and ESI preservation procedures; (ii) identifying custodians of potentially relevant ESI; (iii) understanding the client's ESI system and storage; (iv) determining and advising the client on alternatives for the collection and preservation of ESI and associated costs; and (v) ensuring that the collection procedures, software and/or databases created will permit the lawyer to provide responsive ESI in an appropriate manner.[13]

Lawyers must assess their own e-discovery skills and determine whether or not they can meet the demands of the representation. Lawyers who lack the skills

themselves may associate with another lawyer or expert who has the necessary skills.[14] However, the lawyer will remain responsible and must ensure that the work of the associated lawyer or expert is done properly.[15]

The consensus among lawyers is that understanding the risks and benefits associated with the technology they use in their practice is fundamental to providing competent representation to clients—even without a formal adoption of Comment 8 in their respective state's rules of professional conduct, or technology requirement in their CLE obligations.[16] The challenge, of course, is staying abreast of technology given the speed at which it continues to advance and evolve. In that regard, perhaps a mandatory CLE requirement makes sense, since the lawyer's understanding of technology must also evolve.[17] This way lawyers are well prepared to "take reasonable steps to protect clients from injury resulting from ill-considered uses of technology."[18]

III. Protecting Client Confidential Information and Cybersecurity (and User) Threats

One of the fundamental principles of the attorney-client relationship is the lawyer's duty of confidentiality. A lawyer's assurance to a client that he or she will not reveal information relating to the representation, absent the client's consent, encourages fulsome disclosure of information necessary for effective representation. Confidentiality "contributes to the trust that is the hallmark of the client-lawyer relationship."[19] Model Rule 1.6(a), which sets forth the basic duty of confidentiality, provides that:

> 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).[20]

The duty of confidentiality is expansive, encompassing all information the lawyer gains through the representation, regardless of whether the lawyer received it directly from the client or another source.[21]

The ubiquitous (and increasing) use of technology in legal practice raises serious challenges to lawyers obligated to maintain client confidentiality. This is particularly true when the lawyer using that technology does not fully appre-

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

ciate its limits and vulnerabilities. It is no longer enough for a lawyer to lock client files in an office; lawyers must think about cyber threats from third parties and inadvertent disclosure due to their own or their employees' failure to follow security protocols. Recognizing these risks, the ABA adopted the Ethics 20/20 Commission's recommendation to add new subsection (c) to Model Rule 1.6, which would require lawyers to take steps to prevent the inadvertent or unauthorized disclosure of client information:

> A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client.[22]

What are "reasonable efforts"? The comment to new subsection (c) indicates that the rule envisions flexibility depending on the nature of the information to be protected as well as the resources of the firm.[24] Given that many cyber attacks and inadvertent disclosure of client information are a result of user error, at a minimum, lawyers (and their employees) need to have a basic understanding of the devices, computers, software, and other systems that they are using. The next sections discuss specific technology used by lawyers in their practice and best practices to prevent unauthorized access or disclosure of client information.

A. Cybersecurity

1. Protecting Client Confidential Information from Hacking and Other Unauthorized Access

Law firms electronically store vast amounts of confidential client information on their computers and servers.[24] In addition to confidential personal and financial information about their clients, lawyers in certain practice areas have access to sensitive information that has substantial economic value, such as confidential information about pending mergers and acquisitions, product development, intellectual property, and other financial information about publicly traded issuers. The potential value of this non-public information is obvious. Law firms are a far more attractive target for hackers than the corporate clients themselves because law firms often employ safeguards that are *inferior* to those used by the firms' clients.[25] Additionally, because the law firm will only usually have information

relevant to a limited number transactions or matters for the client, the sensitve information stored at the law firm is likely to be far less voluminous than the information held by the client—and thus easier to identify, steal, and monetize.[26]

Indeed, between 2011 and March 2017, over two-thirds of the country's 100 largest law firms (by revenue) experienced a cyber attack.[27] "Cybersecurity recognizes a . . . world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if.'"[28] In 2016, *The Wall Street Journal* reported that hackers had gained access to client files at some of the largest law firms in the country, including Cravath Swaine & Moore and Weil Gotshal & Manges, in connection with an insider trading scheme that involved planned mergers. The hackers, three foreign nationals, used stolen information to trade in advance of mergers, reaping over $4 million in profits.[29]

Other types of cyber attacks can be even more devastating to the law firm's practice and reputation. For example, in 2017, DLA Piper fell victim to an apparent "ransomware" (or "wiper-ware") attack, which disabled its operations across the globe for the first half of the year.[30] In a ransomware attack, a hacker obtains control of the client files and holds them "hostage" until the firm pays a fee. The Federal Trade Commission has described ransomware as "one of the most serious online threats facing people and business today."[31] Other firms have been victims of "wiper-ware"—malware that actually destroys client files altogether. Alternatively, a hacker can obtain client information purely for the purpose of publicly disclosing that information, as demonstrated in the now infamous "Panama Papers" incident, in 2016, when hackers stole and then publicly disclosed 11.5 million client records from the law firm Mossack Fonseca.[32]

Cybersecurity breaches can expose firms to significant potential liability. A security breach can reveal nonpublic information or a litigation strategy, disclose confidential information about both clients and employees, and result in the theft of funds held in trust accounts. Law firms that fail to take reasonable steps to safeguard their systems and information face serious repercussions, including, among other things, loss of clients, malpractice suits, and bar disciplinary proceedings.[33] For example, in December 2016, a Chicago law firm became the first firm in the United States sued in a putative class action for alleged data security vulnerabilities.[34] Moreover, "[w]ith 46 states and three U.S. territories having enacted breach notification requirements, law firms cannot hope to escape responsibility by failing to disclose an incident."[35]

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

Despite the high stakes and increasingly alarming headlines, a substantial number of firms still have not implemented sufficient cybersecurity systems, protocols, and training. Part of the problem is cost. At a minimum, cybersecurity requires having up-to-date software, which is expensive.[36] Even for large law firms, the economics of the practice place internal limits on the funds law firms will spend on new software programs and training.[37]

However, the best firewalls and encryption software cannot prevent security breaches caused by user error, which is why lawyers should not adopt a "set it and forget it" approach. For example, in 2015, Chinese nationals engaged in systemic cyber attacks against a number of major U.S. law firms to obtain information to facilitate insider trading.[38] The hackers obtained access to the email accounts of well-known partners (with practice areas that included mergers and acquisitions and intellectual property) and then relayed messages and other data from the partners' in-boxes to outside servers. Although many of the firms had strong firewalls protecting their own servers from direct misappropriation of information, the firms had failed to detect the "spear-phishing"[39] attacks that gave the hackers access to the partners' emails.[40]

Training law firm attorneys and support staff can substantially reduce the chances of a successful cyber attack. Seventy percent of law firms responding to the 2016 ABA Survey reported having some form of training available at their firm; however, a closer look at the numbers reveals a disparity between larger and small firms.[41] Live training has been found to be most effective among participants, but there are many less costly web-based options, including those offered free by the software and web-based program providers.[42]

Although it may be impossible to safeguard against every possible security risk, Model Rule 1.6(c) requires lawyers to use *reasonable* efforts to safeguard confidential client information. At a minimum, law firms should identify the nature of the information that needs to be secured, identify the threats to that information, assess their resources for development of a security protocol and, if necessary, consult with IT and cybersecurity specialists to develop and implement a cybersecurity program tailored to the nature and scope of the firm's practice.[43] The ABA recommends a variety of cybersecurity protocols to help law firms better safeguard client information against cyber attacks. Recommendations include:

- implementing firewalls and anti-malware/anti-spyware/antivirus software on all devices on which client confidential information is transmitted or stored;
- using secure Internet access methods to communicate, access, and store client information (such as through secure Wi-Fi, the use of a virtual private network, or other secure Internet portals);
- using unique complex passwords, changed periodically, including two-factor authentication;[44] and
- routinely updating and applying all necessary security patches and updates to operational and communications software. [45]

Implementing these procedures as part of a firm-wide privacy policy and incorporating ongoing training are proactive ways to prevent cyber attacks and other data breach incidents caused by human error. To the extent law firms use third-party vendors, investigators, and other service providers, firms should vet (and regularly review) those third parties to ensure they have appropriate safeguards and cyber policies in place to protect confidential information. Cyber insurance for law firms and third-party vendors is now also available to protect firms and their clients.[46]

2. Obligations After a Breach

As discussed above, a cyber attack is increasingly becoming a question of when, not if. If a data breach occurs, lawyers may have ethical obligations that depend on a number of factors, including "the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorneys' roles, level of authority, and responsibility in the law firm's operations."[47]

Just as lawyers must safeguard and monitor paper files to ensure there are no thefts, lawyers must also safeguard and monitor their electronic files to ensure that client information is protected. Lawyers must make reasonable efforts to monitor their electronic resources to determine whether a breach has occurred.[48] "When a breach of protected client information is either suspected or detected, Rule 1.1 requires that a lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."[49] The ABA suggests that lawyers adopt "incident response plans," which accomplish the following:

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

> Identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.[50]

If a lawyer suspects or knows that a breach occurred, the lawyer must then make reasonable attempts to determine which client information was accessed, just as a lawyer would have to do if it were physical files that were inappropriately accessed.

If a data breach occurs, the lawyer may have an obligation under Model Rule 1.4 to notify the client of the breach. If the data breach "involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event," the lawyer has a duty to notify current clients of the breach.[51] However, the ABA failed to extend such obligation to former clients "in the absence of a black letter provision requiring such notice."[52] It should be noted that Model Rule 1.16(d) has been interpreted "as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely."[53] Effective implementation of such policies may reduce the impact of a data breach on former client data.

Lawyers should also be cognizant of other legal requirements to disclose a data breach to both former and current clients. For example, state or federal law may require that the lawyer notify both current and former clients of a data breach that involves loss or disclosure of personally identifiable information.[54]

B. Lawyering in the Cloud: File-Sharing and Cloud Computing

Lawyers and law firms are increasingly using file-sharing and cloud-based services—also known as software-as-a-service (SaaS) models—in their practice. "Although there are different types of cloud services (such as those providing complete platforms or infrastructure), SaaS providers generally allow users to register for online services (many times for free for basic services) that permit them to use the software "service" as opposed to running the software natively on their computer."[55] SaaS services provide file storage and file-sharing capabilities, accessible across multiple devices or platforms from anywhere in the world.[56] Firms using SaaS no longer need to store documents locally on the hard drives of their computers or servers physically located on the firm's premises.[57]

File-sharing and cloud-based services, such as Dropbox, Google Drive, and Box, Inc., provide significant benefits to law firms. These services offer a convenient way to share files and documents with clients and co-counsel. Instead of shipping voluminous discovery during litigation, lawyers can "upload" a production with an invitation and password to opposing counsel. Because SaaS eliminates the need to save clients' sensitive documents and information on a laptop or other device, the risk of a security breach in the event of loss or theft of the device is reduced. In sum, use of cloud services can simplify document management and control costs.[58] These services also manage their own cybersecurity, software updates, and backups, in addition to employing their own IT staff, allowing law firms to cut substantial internal IT costs.[59]

SaaS technology is not without its risks. For example, Dropbox, the most highly used SaaS according to the 2017 ABA Tech Report, was hacked in 2013 and again in 2016, compromising approximately 68 million user login credentials.[60] Given our professional obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure" of confidential client information under Model Rule 1.6(c), it is incumbent upon lawyers to investigate available SaaS options and the provider's security measures to keep data safe.[61] Lawyers should avoid the "free" or "basic" service offered by these SaaS providers and opt for premium versions that offer heightened authentication and protections. An additional step may be to use data encryption to ensure that data is secure even if the SaaS service is compromised.[62] Of course, even when a firm has selected an excellent SaaS with appropriate security and support, training its lawyers, employees, and even outside consultants is essential.[63]

Several states have addressed the concerns of confidentiality, competence, and proper supervision of nonlawyers associated with the use of file-sharing and cloud-based services.[64] Many states have allowed the use of file-sharing and cloud-based services, as long as lawyers take reasonable steps and adequately assess the potential risks associated with the service, including:

- conducting due diligence to ensure that the online data storage provider has an enforceable obligation to preserve confidentiality and security of the information, to return the information if the law firm changes providers, and to notify the law firm if it is served with process requiring the production of client information;

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

- investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures in order to ensure that they adequately protect confidential information; and
- employing available technology and procedures offered by the SaaS to guard against reasonably foreseeable attempts to infiltrate data that is stored.[65]

The ABA has also provided additional guidance on selecting an SaaS service, recommending that lawyers ask and answer a series of questions about the security features of the service and other issues that implicate lawyers' ethical obligations, including storage and retrieval of client information.[66]

Texas cautions lawyers to remain vigilant when using cloud-based electronic storage and software systems. For example, a lawyer should be aware of whether a vendor or system "appears to be unusually vulnerable, based on systemic failures by that vendor or system."[67] In other words, if the lawyer is or should be aware that the vendor has been subjected to cyber attacks in the past, it may be less reasonable for the lawyer to trust the vendor. Additionally, a lawyer may determine that certain client information is too vulnerable to risk its possible disclosure or unauthorized access through a cloud-based system. In such a case, the lawyer may need to adopt additional encryption or other technological safeguards.[68]

C. Electronic Communications

Lawyers' use of email in their practice is nearly universal.[69] Email provides lawyers with an efficient, easy, and inexpensive way to communicate with clients, co-counsel, opposing counsel, and others. If their clients use email, lawyers can more easily comply with their obligations under Model Rule 1.4, which requires lawyers, among other things, to "keep the client reasonably informed," consult with the client, and respond to requests for information and updates.[70] Given our obligation to maintain the confidentiality of client information, however, lawyers need to make reasonable efforts to protect that information from being compromised by both external threats and user error.

As an initial matter, the ABA and many states that have addressed lawyers' use of email to transmit information relating to the representation of a client have concluded that it does not violate the professional ethical obligations as long as the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access to information relating to the representation.[71] Lawyers do not nec-

essarily have to encrypt an email message to a client, for example, if the lawyer is using a reputable and established email service provider that secures its own servers. This is because all of us, including lawyers, have a reasonable expectation of privacy in our communications with others, just as we do when using the U.S. Postal Service or a telephone.

Despite a reasonable expectation of privacy, however, lawyers are still required under Model Rule 1.6(c) to take reasonable steps to protect transmission of confidential client information. This starts with selecting an email service provider that has secured servers and encryption technology that will protect the law firm's email accounts and data from outside threats.[72] Indeed, most interceptions of emails are rare; the unauthorized access or theft of emails typically occurs through an outside hack of the email server itself or user error (such as clicking on a "phishing" email).

Even though interceptions are rare, lawyers should still consider encryption of emails that contain confidential information. By default, when a user sends a message, it is turned into code when in transit (transforming the plain text into unreadable cipher text by the sender's email server), but when it reaches the recipient's inbox, the message is transformed back to readable plain text by the recipient's email server. Most email providers, such as Microsoft and Google, offer additional levels of encryption, namely S/MIME enhanced encryption,

When a lawyer sends an email to the wrong recipient, he or she risks violating Model Rule 1.6 and waiving the attorney-client and work-product privileges.

which lawyers should consider using when sending sensitive client information. S/MIME requires both the sender and recipient to enter a private key to encrypt and decrypt the message, respectively.[73] This enhancement feature keeps unau-

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

thorized parties from reading the contents of an email in the event of a breach. Lawyers should evaluate on a case-by-case basis whether the electronic communication they are sending should be encrypted.[74]

User error also contributes to the inadvertent disclosure of confidential information when using email. When a lawyer sends an email to the wrong recipient, he or she risks violating Model Rule 1.6 and waiving the attorney-client and work-product privileges.

One of the most common causes of lawyers sending an email to the wrong recipient is through the "auto-complete" or "suggest names" feature in the email settings, usually set as a default. The auto-complete feature typically recommends names when typing a recipient's name or email address into the To, Cc, and Bcc fields.[75] While this tool is convenient for all email users, it also presents the risk of linking the wrong person to the message (either because the names are similar or because the user accidentally clicks on the wrong name). Typing out the email addresses of the intended recipients is a foolproof way to ensure that the intended recipients are appropriately linked to the outgoing message. Law firms can also opt to purchase software programs that detect when an incorrect recipient is linked to an outgoing message and prevent the email from being sent.[76]

Lawyers should also think about the attachments to their emails. Even if no confidential client or work-product information is in the text of the email, attachments may contain metadata. The ABA has defined metadata as embedded information contained in electronic documents, which include the last date and time that a document was saved, and data on when it last was accessed.[77] Anyone who has an electronic copy of such a document usually can "right click" on it with a computer mouse (or equivalent) to see that information.[78] When sending a file through email, lawyers should ensure that they have scrubbed the file for metadata, usually a simple process accessed through the software program in use.

In the event of inadvertent disclosure to third parties, Model Rule 4.4(b) provides some protection and comfort to the sender:

> A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.[79]

If the recipient is a lawyer, he or she is ethically obligated to notify the sender and follow his or her instructions on whether the lawyer should return or destroy the document or ESI. However, some jurisdictions do require a lawyer to advise his or her client that confidential information was inadvertently transmitted to and read by opposing counsel.[80]

Lawyers should also exercise caution when receiving emails, particularly suspicious emails from unknown individuals allegedly seeking legal representation. Many cyber attacks on law firms have occurred because the hackers were granted access to the firm's systems through an inadvertent click on an email.[81] Through cyber resilience education, lawyers can learn to recognize the warnings signs and avoid opening a link that may infect their law firm's system with malware or ransomware. Lawyers should consider participating in CLE-approved technology and cybersecurity courses. Lawyers and law firms can also join the Legal Services Information Sharing and Analysis Organization (LS-ISAO), an information-sharing group that disseminates information about cyber threats.[82] LS-ISAO allows lawyers to check if the suspicious email or sender has already been flagged as cyberterrorism by others in the legal community. The LS-ISAO also provides various educational tools to help lawyers learn how to respond to cyber threats and learn which cybersecurity tools can most effectively prevent a breach.[83]

IV. Avoiding Social Media Landmines

Lawyers' use of social media to promote their practice has expanded significantly in the last decade. "Social media" encompasses all websites and applications that enable users to create and share content or participate in social networking.[84] According to the ABA's 2017 technology survey, over 90% of lawyers use social media, and 73% actively use social media as part of their marketing strategy.[85] The most common social networking sites lawyer use are Facebook, LinkedIn, and Twitter.[86] By posting or "tweeting" about the latest legal issues, trends, and successes through social media sites, "blogging" and using other platforms, lawyers can expand their professional networks, establish their expertise in a given field of practice, and grow their client base.[87]

However, in contrast to members of the public at large, lawyers are always subject to the professional responsibility and ethics rules of their respective states. Indeed, a lawyer can violate professional rules of conduct even when not acting in a professional capacity.[88] In March 2018, the ABA's Standing Committee on

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

Ethics and Professional Responsibility issued Formal Opinion 480, reminding lawyers who "communicate about legal topics in public commentary" that they must comply with the professional conduct rules governing their practices, the most significant of which is the duty of confidentiality.[89] Formal Opinion 480 identified a number of potential landmines for lawyers using social media, including, among other things, inadvertent disclosure of confidential client information, improper solicitation, and inadvertently forming attorney-client relationships with readers of public commentary.[90]

A. Inadvertent Disclosure Through Posting, Blogging, and Location Technology

Even with the best cybersecurity software and policies in place, a lawyer may nevertheless inadvertently compromise confidential client information (including client identities) through a careless tweet, Facebook or blog post, or even use of a listserv. The duty to protect confidential client information extends to current, former, and prospective clients.[91]

Before posting any information about a client or a client's representation online, a lawyer must obtain the client's consent, unless the disclosure meets one of the exceptions listed in Rule 1.6(b).[92] ABA Formal Opinion 480 reminds lawyers that the duty of confidentiality extends not only to matters or information communicated by the client, but all information learned during the scope of his or her representation, even information that is otherwise publicly available.[93] Absent client consent, lawyers who discuss their practice area, legal developments, and case examples should make every reasonable effort to prevent against the inadvertent disclosure of confidential client information and, depending on his or her jurisdiction, the client's identity.[94]

The use of "hypotheticals" can violate Rule 1.6 "if there is a reasonable likelihood that a third party may ascertain the identity or situation of the client from the fact set forth in the hypothetical."[95] In 2010, for example, an attorney received a sixty-day suspension from the Illinois Supreme Court for disclosing too much information about her clients on a blog.[96] The blog was not password-protected, and the attorney referred to her clients by their first name, a derivative of their first name, or jail ID number, and further disclosed that some of her clients had committed perjury.[97] Other posts included derogatory comments about judges, providing sufficient information to ascertain their identities.[98]

Public posts made in response to a client's public comments can get an attorney into trouble. The Georgia Supreme Court rejected a petition for voluntary reprimand (the mildest form of public discipline permitted under that state's rules) where a lawyer admitted to disclosing information online about a former client in response to negative reviews on consumer websites.[99]

In another case, a Florida public defender lost her job after making an off-the-cuff comment and posting a picture of her client on her private Facebook page.[100] During the middle of a murder trial, the public defender took a picture of her client changing into clothes that his family had brought with them for him to wear during the trial. She then posted the photo of her client's leopard-print underwear, with a caption making fun of its appropriateness as courtroom attire. Although her Facebook page was private, someone saw the post and notified the judge, who declared a mistrial. The lawyer was promptly terminated from her employment, and her supervisor told the press "that clients are entitled to lawyers' loyalty and respect, adding that posting humiliating photos undermines the client-lawyer relationship."[101]

Lawyers should also be careful when using listservs. Although listservs are a valuable and inexpensive way to obtain advice and guidance from fellow practitioners, they can present problems if the attorney posing the question or referral provides too much information about the client. In a May 2012 opinion, the Illinois State Bar Association's Ethics Committee advised that attorneys seeking guidance from others through a listserv without their client's consent is permissible if the inquiry will not reveal sufficient information about his or her client.[102]

Lawyers can also inadvertently disclose confidential information through a social media site's technology. For example, Facebook and LinkedIn have the technology to import contacts from Outlook; thereafter, any of the user's connected "friends" can easily identify others with whom a lawyer is "friends," including the identify of his or her clients. When combined with geo-mapping and location services technology of a smartphone loaded with the social media app, a lawyer may inadvertently reveal a meeting with a client or an expert on a matter.

As with the use of a lawyer's own computers, devices, and firm software, technological competence is key. Lawyers can ensure against inadvertent disclosures by understanding the technology and privacy settings of the social media platforms and apps they are using with their clients and in their practice.

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

B. Advertising, Solicitation, and Unauthorized Practice of Law

Lawyers' use of social media to promote their practice and expertise presents additional challenges. Unlike print media, where a lawyer can limit his or her message to a specific audience (and otherwise ensure it complies with applicable professional rules in his or her jurisdiction), social media does not have jurisdictional boundaries. Moreover, certain networking sites such as LinkedIn have fields that allow the user to list "specialties" and other persons linked to the user to "recommend" someone for a particular specialty or expertise. These functions may create problems for lawyers, depending on their jurisdiction.[103]

Whether using "old" or new social media, lawyers are clearly prohibited from making any "false or misleading communication" about their services.[104] Beyond this prohibition, the rules are less clear. The ABA approved changes to Model Rule 1.8, Duties to Prospective Clients, in recognition of the fact that an initial contact with a potential client may occur in many ways other than a face-to-face meeting. The amended rule provides that a person who "consults" with a lawyer (replacing the word "discusses") about the possibility of forming a client-lawyer relationship with respect to a matter is considered a "potential client."[105]

The Ethics 20/20 Commission did not suggest any changes to the text of Rule 7.2, Advertising, which generally allows attorneys to "advertise services through written, recorded or electronic communication, including public media." It did propose, however, changes to Comment 5, adopted by the ABA, to clarify prohibitions against paying others for the recommendation of a lawyer's services, explaining that lawyers could use lead generation services (*e.g.*, "pay-per-click" services) as long as those services do not "recommend" the lawyer.[106]

Finally, the ABA recently reminded lawyers that they "should take care to avoid inadvertently forming attorney-client relationships with readers of their public commentary."[107] In contrast to the publication of an article, commentary, or advertisement in print media, social media opens the door to interaction. A blog post, for example, usually invites comments and further interaction, which could give rise to an inadvertent client-lawyer relationship. ABA Formal Opinion 480 suggests that "where practicable, a lawyer should include appropriate disclaimers on websites, blogs," and other posts.[108]

C. Using Social Media As an Investigative Tool

Social media use has become ubiquitous. As a result, it has also had an important role in litigation. Reviewing social media accounts, profiles, and posts of parties, witnesses, and jurors is a valuable way to obtain relevant information for a pending litigation, outside the formal discovery processes.[109] However, many social media sites provide an electronic notification to the account holder when someone has viewed his or her page. Such notifications may implicate a lawyer's ethical obligations.

The New York State Bar has issued social media guidelines to provide some guidance on the permissible uses of social media during the course of a representation.[110] Guideline 4 governs the review and use of evidence from social media. Generally, a lawyer is permitted to view the "public" portions of a user's social media account.[111] However, it becomes much more complicated if a lawyer sends a "friend" request or seeks to view the restricted portion of a user's page.

If the person is unrepresented, New York's guidance states that a lawyer is permitted to communicate with the individual and seek to obtain access to the restricted portions of the person's social media account. However, the lawyer must do the following:

> However, the lawyer must use her full name and an accurate profile, and may not create a different or false profile in order to mask her identity. If the unrepresented party asks for additional information from the lawyer in response to the communication or access request, the lawyer must accurately provide the information requested by the person or otherwise cease all further communications and withdraw the request if applicable.[112]

If a party is represented, the lawyer should not have any communication with the person without permission of that person's counsel and, as a result, should not attempt to view restricted portions of their social media accounts.[113] Pursuant to a lawyer's ethical obligations, the lawyer should also not use an agent to do that which they cannot do themselves.[114]

The New York County Lawyers Association recently issued an opinion specifically with respect to a lawyer's use of Snapchat to obtain information about adverse parties.[116] However, because of the way Snapchat is configured, it is not possible for a lawyer to access a user's page unless a request is made to the person

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

to "add" the lawyer as a "friend." Unlike certain other social media platforms, Snapchat's "add friend" feature does not give the lawyer the opportunity to make the requisite disclosures. Accordingly, "lawyers are ethically prohibited from sending an 'add friend' request to an adverse party or witness."[116]

V. Conclusion

The intersection of technology and legal practice presents exciting possibilities and creates new challenges for lawyers. Staying technologically competent, obtaining assistance when necessary, and remaining vigilant of our professional responsibilities are the keys to successfully meeting those challenges and practicing law in the twenty-first century.

Professor **Teresa J. Verges** is the Director of the University of Miami School of Law's Investor Rights Clinic and Lecturer in Law. Professor **Christine Lazaro** is a Professor of Clinical Legal Education and the Director of the Securities Arbitration Clinic at St. John's University School of Law. A version of this article has been published in the Course Handbook for PLI's Securities Arbitration 2019.

NOTES

1. Model Rules of Prof'l Conduct R. 1.1 (Am. Bar Ass'n 2018).
2. Cal. State Bar, Formal Op. 2010-179 (2010).
3. *See, e.g.*, Fla. Bar Ass'n, Op. 10-2 (2010) ("Lawyers must learn such details as whether the Device has the ability to store confidential information, whether the information can be accessed by unauthorized parties, and who can potentially have access to the information."). Similarly, lawyers need to ensure that the transmission of confidential client information is secure. *See, e.g.*, Fla. Bar Ass'n, Op. 06-02 (2006) ("A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata.").
4. *See* David Ries, *2017 Security*, ABA (2017), www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html ("Public wireless (WiFi) networks present a high security risk, particularly if they are open . . . both authorized users and attackers, may be able to intercept or view data and electronic communications transmitted over the network."); *see also* Ken Kerschberg, *Your Ethical and Legal Duties When Using Wireless Networks*, Forbes (Dec. 12, 2011), www.forbes.com/sites/benkerschberg/2011/12/12/your-ethical-and-legal-duties-when-using-wireless-networks/#4529b1e23e9b ("In 2010, for example, Google famously swept data from thousands of unsecured private networks, an act known as "wardriving" that many hackers continue to this day."); Robert Siciliano, *What Is Wardriving?*, McAfee (June 23, 2014), https://securingtomorrow.mcafee.com/consumer/identity-protection/wardriving/ ("We call the act of cruising for unsecured wireless networks 'war driving.'").
5. Mark Rosch, *2017 Technology Training*, ABA (Dec. 1, 2017), www.americanbar.org/groups/law_practice/publications/techreport/2017/training.html.
6. Every state except California has adopted the Model Rules of Professional Conduct, and thirty-seven of those states have also adopted the comments. ABA CPR Policy Implementation Comm., State Adoption of the ABA Model Rules of Professional Conduct and Comments (June 5, 2017), www.americanbar.org/content/dam/aba/administrative/professional_responsibility/adoption_mrpc_comments.authcheckdam.pdf. Thirty-six states have adopted Comment 8: Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Massachusetts, Minnesota, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. *See* Robert J. Ambrogi, *Tech Competence*, LawSites (2019), www.lawsitesblog.com/tech-competence/ (last visited June 20, 2019).
7. Cal. State Bar, Formal Op. 2010-179 (2010), *supra* note 2.
8. *See In re* Amendments to Rules Regulating Fla. Bar 4-1.14 and 6-10.3, 200 So. 3d 1225, 1228 (Fla. 2016).

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

9. *See CLE Requirements in North Carolina for Lawyer*, N.C. State Bar Continuing Legal Educ., www.nccle.org/for-lawyers/requirements/renewing-lawyers/ (last visited July 26, 2019).
10. *See Committee on Technology and the Legal Profession*, N.Y. State Bar Ass'n, www.nysba.org/CustomTemplates/SecondaryStandard.aspx?id=71935 (last visited July 26, 2019).
11. *See Online Participatory MCLE Programs Related to Technology*, State Bar of Cal., www.calbar.ca.gov/Attorneys/Conduct-Discipline/Ethics/Ethics-Technology-Resources/Online-Participatory-MCLE-Programs (last visited July 26, 2019).
12. *See Featured Online Technology CLE Packages*, State Bar of Tex., www.texasbar.com/AM/Template.cfm?Section=articles&ContentID=37468&Template=/CM/HTMLDisplay.cfm (last visited July 26, 2019).
13. N.Y. Cty. Lawyers Ass'n Prof'l Ethics Comm., Formal Op. 749 (2017).
14. *Id.*
15. *Id.*
16. Rosch, s*upra* note 5. "Overall, 83.4% of respondents indicated it was 'Very important' or 'Somewhat important' to receive training on their firm's technology. Those responding that it was 'Not very important" or 'Not at all important' were only 16.6%. Even though this is a relatively low percentage, it is still too high."
17. Steven M. Puiszis, A Lawyer's Duty of Technological Competence, at 4 (Am. Bar Ass'n 2017), www.americanbar.org/content/dam/aba/events/professional_responsibility/2017%20Meetings/Conference/conference_materials/session4_information_governance/puiszis_lawyers_duty_technological_competence.authcheckdam.pdf.
18. *Id.* at 1 (quoting Anthony E. Davis, *The Ethical Obligation to Be Technologically Competent*, N.Y.L.J. 3 (Jan. 8, 2016)).
19. Model Rules of Prof'l Conduct r. 1.6 cmt. 2 (Am. Bar Ass'n 2018).
20. Model Rules of Prof'l Conduct r. 1.6(a). Subsection (b) of the rule provides exceptions to the duty of confidentiality, allowing disclosure in seven specific and limited circumstances absent client consent, including, among other things, to prevent bodily harm or death, the crime-fraud exception, to secure legal advice about the attorney's compliance with the professional rules of conduct, or pursuant to court order or law. Model Rules of Prof'l Conduct r. 1.6(b).
21. *Id.* cmt. 3.
22. Model Rules of Prof'l Conduct r. 1.6(c); *see also Ethics 20/20 Proposal to Amend Rule 1.6 (Confidentiality of Information)*, Legal Ethics Forum (Feb. 27, 2012), www.legalethicsforum.com/blog/2012/02/ethics-2020-proposal-on-rule-16-confidentiality-of-information.html.
23. Comment 18 to Rule 1.6 explains that "[f]actors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or important piece of software excessively difficult to use)." *Id.* cmt. 18.

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

24. Sean Griffin, *Hacks, Files, and Ethical Gapes: Attorney's Liability for Data Breaches*, For the Defense 16 (Nov. 2016), www.dykema.com/media/site_files/128_Attorneys_%20Liability%20for%20Data%20Breaches%20--%20Sean%20C.%20Griffin.pdf.
25. *Id*. at 15–16; *see also* Melissa Maleske, *A Soft Target for Hacks, Law Firms Must Step Up Data Security*, Law360 (Sept. 23, 2015), www.law360.com/articles/706312/a-soft-target-for-hacks-law-firms-must-step-up-data-security; Daniel A. Cotter, *The Use of Technology by Lawyers and the Rules of Professional Conduct*, 30 CBA Rec. at 30, 31 (Sept. 2016) ("Attorneys and firms are increasingly the targets of hacking and phishing scams, and some law firms have been sued, facing allegations that the firms' data security practices were insufficient to protect confidential client information.").
26. Griffin, *supra* note 24, at 16.
27. Julie Sobowale, *Law Firms Must Manage Cybersecurity Risks*, ABA J. (Mar. 1, 2017), www.abajournal.com/magazine/article/managing_cybersecurity_risk.
28. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477 (2017). "Cybersecurity" is defined as measures taken to protect a computer or computer system against unauthorized access or attack. *Cybersecurity*, Merriam-Webster, www.merriam-webster.com/dictionary/cybersecurity (last visited July 26, 2019).
29. Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, Wall St. J. (Mar. 29, 2016), www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.
30. Jeff John Roberts, *Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear*, Fortune (June 29, 2017), http://fortune.com/2017/06/29/dla-piper-cyber-attack/.
31. Ben Rossen, *How to Defend Against Ransomware*, Fed. Trade Comm'n (Nov. 10, 2016), www.consumer.ftc.gov/blog/how-defend-against-ransomware.
32. Bastian Obermayer et al., *The Panama Papers: Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption*, Int'l Consortium of Investigative Journalists (Apr. 3, 2016), www.icij.org/investigations/panama-papers/20160403-panama-papers-global-overview/.
33. Griffin, *supra* note 24, at 18 ("Further, these breach notification requirements often require notice to law enforcement, civil or criminal penalties, and private causes of action."); *see also* Lorelai Laird, *Uber Ousts In-House Counsel Who Suppressed Information About 2016 Data Breach*, ABA J. (Nov. 22, 2017), www.abajournal.com/news/article/uber_ousts_in_house_counsel_who_suppressed_information_about_2016_data_brea; Brian Womack, *Yahoo Counsel Leaves After Hack Investigation Finds Lack of Action*, Bloomberg (Mar. 2017), www.bloomberg.com/news/articles/2017-03-01/yahoo-counsel-bell-leaves-after-hack-probe-finds-lack-of-action.
34. Roy Strom, *Chicago's Johnson & Bell First US Firm Publicly Named in Data Security Class Action*, Am. Laws. (Dec. 9, 2016), www.americanlawyer.com/id=1202774361560/Chicagos-Johnson--Bell-First-US-Firm-Publicly-Named-in-Data-Security-Class-Action?slreturn=20170419115647).
35. Griffin, *supra* note 24, at 18. Breach notification requirements typically require lawyers to notify law enforcement of the data breaches, exposing the firm to civil penalties and private actions.

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

36. Julie Sobowale, *Law Firms Must Manage Cybersecurity Risks*, ABA J. (Mar. 1, 2017), www.abajournal.com/magazine/article/managing_cybersecurity_risk.
37. *Id.*
38. Jeff John Roberts, *Exclusive: China Stole Data from Major U.S. Law Firms*, FORTUNE (Dec. 7, 2016), http://fortune.com/2016/12/07/china-law-firms/.
39. "Spear-phishing" is the practice of sending fraudulent e-mails to extract financial data from computer users for the purposes of identity theft, by mimicking a sender the recipient knows. *Spear-phishing*, DICTIONARY.COM, www.dictionary.com/browse/spear-phishing?s=t (last visited July 26, 2019).
40. Roberts, *supra* note 38.
41. Mark Rosch, *2016 Technology Training*, ABA (Dec. 1, 2016), www.americanbar.org/groups/law_practice/publications/techreport/2016/training.html. Survey respondents who were solo practitioners or practiced in firms of two to nine lawyers were also more likely to respond that it was "not very important" to receive training on their firm's technology, and less likely to respond that it was "very important" or "somewhat important." *Id.*
42. *Id.*
43. Ries, *supra* note 4. Revised Resolution 109 on cybersecurity adopted at the ABA Annual Meeting in August 2014 is applicable to all private and public sector organizations, which includes law firms. AM. BAR ASS'N CYBERSECURITY LEGAL TASK FORCE, REPORT TO HOUSE OF DELEGATES: REVISED RESOLUTION 109 (Aug. 2014), www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf.
44. Two-factor authentication works by sending an access code to a secondary device and then requiring the user to then enter the code into the first device to get access to the account. Typically, the hacker does not have access to the secondary device and cannot get access to the account even after stealing the user's credentials. Law firms should enable two-factor authentication for access to its servers or other systems that contain confidential client information. *See* Jeff John Roberts, *Most People Aren't Using This Critical Web Security Feature*, FORTUNE (Nov. 7, 2017), http://fortune.com/2017/11/07/cybersecurity-2fa-two-factor-authentication/.
45. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477, *supra* note 28.
46. Daniella Isaacson, *The State of Cybersecurity in the Legal Industry: Are Things Improving?*, LAW.COM (Dec. 10, 2017), www.law.com/sites/ali/2017/12/10/the-state-of-cybersecurity-in-the-legal-industry-are-things-improving/.
47. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018).
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*

55. Tom Kulik, *IP, Legal Ethics and the Cloud: 3 Things to Consider Regarding Client Confidential Information*, Above the Law (Nov. 6, 2017), https://Abovethelaw.com/2017/11/ip-legal-ethics-and-the-cloud-3-things-to-consider-regarding-client-confidential-information/.
56. *Id.*
57. *Inadvertent Disclosure of Confidential Information: File Sharing and Privilege Waiver*, Jenkins Fenstermaker, PLLC (Feb. 27, 2018), www.jenkinsfenstermaker.com/blog/2018/02/inadvertent-disclosure-of-confidential-information.shtml.
58. *See* Dennis Kennedy, *2018 Cloud Computing*, ABA (Jan. 14, 2019), www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cloud/; *see also* Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011).
59. Chad Burton, *2017 Virtual Law Practice*, Am. Bar Ass'n (Dec. 1, 2017), www.americanbar.org/groups/law_practice/publications/techreport/2017/virtual_law_practice.html.
60. Kulik, *supra* note 55.
61. Citrix, *The Ethics of File Sharing for Attorneys*; Law Practice Today (Aug. 14, 2015), www.lawpracticetoday.org/article/the-ethics-of-file-sharing-for-attorneys/.
62. Encryption is the practice of converting information or data into code, especially to prevent unauthorized access. *Encryption*, Dictionary.com, www.dictionary.com/browse/encryption (last visited July 26, 2019); *see also* Kulik, *supra* note 55.
63. Dan Pinnington & Ian Hu, *2017 Practice Management*, Am. Bar Ass'n (Dec. 1, 2017), www.americanbar.org/groups/law_practice/publications/techreport/2017/practice_management.html.
64. For example, states permit the use of file-sharing services so long as attorneys exercise reasonable care when doing so. *See* N.Y. State Bar Ass'n, Op. 842 (2010) ("A lawyer may use an online data storage system . . . provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with a lawyer's obligations under Rule 1.6."); State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010) (attorneys must take reasonable precautions when using technology that may be susceptible to unauthorized access by third party); Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011) ("An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes *reasonable* care to assure that (1) all such materials remain confidential, and (2) *reasonable* safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.") (emphasis added).
65. Fla. Bar Ass'n, Op. 12-3 (2013); *see also* Fla. Bar Ass'n, Op. 10-2 (2010); Fla. Bar Ass'n, Op. 07-2 (2008); Ala. State Bar Office of Gen. Counsel, Formal Op. 2010-02 (2010); State Bar of Ariz. Ethics Comm., Op. 09-04 (2009); Iowa State Bar Ass'n Comm. on Ethics and Practice Guidelines, Op. 11-01 (2011); N.Y. State Bar Ass'n Comm. on Prof'l Ethic, Op. 842 (2010); Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011).
66. Nicole Black, *The Ethics of Cloud Computing for Lawyers*, ABA (Sept. 1, 2012), www.americanbar.org/groups/gpsolo/publications/gpsolo_ereport/2012/september_2012/ethics_cloud_computing_lawyers/; *see also* Jason M. Rosenthal, *Keeping Your Data,*

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

Not Your Head, in the Cloud (Nov. 22, 2013), http://apps.americanbar.org/litigation/committees/insurance/articles/112213-data-cloud-discovery.html.

67. Prof'l Ethics Comm. for State Bar of TX, Opinion No. 680 (2018).
68. *Id.*
69. Pinnington & Hu, *supra* note 63 ("Almost 100% of attorneys have embraced email in their practice.").
70. Model Rules of Prof'l Conduct r. 1.4.
71. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477, *supra* note 28.
72. *See id.*
73. *Email Encryption in Office 365*, Microsoft (Oct. 29, 2018), https://support.office.com/en-us/article/email-encryption-in-office-365-c0d87cbe-6d65-4c03-88ad-5216ea5564e8; *see also* David Ries, *Encryption Made Simple for Lawyers*, 29 GPSolo Nov./Dec. 2012: Privacy & Confidentiality (Nov. 1, 2012), www.americanbar.org/groups/gpsolo/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers/ (membership required).
74. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477, *supra* note 28.
75. *Manage Suggested Recipients in the To, Cc, and Bcc Boxes with Auto-Complete*, Microsoft, https://support.office.com/en-us/article/manage-suggested-recipients-in-the-to-cc-and-bcc-boxes-with-auto-complete-dbe46e31-c098-4881-8cf7-66b037bce23e (last visited July 27, 2019).
76. *See Enhanced Security Infrastructure*, Egress, www.egress.com/en-US/what-we-offer/infrastructure-services (last visited July 27, 2019) ("Egress technology can be used to monitor data sharing patterns to understand who staff email and stop them sending emails to incorrect recipients.").
77. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006). Some word processing programs allow users, when they review and edit a document, to "redline" the changes they make in the document to identify what they added and deleted. The redlined changes might be readily visible, or they might be hidden, but even in the latter case, they often will be revealed simply by clicking on a software icon in the program. Similarly, some programs also allow users to embed comments in a document. The comments may or may not be flagged in some manner, and they may or may not "pop up" as a cursor is moved over their locations.
78. *Id.*
79. Model Rules of Prof'l Conduct r. 4.4(b). Although the ABA does not currently prohibit attorneys mining for metadata, several states have extended the reach of Model Rule 4.4(b) to include a prohibition of data mining techniques by recipient attorneys on documents received during discovery to obtain additional information. *See* State Bar of Ariz. Ethics Comm., Op. 07-03 (2007); Fla. Bar Ass'n, Ethics Op. 06-02 (2006); N.H. Bar Ass'n Ethics Comm., Op. 2008-09/4 (2008); N.C. State Bar Ethics Comm., 2009 Formal Ethics Op. 1 (2010); D.C. Bar Legal Ethics Comm., Op. 341 (2007); W. Va. Rules of Prof'l Conduct r. 4.4 cmt. 2. New York and Mississippi prohibit mining for metadata under Model Rule 8.4(c) and (d), which prohibits engaging in conduct "involving dishonesty, fraud, deceit, or misrepresentation." *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749 (2001);

Miss. Bar Ethics Comm., Op. 259 (2012); *see also* Ala. State Bar Office of Gen. Counsel, Formal Op. 2007-02 (2007) ("this opinion is consistent with Formal Opinion[ ] 749 . . . of the New York State Bar."); Me. Bd. of Overseers of Bar Prof'l Ethics Comm., Op. 196 (2008) ("[F]ollowing the general analysis of New York . . . we find that an attorney may not ethically take steps to uncover metadata.").

80. Ill. State Bar Ass'n Bd. of Governors, Op. 98-04 (1999).
81. Nicole Hong & Robin Sidel, *Hackers Breach Law Firms Including Cravath and Weil Gotshal*, Wall St. J. (Mar. 29, 2016), www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.
82. *Id.*
83. Legal Servs. Info. Sharing & Analysis Org. (LS-ISAO), https://grfederation.org/ls-isao (last visited July 27, 2019).
84. *Social Networking*, Oxford Learner's Dictionary, www.oxfordlearnersdictionaries.com/us/definition/english/social-networking?q=social+networking (last visited July 27, 2019). "Social networking" is the use of websites that enable users to interact with one another, find and contact people with common interests or connections. Social networking sites such as Facebook or LinkedIn, among others, allow users to establish a "profile" through which they interact and share updates, photos, commentary, and life events with other users in their networks.
85. Allison Shields, *2017 Social Media and Blogging*, ABA (Dec. 1, 2017), www.americanbar.org/groups/law_practice/publications/techreport/2017/social_media_blogging.html; *see also* Attorney at Work, 2017 Social Media Marketing Survey Report (2017) (reporting similar trends and usage of social media among lawyers), www.attorneyatwork.com/wp-content/uploads/2017/03/2017-Social-Media-Marketing-Survey-Report-@-AttorneyatWork.pdf (last visited June 20, 2019).
86. "LinkedIn is still the leading social network for lawyers, although its use seems to have declined a bit recently. According to the *2017 Survey*, 53% of respondents report LinkedIn use by their firms. Solos this year also reported a 53% rate of LinkedIn use by their firms. Close to half of lawyers in firms of less than 50 lawyers report that their firms use LinkedIn, and firms of 100+ continue to have the largest firm presence on LinkedIn, between 63–73%." Shields, *supra* note 85. Facebook is the second most popular social network, with Twitter a distant third. *Id.*
87. *Id.*; *see also* Nielsen, 2016 Nielsen Social Media Report 8 (2017) ("Social Media gives marketers the chance to reach out directly to consumers, amplify their messages and pitch their best value proposition to their best consumers wherever they may be – basement, bedrooms, or bars."). *See generally* Manu Mathew, *How to Reach, Engage and Measure Today's Empowered Consumer*, Nielsen (May 31, 2018), www.nielsen.com/us/en/insights/news/2018/perspectives-how-to-reach-engage-todays-empowered-consumer.html ("These techniques allow marketers to target consumers more precisely with more personalized, relevant information than ever before.").
88. For example, the Oregon Supreme Court found that an attorney engaged in "dishonesty" when he impersonated a former classmate who was then a teacher. Posing as the teacher, the attorney created a *Classmates.com* page in the teacher's name and posted messages implying

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

that the teacher had had sexual relations with students. *In re* Complaint as to Conduct of Carpenter, 95 P.3d 203, 205–06 (Or. 2004). The court issued a public reprimand, holding that ethical conduct rules are designed to protect "the public's interest in the integrity and trustworthiness of lawyers." *Id.*; *see also* Shane Witnov, *Investigating Facebook: The Ethics of Using Social Media Websites in Legal Investigations*, 28 Santa Clara High Tech. L.J. 31, 43–45 (2011).

89. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 480 (2018).
90. *Id.*
91. As discussed above, Model Rule 1.6 requires attorneys to protect against the inadvertent disclosure of confidential information of clients. Model Rule 1.9(c)(2) prevents attorneys from revealing information about their representation of former clients, and Model Rule 1.18(b) prevents lawyers from revealing confidential information they may learn from prospective clients, even when no attorney-client relationship ensues.
92. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 480, *supra* note 89; *see also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 10-457 (2010) ("Specific information that identifies current or former clients or the scope of their matters . . . may be disclosed, as long as the clients or former clients give informed consent . . ."). "Website disclosure of client identifying information is not normally impliedly authorized because the disclosure is not being made to carry out the representation of a client, but to promote the lawyer or the law firm." *Id.*
93. *Id.* There is some conflict among jurisdictions on whether the disclosure of publicly available information constitutes a violation of the lawyer's confidentiality obligations. Several jurisdictions have held that a lawyer must maintain the confidentiality of information learned through representation even if it is otherwise publicly available, such as through public court filings or other public record: *In re* Anonymous, 932 N.E.2d 671 (Ind. 2010); Iowa S. Ct. Attorney Disciplinary Bd. v. Marzen, 779 N.W.2d 757 (Iowa 2010); State Bar of Ariz., Op. 00-11 (2000); Colo. Bar Ass'n, Formal Op. 130 (2017). However, Louisiana and Virginia have held that disclosure of publicly filed information did not violate Rule 1.6. *In re* Sellers, 699 So. 2d 1204 (La. 1996) (disclosure of collateral mortgage to third party did not violate Rule 1.6 because mortgage was matter of public record); Hunter v. Va. State Bar, 744 S.E.2d 611 (Va. 2013) (Rule 1.6 did not prohibit attorney from posting information revealed in completed criminal trials of former clients).
94. The ABA Standing Committee on Ethics and Professional Responsibility has taken the position that Rule 1.6 prohibits the disclosure of a client's identity without consent (or one of the exceptions in 1.6(b)). *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 480, *supra* note 89 (citing opinions issued from Arizona, Wisconsin, Nevada, and New York stating that a client's identify is protected under Rule 1.6). The California bar, however, has held that in most situations "the identity of a client is not considered confidential" and, depending on the circumstances, may be disclosed without consent. State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2011-182 (2011).
95. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 480, *supra* note 90.
96. *In re* Disciplinary Proceedings Against Kristine Ann Peshek, 798 N.W.2d 879 (Wis. 2011).
97. *Id.*

98. *Id.* The Supreme Court of Wisconsin imposed reciprocal sanctions for the attorney's conduct, a sixty-day suspension, quoting extensively from the materials and information filed in the Illinois proceeding. *See* Office of Lawyer Regulation v. Peshek, 798 N.W.2d 879 (Wis. 2011). In addition to a violation of Rule 1.6, the Illinois attorney admitted "conduct which tends to defeat the administration of justice or bring the courts or the legal profession into disrepute," and, for failing to inform the court of a client's misstatement of fact to the court, violations of Illinois Rules of Professional Conduct, Rules 1.2(g), 3.3(a)(2), and 8.4(a)(4), (5). *Id.*
99. *In re* Skinner, 740 S.E.2d 171 (Ga. 2013).
100. Martha Neil, *Lawyer Puts Photo of Client's Leopard-Print Undies on Facebook; Murder Mistrial, Loss of Job Result*, ABA J. (Sept. 13, 2012), www.abajournal.com/news/article/lawyer_puts_photo_of_clients_leopard-print_undies_on_facebook_murder_mistri.
101. *Mocking Lawyer Posts Photo of Her Client's Leopard Print Underwear on Facebook Causing Mistrial in Murder Case*, Daily Mail (Sept. 13, 2012), www.dailymail.co.uk/news/article-2202778/Lawyer-posts-photo-clients-leopard-print-underwear-Facebook-causing-mistrial-murder-case.html.
102. Ill. State Bar Ass'n Comm. on Rules of Prof'l Conduct, Op. 12-15 (2012).
103. *See, e.g.*, State Bar of Ariz., Op. 97-04 (1997) (attorneys cannot mention on website or in "chat room" that he or she specializes in an area of practice that is not recognized by Arizona's Board of Legal Education). In an ethics advisory opinion, the South Carolina Bar concluded that lawyers could participate on free websites that provide information about attorneys nationwide, claim their profiles, and even invite peers, clients, and former clients to rate them. S.C. Bar Ethics Advisory Comm., Op. 09-10 (2009). However, the South Carolina Bar warned that all such endorsements, ratings, and content "claimed" by a lawyer are governed by the Rules of Professional Conduct, and the lawyer is responsible for the content. *Id.*
104. Model Rules of Prof'l Conduct r. 7.1 (Communication Concerning a Lawyer's Services).
105. Model Rules of Prof'l Conduct r. 1.8(a). The comments to the rule suggest that "consultation" is beyond a casual contact due to a posting or blog:

> Whether communications, including written, oral or electronic communications, constitute a consultation depends on the circumstances. For example, a consultation is likely to have occurred if a lawyer, either in person or through the lawyer's advertising in any medium, specifically requests or invites the submission of information about a potential representation without clear and reasonably understandable warnings and cautionary statements that limit the lawyer's obligations . . . In contrast, a consultation does not occur if a person provides information to a lawyer in response to advertising that merely describes the lawyer's education, experience, areas of practice, and contact information, or provides legal information of general interest.

Id., cmt 2. It is necessary to consult with each state's rules of professional practice. In Florida, for example, the Florida Bar's Standing Committee on Advertising issued guidelines for use of social media, including, among other things, Guidelines for Networking Sites

Teresa J. Verges & Christine Lazaro, Technology in Legal Practice: Keeping Ethical Obligations in Mind, 3 PLI Current No. 3 (Summer 2019).

and Guidelines for Video Sharing Sites. The committee made a distinction between purely personal pages used solely to maintain social contact with family and friends, and those used to promote the lawyer or law firm's practice, which are subject to lawyer advertising rules. Fla. Bar Standing Comm. on Advert., *Guidelines for Networking Sites, in* Handbook on Lawyer Advertising and Solicitation 120–21 (11th ed. 2018). Similarly, the Florida Bar distinguished between personal videos and those sent on an unsolicited basis for the purpose of obtaining legal business. *Id.*

106. Model Rules of Prof'l Conduct r. 7.2 cmt. 5 (Am. Bar Ass'n 2018).
107. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 480, *supra* note 89.
108. *Id.* at 1 n.4.
109. *See* N.Y. State Bar Ass'n, Social Media Ethics Guidelines (June 20, 2019), www.nysba.org/socialmediaguidelines17/.
110. *Id.*
111. *Id.*, Guideline No. 4.A. The permission is premised on the idea that a user does not have an expectation of privacy with respect to public portions of social media accounts.
112. *Id.*, Guideline No. 4.B. In New York, the lawyer need not provide a reason for the "friend" request so long as the lawyer uses his or her real name and profile. However, New York goes on to note that other jurisdictions do require that the lawyer also provide additional information as part of the request to fully apprise the person of the lawyer's role and intentions. For example, the New Hampshire Bar Association holds that an attorney must "inform the witness of the lawyer's involvement in the disputed or litigated matter," the disclosure of the "lawyer by name as a lawyer" and the identification of "the client and the matter in litigation." N.H. Bar Ass'n Ethics Advisory Comm., Op. 2012-13/05 (2012). The Massachusetts and San Diego Bar Associations simply require disclosure of the lawyer's "affiliation and the purpose for the request." Massachusetts Bar Ass'n Comm. on Prof Ethics, Op. 2014-5 (2014); San Diego County Bar Ass'n Legal Ethics Comm., Op. 2011-2 (2011); *see also* Tom Gantert, *Facebook "Friending" Can Have Ethical Implications*, LegalNews (Sept. 27, 2012). The Philadelphia Bar Association notes that failure to disclose the attorney's true intention constitutes an impermissible omission of a "highly material fact." Phila. Bar Ass'n Prof'l Guidance Comm., Op. Bar 2009-2 (2009). *Id.*, cmt.
113. *Id.*, Guideline No. 4.C.
114. *Id.*, Guideline No. 4.D; *see also* Model Rules of Prof'l Conduct r. 5.3 and r. 8.4 (Am. Bar Ass'n 2018).
115. N.Y. Cty. Lawyers Ass'n Prof'l Ethics Comm., Formal Op. 750 (2018).
116. *Id.*