By Elizabeth B. Vandesteeg

Technology and Legal Ethics: A User's Manual (Part I)

Editor's Note: *This new column addresses the wide-ranging issues of data security and privacy fundamentals, including ethical considerations, for the restructuring professional. Those interested in contributing for this column should contact Ms. Vandesteeg at evandesteeg@sfgh.com.*

Coordinating Editor Elizabeth B. Vandesteeg
Sugar Felsenthal Grais & Helsinger, LLP Chicago

Lisa Vandesteeg is chair of the Litigation and Dispute Resolution Group of Sugar Felsenthal Grais & Helsinger LLP in Chicago. Her practice includes bankruptcy, commercial litigation, business disputes and privacy and data-security issues. She is a Certified Information Privacy Professional for the U.S. Private Sector, as qualified by the International Association of Privacy Professionals. A 2017 ABI "40 Under 40" honoree, she serves as an associate editor for the ABI Journal.

Once upon a time, certain attorneys embraced the view that being a Luddite[1] was a point of pride; they had practiced in paper for decades, and new-fangled technology was unnecessary to provide top-notch service to their clients. This worldview has ever-decreasing adherents, as technology has reached into nearly every facet of the practice of law. Not only is facility with technology a practical business requirement to adequately serve clients, it is now also an ethical requirement imposed upon attorneys in most states. Standard rules of professional conduct mandate that attorneys both take reasonable steps to keep the client data that they hold secure and provide notice to clients should there be an unauthorized disclosure of such data.

For bankruptcy attorneys, the implications of these standards are particularly far-reaching. While commercial litigators and their transactional counterparts might be privy to confidential data, it is likely that such information will be discrete and related solely to the dispute or deal at issue. There will be only a few parties involved, and the process will not require public disclosures beyond limited public filings.

On the other hand, bankruptcy is a process that requires comprehensive disclosures and involves numerous parties. Bankruptcy attorneys, particularly those representing corporate debtors, might find themselves responsible for an entire company's data, including all financial, proprietary and employee information. They must understand the types of potentially sensitive information in their possession and the proper ways to safeguard it from unauthorized access or disclosure.

This article is the first in a two-part series discussing the fundamentals of the intersection of cybersecurity and ethics for bankruptcy attorneys. This article discusses the key ethical rules in the realm of technology and data security. The second article, which will appear in a later issue, will provide guidance as to the best practices with respect to securing and transferring client data as part of information-security programs for law firms, as well as the necessary steps that law firms must take to notify clients in the event of a data breach and loss of client information.

Technological Competence: The Cornerstone of Cyber Ethics

Any attorney's first and most important ethical duty to clients is to provide competent legal representation. Model Rule 1.1 of the American Bar Association's (ABA) Model Rules of Professional Conduct[2] requires that such "competent representation" to a client include the requisite legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[3]

An attorney's ability to provide that competent representation includes a requirement of technological facility. Specifically, Comment 8 to Model Rule 1.1 requires an attorney to keep abreast of "the benefits and risks associated with relevant technology."[4] With this addition, the Model Rule's definition of "competency" now mandates that attorneys maintain both a substantive knowledge of law *and* proficient skills with the ever-evolving technology available to attorneys and clients.

In the seven years since the ABA adopted Comment 8 to Model Rule 1.1, 38 states have included similar requirements in their ethical rules.[5] For attorneys, achieving and maintaining a certain level of technological proficiency is simply no longer optional.[6]

What to Do?

Technology invades nearly every province of legal practice — from the use of timekeeping and

1 A "Luddite" is defined as someone "who is opposed to especially technological change." *Merriam-Webster Dictionary*, *available at* merriam-webster.com/dictionary/Luddite (last visited Jan. 7, 2020).

2 The ABA Model Rules of Professional Conduct were adopted by the ABA House of Delegates in 1983 and serve as models for the ethics rules of most U.S. jurisdictions. Some variation has been adopted by all 50 states.

3 Model Rules of Prof'l Conduct R. 1.1 (2019).

4 Model Rules of Prof'l Conduct R. 1.1, cmt. 8 (2019) (adopted in 2012).

5 At the time of this article, 11 states have yet to enact versions of Comment 8 in their rules of professional responsibility or otherwise recognize the technological competence duty: Alabama, Alaska, Georgia, Hawaii, Maine, Maryland, Mississippi, Nevada, New Jersey, Oregon and South Dakota. While one of the remaining states, California, has not formally adopted the change to its rules of professional conduct, it has issued an ethics opinion expressly acknowledging the technological competence duty in the context of e-discovery in litigation. State Bar of Calif. Standing Comm. Prof'l Responsibility and Conduct Formal Op. No. 2015-109 (2015).

6 At least two states, Florida and North Carolina, now mandate not only technological competence, but also technology training as part of their continuing legal education programs.

continued on page 49

from page 12

billing software to the redaction required of e-filers to e-discovery, and from vetting vendors for security compliance to training staff and attorneys on recognizing security risks. The complex relationship between new technological opportunities and the accompanying risks can create a confusing landscape for attorneys.

For example, the use of third-party service providers, such as cloud-based document-management and storage companies, might benefit an attorney in the form of increased efficiency in moving away from paper records. However, that attorney must monitor how those service providers secure and store client data. The widespread availability of public wireless networks also provides attorneys with the chance to check email and perform work remotely from nearly any location, but such networks also bring heightened risk of exposing client data to bad actors who monitor and intercept internet traffic on those networks.

How, then, do attorneys comply with this requirement for technological competence? "Competence" in technology cannot be satisfied by merely hiring qualified IT personnel and considering the matter solved. The Model Rules make it clear that attorneys must educate themselves on both the risks and benefits of technology, either through self-study (*e.g.*, by attending continuing legal education seminars, such as those offered at ABI conferences), associating with knowledgeable individuals in their law practice, or otherwise receiving training on relevant technology.[7]

Attorneys must know enough about the new technology they use to perform legal services to ensure that they are compliant with their professional responsibilities to keep client information confidential and secure. An attorney using new technology without learning how to operate it safely is running afoul of the fundamental ethical obligations.

Confidentiality: Lock It Up

While technology may have changed the means by which attorneys maintain and transmit sensitive information, the duty of confidentiality remains unchanged. Model Rule 1.6 prohibits an attorney from revealing "information relating to the representation of a client" unless such client gives informed consent, or the disclosure is "impliedly authorized" or otherwise permitted.

Attorneys are ethically required to make "reasonable efforts" to prevent inadvertent or unauthorized disclosure of — or unauthorized access to — information relating to the representation of a client (or former client).[8] Attorneys can take some comfort in knowing that the Model Rules provide that unauthorized access or inadvertent disclosure of client information "does not constitute a violation of paragraph (c) [of Model Rule 1.6] if the lawyer has made reasonable efforts to prevent the access or disclosure."[9]

In typical lawyerly fashion, the "reasonable efforts" standard is a fuzzy one, and the determination of whether efforts are indeed reasonable is a fact-specific inquiry. Relevant factors include the sensitivity of the information, the risk of disclosure without additional precautions, the cost of extra measures, the difficulty of adding safeguards, and whether more safeguards adversely affect the lawyer's ability to represent the client.[10]

The onus is also on an attorney to analyze and determine any appropriate safeguards regarding the transmission of confidential information. The Model Rules specify that this does not necessarily require the use of special security measures (such as encrypting every email), but prompt lawyers to consider whether special security measures are warranted with respect to particularly sensitive information or material protected by law or confidentiality agreements.[11]

Attorneys must train themselves, their employees and their vendors in the use of reasonable, situation-specific safeguards for client data and other sensitive information.

What to Do?

The "reasonable efforts" standard requires an informed and delicate balancing act. Attorneys must implement strong data-security practices in order to safeguard client data and comply with ethical responsibilities. However, at the same time, attorneys must take into account both the actual cost of additional security measures (technological or otherwise), and also the potential adverse impact of such security on the lawyer's ability to practice law. For example, while requiring encryption of every document in a firm's database might make the data extremely secure, it would also create a practical inability for attorneys to efficiently perform work.

This standard requires attorneys to be well-versed enough in technological matters to appropriately assess what security measures are sufficient and when. For example, "reasonable efforts" for an attorney dealing with an individual client's personal or financial data may involve encrypting any email providing that information to another recipient or arranging for an alternative means of secure transmission. For example, an attorney representing a corporation seeking to sell its assets pursuant to § 363 of the Bankruptcy Code should perform due diligence on the cloud-based document-hosting service that might be used as the data room to confirm that it has sufficient security safeguards in place. Attorneys must also be aware of and avoid common and well-known data

7 Model Rules of Prof'l Conduct R. 1.1, cmts. 1, 6, 8 (2019). *See, e.g., James v. Nat'l Fin. LLC*, No. 8931-VCL, 2014 WL 6845560 (Del. Ch. Dec. 5, 2014) (discussing competence as requirement of Pennsylvania and Delaware rules of professional conduct in the context of e-discovery violations).

8 Model Rules of Prof'l Conduct R.1.6(c) and cmt. 20 (2019) (adopted in 2012).

9 Model Rules of Prof'l Conduct R. 1.6, cmt. 18 (2019).

10 *Id. See, e.g.*, State Bar of Ariz. Ethics Op. 09-04 (2009) (discussing standards for electronic access to client files).

11 Model Rules of Prof'l Conduct R. 1.6, cmt. 19 (2019).

continued on page 50

from page 49

security risks, such as the use of unsecured wireless networks in coffee shops and airports, and instead use a secured wireless network to communicate with clients.

Supervisory Responsibilities

Attorneys are required to not only be competent in their own legal practice but also be responsible for the actions taken by those under their supervision.

Junior Attorneys

Partners and other supervisory attorneys are required to "make reasonable efforts" to ensure that the firm has in effect measures "giving reasonable assurance" that all lawyers in the firm conform to the ethical rules. A supervising attorney must also make "reasonable efforts" to ensure that junior lawyers adhere to the ethical rules.[12]

When considering those responsibilities in the context of technology and data security, senior attorneys must instruct junior attorneys on the responsibility to safeguard client data. Supervisory attorneys must provide training (ideally as part of and in compliance with a holistic information-security program) on critical security issues, including using care when emailing recipients outside the firm; avoiding the use of public unsecured wireless networks; and properly securing devices containing client data such as mobile phones, tablets and laptops. Partners cannot turn a blind eye when they see junior lawyers failing to take such precautions, or they risk ethical violations themselves.

Nonlawyer Employees and Vendors

Similarly, lawyers are responsible for overseeing nonlawyers employed or retained by, or associated with, a lawyer. This rule contemplates the oversight responsibilities triggered by an attorney's use of both nonlawyer employees within a firm and service providers outside the firm, and requires an attorney to take "reasonable efforts" (there is that fuzzy standard again!) to ensure that services are provided in a manner that is compatible with the lawyer's professional obligations.[13]

Law firms regularly employ nonlawyers, including paralegals, secretaries or law clerks. A lawyer must give such assistants "appropriate instruction and supervision" concerning the ethical aspects of their employment, "particularly regarding the obligation not to disclose information relating to the representation of a client."[14]

Attorneys also frequently make use of external vendors in legal practice, such as investigators, expert witnesses, e-discovery vendors and cloud-based services for hosting firm and client data. For bankruptcy practitioners, this might also include third parties such as claims and noticing agents.

What to Do?

What do these supervisory responsibilities require on a practical level? Read in tandem with the competence required of Model Rule 1.1 and the need to safeguard client confidences in Model Rule 1.6, these supervisory responsibilities require attorneys to know enough about technology and data security to appropriately hire and supervise junior attorneys, nonlawyers and service providers.

An attorney may not simply hire any vendor they hear about without first investigating that vendor's particular data-security practices and confirming that the vendor stores and transmits any data it handles in a manner that is compatible with that attorney's professional obligations. "Reasonable efforts" to ensure that an external vendor is performing its work in a manner compatible with the lawyer's professional obligations should include consideration of such factors as "the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality."[15]

Similarly, there is no way for an attorney to avoid ethical responsibilities by blaming a breach on an assistant who may have clicked on a bad email link or responded to a fraudulent request for a wire transfer. Attorneys, particularly supervisory attorneys such as partners, should implement an information-security program to ensure that proper supervision and standards are in place in order to comply with ethical responsibilities. An attorney should also provide training to staff members in areas such as email security awareness, proper procedures for sending and receiving wire transfers, procedures for storing and destroying client documents and data, and protocols for sending client data outside the firm.

Conclusion

Technological competence and appropriate data-security measures are no longer a problem that can be outsourced to IT. Attorneys must train themselves, their employees and their vendors in the use of reasonable, situation-specific safeguards for client data and other sensitive information. This is not only a prudent business move, but it is also required by ethical rules in most states. With proper training and oversight, attorneys can comply with these ethical rules and ensure the security of client data. abi

12 Model Rules of Prof'l Conduct R. 5.1 (2019).
13 Model Rules of Prof'l Conduct R. 5.3 (2019).
14 Model Rules of Prof'l Conduct R. 5.3, cmt. 2 (2019).
15 Model Rules of Prof'l Conduct R. 5.3, cmt. 3 (2019). *See, e.g.*, Ill. State Bar Assoc. Advisory Op. No. 16-06 (2016) (discussing "reasonable efforts" to employ when selecting and hiring cloud computing vendor).