Published in the 2018 January/February issue of the *Hennepin Lawyer*, a membership publication of the Hennepin County Bar Association. Used with permission. 612-752-6000 thl@hcba.org

Technological Literacy: The New Normal for Legal Practice

By Bryan R. Feldhaus

Minnesota's Rules of Professional Conduct impose various professional obligations upon the conduct of a lawyer, such as the duties of competency and confidentiality. Those duties have historically required a lawyer to maintain the requisite legal knowledge and skill to represent a client, and to protect that client's confidential documents from disclosure.

Now, however, neither knowledge of the law nor the protection of privileged documents is sufficient to satisfy a lawyer's professional obligations under the Minnesota Rules of Professional Conduct. Instead, the Rules of Professional Conduct, which were amended in 2015 to account for the increased use of technology in legal practice, now require a lawyer to maintain technological literacy in legal practice. Such technological literacy is critical because lawyers are attractive, and increasingly frequent, targets, of cyber criminals.

To develop technological literacy, a lawyer is required to know, understand, and assess the benefits and burdens of utilizing legal technology in an attorney-client relationship, and to discuss those benefits and burdens with clients. This article examines the importance of technological literacy in legal practice based on cybersecurity trends, and analyzes the ways in which a lawyer can satisfy his or her obligation to become technologically literate.

I. Cybersecurity Trends and Legal Practice

2016 was a watershed year for cybersecurity and legal practice. The year opened with warnings from the FBI and U.S. Attorney for the Southern District of New York about cyber threats to law firms, saw multiple and varied cyber attacks on law firms, and concluded with the American Bar Association's 2016 Legal Technology Survey, which confirmed that all lawyers, regardless of firm size, must implement reasonable measures to protect electronic client information.

For example, in its survey, the ABA reported that although 26 percent of law firms with more than 500 attorneys experienced a cybersecurity breach in 2016, 25 percent of firms with 10 to 49 attorneys also experienced a breach. Further, the breach incidence rate for solo practitioners increased by 5 percent in 2016. Thus, the survey confirms there is little, if any, distinction between firm size and cybersecurity. Cyber threats affect all lawyers who are, and will remain, attractive targets for cyber criminals.

II. Assessing Data Risk in Legal Practice

Lawyers are attractive targets for cyber criminals for three primary reasons. First, lawyers frequently utilize case management, litigation, or other software as repositories for confidential and commercially valuable client information. Lawyers then use those repositories to store protected health information, business or financial records, and trade secret information, most of which is commercially valuable. Additionally, the manner in which lawyers store such information is generally less voluminous and more organized than the manner in which a client stores the same information, which makes a lawyer an even more attractive target.

Second, lawyers regularly transmit or store confidential client information via email, file transfer, or cloud computing software, and multiple devices. A lawyer's frequent use and transmission of confidential and commercially valuable information, across multiple platforms, increases the complexity associated with protecting such information, particularly when third parties are also involved in the chain of custody.

Finally, many lawyers have neither taken the time to assess how technology may jeopardize client confidentiality nor implemented appropriate procedures or security measures to protect against the risks of an inadvertent disclosure or unauthorized access. For example, in the 2016 Legal Technology Survey, approximately 30 percent of respondents either did not know whether they had any cybersecurity policies in place or did not have any cybersecurity policies in place. Presumably an even larger percentage of respondents have not conducted a cybersecurity audit to assess the effectiveness

of their cybersecurity protocols. Thus, many lawyers have failed to develop any technological literacy.

III. Technological Literacy in Legal Practice

To become technologically literate and mitigate against cybersecurity risks, lawyers must evaluate how they obtain, manage, and store confidential client information when utilizing technology in their legal practice. This obligation is now mandated by the Minnesota Rules of Professional Conduct, which were amended on April 1, 2015, to reflect the increasing influence of technology on legal practice.

A. Competency

Minn. R. Prof. Conduct 1.1 obligates a lawyer to provide competent representation to a client, which requires a lawyer to possess the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation. In the context of cybersecurity, Rule 1.1 requires lawyers to evaluate and understand the benefits and burdens of legal technology in their client representation.

For example, in 2015, Comment 8 to Rule 1.1 was amended to include the phrase "including the benefits and risks associated with relevant technology." Minn. R. Prof. Conduct 1.1, Cmt. [8]. As a result of that amendment, Rule 1.1 now requires a lawyer to understand how technology can help and harm a client representation.

This competency obligation was previously articulated by Mr. Joshua Brand, Senior Associate Director at the Office of Lawyers Professional Responsibility: "As an initial matter, an attorney must have at least a base-level comprehension of the technology and the implications of its use. While no attorney is required to know precisely how cutting-edge technology truly works or be a computer genius, the competence requirements of the Rules necessitate at least a cursory understanding of any technology used if for no other reason than to enable an attorney to effectively communicate to a client the pros and cons of its use in the representation." Brand, "The Ethics of Cloud Storage," Minn. Lawyer, Dec. 30, 2011.

Although Mr. Brand's article was written to discuss the ethics of cloud storage services, such as Dropbox or Google Drive, his comments illustrate the technological literacy that a lawyer must possess to satisfy the competency requirement of Rule 1.1. An attorney must be able to effectively communicate to a client the pros and cons of utilizing specific technology in that client's representation. This requires a lawyer to understand the tech tools and devices used in legal practice, as well as remain aware of changes in such technology and the risks poses to client confidentiality.

B. Communication

Minn. R. Prof. Conduct 1.4 requires a lawyer to promptly inform a client about decisions or circumstances of a legal matter, and explain a matter to the extent necessary to permit the client to make informed decisions. The 2015 Amendments to the Rules of Professional Conduct clarify the lawyer's obligations to communicate with clients through the use of technology.

First, the 2015 Amendments modified the definition of a "writing" in Rule 1.0 to include all "electronic communications." Previously, the Rule referred only to emails, which did not include other forms of communication that lawyers may use with clients, such as text message, Facebook message, or Snapchat, which are now considered "writings" under Rule 1.0.

The 2015 Amendments also expand the reach of LPRB Opinion No. 19, which was issued by the Lawyers Professional Responsibility Board in 1999, and was later amended in 2010. In its original form, Opinion No. 19 permitted lawyers to utilize "digital cordless and cellular telephones" when communicating with clients. It was amended in 2010 to permit lawyers to utilize unencrypted email along with other technology when communicating with clients provided that a lawyer advised a client about communicating confidential information through "insecure means."

The Opinion states that "[w]hen the lawyer knows, or reasonably should know, that a client or other person is using an insecure means to communicate with the lawyer about confidential client information, the lawyer shall consult with the client about the confidentiality risks associated with inadvertent interception and obtain the client's consent." Thus, the Opinion requires a lawyer to assess the technology used in a client representation as it relates to confidential information and obtain the client's consent to communicate if the means of communication is "insecure."

One way for a lawyer to satisfy that obligation is to incorporate disclosures in a client engagement agreement, and discuss those disclosures with a client. For example, a disclosure in a client engagement agreement may inform a client about the methods of transmitting client information, such as encrypted or unencrypted email, the risks of those methods, and whether other practices specific to that attorney-client relationship should be implemented to minimize the risks of an inadvertent disclosure.

C. Confidentiality

Minn. R. Prof. Conduct 1.6 governs the confidentiality of client information. It generally precludes a lawyer from knowingly revealing or allowing others to access confidential client information. The obligation to protect electronic client information was previously assumed under the prior version of the Rules of Professional Conduct but is now specifically included in Rule 1.6(c), which provides that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Minn. R. Prof. Conduct 1.6(c).

The 2015 Amendment to Rule 1.6(c) also imposes three additional obligations on lawyers to develop technological literacy: first, a lawyer must undertake reasonable efforts to prevent the inadvertent disclosure of client information (the inadvertent disclosure is akin to unknowingly producing a privileged document; second, a lawyer must undertake reasonable efforts to prevent unauthorized access to client information (such as precluding a third party from obtaining client information by spear-phishing or hacking); and, finally, the efforts undertaken by a lawyer to protect client confidentiality must be reasonable.

Comment [17] to Minn. R. Prof. Conduct 1.6(c), which was amended in 2015, further clarifies a lawyer's confidentiality obligation: "[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation if the lawyer has made 'reasonable efforts' to prevent the access or disclosure." Comment [17] further provides that "[a] client may require the lawyer to implement special security measures not required by Rule 1.6 or may give informed consent to forgo security measures otherwise required by this Rule." Minn. R. Prof. Conduct 1.6(c), Cmt. [17].

Thus, Comment [17] not only requires a lawyer to implement reasonable efforts to maintain the confidentiality of client information but also requires a lawyer to discuss with a client the security measures governing the lawyer's use, possession, and transmission of confidential client data in at least three respects: what confidential client information is relevant and will be used in a client matter; what security measures has the lawyer implemented to protect that confidential client information; and, finally, what other security measures should be considered in light of the specifics of the client representation?

A lawyer's discussion of confidentiality with a client must also include a discussion about

protecting the confidentiality of client metadata. LPRB Opinion No. 22, which was adopted in March 2010, requires a lawyer to reasonably investigate and protect confidential client metadata when handling client documents. Thus, in addition to evaluating the reasonable efforts necessary to protect confidential client information, a lawyer should be aware of cybersecurity threats and undertake efforts to prevent the inadvertent disclosure or unauthorized access to a client's confidential metadata to maintain technological literacy.

D. Use of Non-lawyer Assistants

Finally, Minn. R. Prof. Conduct 5.3 establishes a lawyer's responsibilities regarding nonlawyer assistants, which is increasingly important due to the frequent reliance on nonlawyer assistants to store and manage electronic client information. Rule 5.3 states that "[w]hen a lawyer utilizes a nonlawyer assistant for such services, the lawyer must make reasonable efforts to ensure the services provided by the nonlawyer assistant comply with a lawyer's professional obligations" Minn. R. Prof. Conduct 5.3.

In the cybersecurity context, this Rule requires a lawyer to verify that a nonlawyer's services will protect the confidentiality of client information to the same degree a lawyer must protect a client's confidential information. Therefore, when retaining a nonlawyer assistant, a lawyer should evaluate the assistant's experience and technological literacy during the retention process to assure that the nonlawyer's services will be compatible with the lawyer's professional obligations.

For example, if a lawyer engages an e-discovery vendor, a lawyer should identify how confidential client information will be transmitted to and maintained by that vendor, the security protocols the vendor has implemented to protect that information, and how the information will be managed after the engagement has ended. This can be achieved by reviewing a copy of the vendor's document retention policies, security procedures, and cybersecurity insurance certificates. This can also be achieved by utilizing appropriate vendor engagement agreements that identify and explain how confidential client information should be managed.

E. ABA Formal Opinion 477R

In addition to the 2015 Amendments to Minnesota's Rules of Professional Conduct, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R on May 22, 2017. That Opinion, which was issued in the context of "when" a data incident will occur in a lawyer's practice, details a lawyer's obligation to secure client information in light of technological advances and cybersecurity risks. *See* ABA Formal Opinion 477R at 2.

The Opinion recommends that lawyers employ a reasonable-efforts standard to assess the security of confidential client information, which standard requires a lawyer to conduct a fact-based analysis regarding the protection of client communications and information in each attorney-client relationship, as well as evaluate the types of information being communicated, the methods of electronic communications employed, and the types of available security measures for each method. *See* ABA Model R. Prof. Conduct. 1.6, Cmt. [18].

Although Formal Opinion 477R does not change the landscape of a lawyer's ethical obligations concerning data privacy (particularly because Minnesota's Rules of Professional Conduct were previously amended in 2015), the Opinion does reiterate that a lawyer should continually evaluate the benefits and risks of legal technology and take reasonable precautions to preserve client confidences when utilizing legal technology in their practices.

Further, the Opinion identifies seven steps that a lawyer should take to satisfy the reasonable-efforts standard, which includes, among other steps, understanding the nature of the cybersecurity threat, understanding how client information is transmitted and stored, and conducting due diligence on vendors that provide technological services. Completing those steps, among other efforts, will allow a lawyer to develop technological literacy and satisfy the professional obligations required by the Minnesota Rules of Professional Conduct and Formal Opinion 477R.

Bryan R. Feldhaus

Bryan@lommen.com

Mr. Feldhaus is a shareholder with Lommen Abdo and advises clients on legal, regulatory, and compliance matters and advocates for clients in litigation and other proceedings. He provides these services in business litigation, professional liability litigation, intellectual property litigation, and data privacy matters. He recently obtained an LL.M. degree in corporate compliance and organizational ethics from the University of St. Thomas School of Law.