MINNESOTA LAWYER
SAINT PAUL LEGAL LEDGER
June 19, 2017 MINNLAWYER.COM Vol. 91 No. 7 | $6.00

Downloading technology in legal practice: ABA Formal Opinion 477

Bryan R. Feldhaus, Esq.
Special to Minnesota Lawyer

Today's tech tools, including mobile devices, cloud computing and social media, punctuate a new era of legal service. With these tools lawyers are able to better serve clients through increased efficiency and responsiveness. But technology has also introduced new risks to legal practice.


Bryan R. Feldhaus

Law firms, like other businesses, are increasingly at risk for data incidents that target client confidences. After all, case management and litigation databases maintained by law firms serve as repositories for confidential, sensitive information of clients. Additionally, client information is routinely transmitted from those repositories to clients and third-parties through email and other tech tools.

To mitigate those concerns, lawyers must monitor and assess how they obtain, manage and store confidential information from clients and utilize technology in their legal practice to prevent the unauthorized or inadvertent disclosure of client information. This is not simply a matter of prudence; it is required under the Minnesota Rules of Professional Conduct. (*See e.g.,* Minn. R. Prof. Conduct 1.0, 1.1, Cmt. [8], 1.4, Cmt. [4], 1.6(c), 5.3, Cmt. [3].)

On April 1, 2015, the Minnesota Rules of Professional Conduct were amended to reflect the increasing influence of technology on legal practice. The impetus for the amendments was the ABA's amendments to the Model Rules of Professional Conduct, which were based on the work of the ABA Commission on Ethics 20/20. That Commission analyzed how technology had changed legal services and proposed amendments to the Model Rules to address those changes. The ABA's Model Rules were fully adopted in February 2013 and Minnesota followed suit by amending its Rules of Professional Conduct in 2015.

I. ABA issues Formal Opinion 477 concerning legal technology.

But as cyber risk has evolved so too must the Rules of Professional Conduct. Recently, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R (Revised May 22, 2017). That opinion (which was issued in the context of "when" a data incident will occur rather than "if" a data incident will occur) details a lawyer's obligation to secure the communication of protected client information in light of technological advances and cybersecurity risks. (ABA Formal Opinion 477R at 2.)

First, the opinion acknowledges that law firms are attractive targets for cyber-attacks for two reasons: law firms obtain, store and use highly sensitive information about clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client; and the information in a law firm's possession is more likely to be of interest to a hacker and likely less voluminous than the information maintained by a client. (*Id.*) (internal citations omitted).

Second, the opinion reiterates that a lawyer is obligated to take "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." (ABA Model R. Prof. Conduct 1.6 (c)). This obligation requires a lawyer to engage in a fact-based analysis regarding the protection of client communications and information, which requires an evaluation of the types of information being communicated, the methods of electronic storage and transmission employed, and the types of available security measures for each method, among other factors. (*See* ABA Model R. Prof. Conduct. 1.6, Cmt. [18].)

Finally, the opinion concludes that a fact-based, reasonable efforts approach should dictate

the type of cybersecurity methods to be employed by a lawyer when maintaining or transmitting confidential client information.

For example, if a matter involves highly sensitive information, then the opinion suggests that a lawyer's efforts to protect such information "might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of telephone, fax and mail in Formal Opinion 99-413. (Formal Opinion 477R at 5.)

Conversely, in matters of normal or low sensitivity, the opinion proposes that "standard security methods with low reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent or unauthorized disclosure." (*Id.*)

The opinion, however, does not suggest what information might constitute "highly sensitive information" or matters of normal or low sensitivity. That obligation falls upon a lawyer when conducting the fact-based, reasonable efforts approach outlined in the opinion.

Nor does the opinion suggest that lawyers should avoid using technology in practice. After all, tech tools have greatly enhanced the quality and efficiency of providing legal services. Thus, even unencrypted email, which is particularly susceptible to cyber risk, remains a generally acceptable method of lawyer-client communication provided that the lawyer has implemented basic and reasonably available security measures. (*Id.*) In other instances, however, such as instances involving "highly sensitive information," unencrypted email is not appropriate and should not be used. (*See id.*)

II. ABA Formal Opinion 477 should shape the use of legal technology.

The critical takeaway from Formal Opinion 477 is that there is no golden rule governing a lawyer's use of technology in legal practice. Instead, a lawyer must assess and understand the types of client information maintained or transmitted, the methods of maintenance or transmission, and the security measures available to protect that information based on the applicable circumstances. The opinion states: "lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable." (*Id.*)

It is also important to understand that lawyers at large law firms are not the only targets for cyber incidents. The 2016 ABA Legal Technology Survey concluded that 25 percent of 10-49 lawyer firms have experienced a security breach whereas 8 percent of solo practitioners have experienced a security breach, both of which represent increases from 2015 levels. (2016 ABA Legal Technology Survey.) Thus, all lawyers, regardless of firm size, must be cognizant of their storage and transmission of electronic client information and undertake the fact-based, case-by-case analysis outlined in Formal Opinion 477 to prevent the inadvertent or unauthorized disclosure of client information. Minn. R. Prof. Conduct 1.6(c).

To conduct that fact-based analysis, a lawyer should take steps to assess the storage and communication of electronic client information, including the following: (1) understand the nature of the cybersecurity threat; (2) understand how client information is transmitted and stored; (3) understand and use reasonable electronic security measures; (4) determine how electronic communications about client matters should be protected; (5) label client confidential information; (6) train lawyers and non-lawyer assistants about technology and information security; and (7) conduct due diligence on vendors providing communication technology. (*See id.*) It is also important for lawyers to evaluate their existing policies and insurance coverages to minimize the risk of a cybersecurity breach involving client information and expedite their response should a cybersecurity breach occur.

Although the opinion was only recently issued by the ABA, its recommendations are not new. As previously stated, the 2012 amendments to the ABA Model Rules introduced a lawyer's obligation to take reasonable efforts to prevent the inadvertent or unauthorized disclosure of client information, which obligation was incorporated into Minnesota's Rules of Professional Conduct in 2015. Thus, the opinion does not change the landscape of a lawyer's ethical obligations concerning data privacy but reiterates 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.

Additionally, ABA Formal Opinion 477 will not be the last pronouncement about professional responsibility and legal technology. As technology evolves so too will a lawyer's professional obligations when using such testimony. After all, it was not long ago that Minnesota's Lawyer Professional Responsibility Board issued Opinion No. 19, which authorized the use of "digital cordless and cellular telephones" to transmit and receive confidential client information. (MN LPRB Op. No. 19, *Using Technology to Communicate Confidential Information to Clients*) (Adopted Jan. 22, 1999; Amended Jan. 22, 2010.)

Now, smartphones are ubiquitous in legal practice as will be future tech tools. The key for lawyers is to minimize the risks of using those tech tools while simultaneously fulfilling their professional duties in an increasingly threatening cyber environment.