ABA Formal Opinion 477R: Securing communication of protected client information

June 2017 | Eye on Ethics

by Peter Geraghty,
director, ETHICSearch

Just this past week, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R (Revised May 22, 2017) on the subject of a lawyer's ethical obligations to protect confidential client information when transmitting information relating to the representation over the internet. The opinion takes a fresh look at advances in technology and ever-increasing cybersecurity threats, and provides guidance as to when enhanced security measures are appropriate.

This opinion is an update to ABA Formal Opinion 99-413 *Protecting the Confidentiality of Unencrypted E-Mail* (1999).

In 99-413, the committee concluded that since email provided a reasonable expectation of privacy, lawyers could use it to communicate with their clients, since it would be just as illegal to wiretap a telephone as it would be to intercept an email transmission. At the same time, the committee recognized that some information is so sensitive that a lawyer might consider using particularly strong protective measures depending on the sensitivity of the information:

> ... The conclusions reached in this opinion do not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of email, just as they would warrant the avoidance of the telephone, fax and mail. – Formal Opinion 99-413 at page 2.

Since the time of Opinion 99-413, times have changed especially in the realm of technology and its many new and evolving manifestations that have become widespread in the profession. Laptop computers, smartphones, social media, cloud storage and Wi-Fi connections have become prevalent and much more commonplace than they were when 99-413 was written nearly 18 years ago.

The ABA Model Rules of Professional Conduct have also undergone several changes, particularly those that focus on a lawyer's obligation to protect client confidences when transmitting information over the internet.

Chief among these were the amendments to Rule 1.1 *Competence* and 1.6 *Confidentiality of Information* of the ABA Model Rules of Professional Conduct that were proposed by the ABA Ethics 20/20 Commission and subsequently adopted by the ABA House of Delegates at the 2012 ABA Annual Meeting. (The Ethics 20/20 Commission's Report and Recommendation concerning these amendments is available here.)

Paragraph 8 of the Comment to Rule 1.1 now states that "a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks of technology...*"

The commission also added a new subpart (c) to Rule 1.6 that states:

> **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.**

Paragraph 18 of the Comment to Rule 1.6 was also amended, making it clear that additional methods of security should be considered depending upon the sensitivity of the information that is to be transmitted.

In Opinion 477R, the committee took note of the increasing sophistication of cyber threats in today's technological environment and recognized that some new forms of electronic communication that have become commonplace may not in every instance provide a reasonable expectation of privacy:

> ...In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic

> security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.
>
> However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, 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 - Formal Opinion 477R at p. 5

In order to determine when additional security methods are required, the committee turned to the factors outlined in paragraph 18 of the Comment to Model Rule 1.6:

- 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).

The committee recommended the following steps lawyers should take to guard against disclosures, including:

1. Understand the nature of the threat. Consider the sensitivity of the client's information and whether it poses a greater risk of cyber theft. If there is a higher risk, greater protections may be warranted.

2. Understand how client confidential information is transmitted and where it is stored. Have a basic understanding of how your firm manages and accesses client data. Be aware of the multiple devices such as smartphones, laptops and tablets that are used to access client data, as each device is an access point and should be evaluated for security compliance.

3. Understand and use reasonable electronic security measures. Have an understanding of the security measures that are available to provide reasonable protections for client data. What is reasonable may depend on the facts of each case, and may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.

4. Determine how electronic communications about clients' matters should be protected. Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider

safeguards such as encryption or password protection for attachments. Take into account the client's level of sophistication with electronic communications. If the client is unsophisticated or has limited access to appropriate technology protections, alternative nonelectronic communication may be warranted.

5. Label client confidential information. Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule 4.4(b) *Respect for Rights of Third Persons,* the inadvertent recipient would be on notice to promptly notify the sender.

6. Train lawyers and nonlawyer assistants in technology and information security. Under Model Rules 5.1 and 5.3, take steps to ensure that lawyers and support personnel in the firm understand how to use reasonably secure methods of communication with clients. Also, follow up with law firm personnel to ensure that security procedures are adhered to, and periodically reassess and update security procedures.

7. Conduct due diligence on vendors providing communication technology. Take steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer.