By: Robert Ambrogi

LawSites

Tracking New and Intriguing Websites and Products for the Legal Profession

ABA Issues Major Ruling on Ethics of Email and Electronic Communications

By Robert Ambrogi on May 12, 2017

The American Bar Association's **Standing Committee on Ethics and Professional Responsibility** has issued a major new opinion providing guidance on the steps lawyers should take to protect client confidentiality in electronic communications.

The new opinion, **Formal Opinion 477** (embedded copy below), updates Formal Opinion 99-413, issued in 1999, to reflect changes in the digital landscape as well as 2012 changes to the ABA's Model Rules of Professional Conduct, particularly the addition of the duty of technology competence in Model Rule 1.1 and changes to Rule 1.6 regarding client confidences.

Most notably, the opinion says that some circumstances warrant lawyers using "particularly strong protective measures" such as encryption. In the 1999 opinion, the committee concluded that unencrypted email was acceptable because lawyers have a reasonable expectation of privacy in all forms of email communications.

In this new opinion, the committee declined to draw a bright line as to when encryption is required or as to the other security measures lawyers should take. Instead, the committee recommended that lawyers undergo a "fact-based analysis" that includes evaluating factors such as:

- 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.
- 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).

In some cases that will require encryption, the committee said, while for matters of "normal or low sensitivity," standard security measures will suffice.

> **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 [above] factors to determine what effort is reasonable.**

While the opinion urged lawyers to take reasonable steps to protect client communications, it said that it was beyond its scope to specify the steps for any given set of facts. Instead, the opinion listed seven considerations that should guide lawyers:

1. Understand the Nature of the Threat.

This includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. "Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft."

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information, so that the lawyer can better manage the risk of inadvertent or unauthorized disclosure of client-related information.

3. Understand and Use Reasonable Electronic Security Measures.

Because access to client communications can occur in different forms, ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process, a lawyer's reasonable efforts include analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions. Further, a lawyer should understand and use electronic security measures such as VPNs or other secure internet portals, use unique complex passwords that are changed periodically, implement firewalls, use anti-malware/anti-spyware/anti-virus software, and apply all necessary security patches.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

The opinion urges that, at the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for client communications. For sensitive communications, a lawyer should use encryption and should consider the use of password protection for any attachments. "Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails." The opinion further notes that a client's lack of technological sophistication or lack of available technology "may require alternative non-electronic forms

of communication altogether." Finally, the opinion notes that extra caution is required when a client uses computers subject to the access or control of a third party (such as a work computer).

5. Label Client Confidential Information.

Lawyers should mark privileged and confidential client communications as such in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. "This can also consist of something as simple as appending a message or "disclaimer" to client emails, where such a disclaimer is accurate and appropriate for the communication."

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Lawyers are ethically obligated to supervise their employees and subordinates to ensure compliance with ethical rules, and that obligation extends to electronic communications, the opinion says. For this reason, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients, as well as on reasonable measures for access to and storage of those communications.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

The opinion reaffirms the principle that lawyers must perform due diligence when selecting an outside vendor. Factors to consider include:

- Reference checks and vendor credentials.
- Vendor's security policies and protocols.
- Vendor's hiring practices.
- The use of confidentiality agreements.
- Vendor's conflicts check system to screen for adversity.
- The availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

If the lawyer lacks the competence to evaluate the vendor, the lawyer may perform the evaluation by associating with another lawyer or expert, or may educate him or herself.

The opinion also says that, when retaining a nonlawyer from outside the firm, the lawyer has further obligations to ensure that the nonlawyer's services are provided in a manner that is compatible with the lawyer's professional obligations.

Duty to Communicate

In addition to the seven factors summarized above, the opinion emphasizes that a lawyer has a duty to communicate with a client about the nature and method of electronic communications.

> **When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved. The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client.**

Changes to Model Rules

The opinion relies heavily on two 2012 changes to the Model Rules. I've written frequently here about the duty of technology competence and I've been maintaining a tally of the **states that have adopted the duty**. This opinion expressly refers to that duty as one of the reasons for issuing an update to its 1999 opinion on email communications.

It also references the 2012 change to Rule 1.6 on confidentiality, which added a new duty in paragraph (c): "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."

The committee concludes its opinion with this summary:

> **"A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.**

This is an extremely important opinion that every lawyer should stop and read today.

For your convenience, the opinion is embedded below.

aba_formal_opinion_477.pdf

LawSites

By: Robert Ambrogi

Copyright © 2019, Robert Ambrogi. All Rights Reserved.