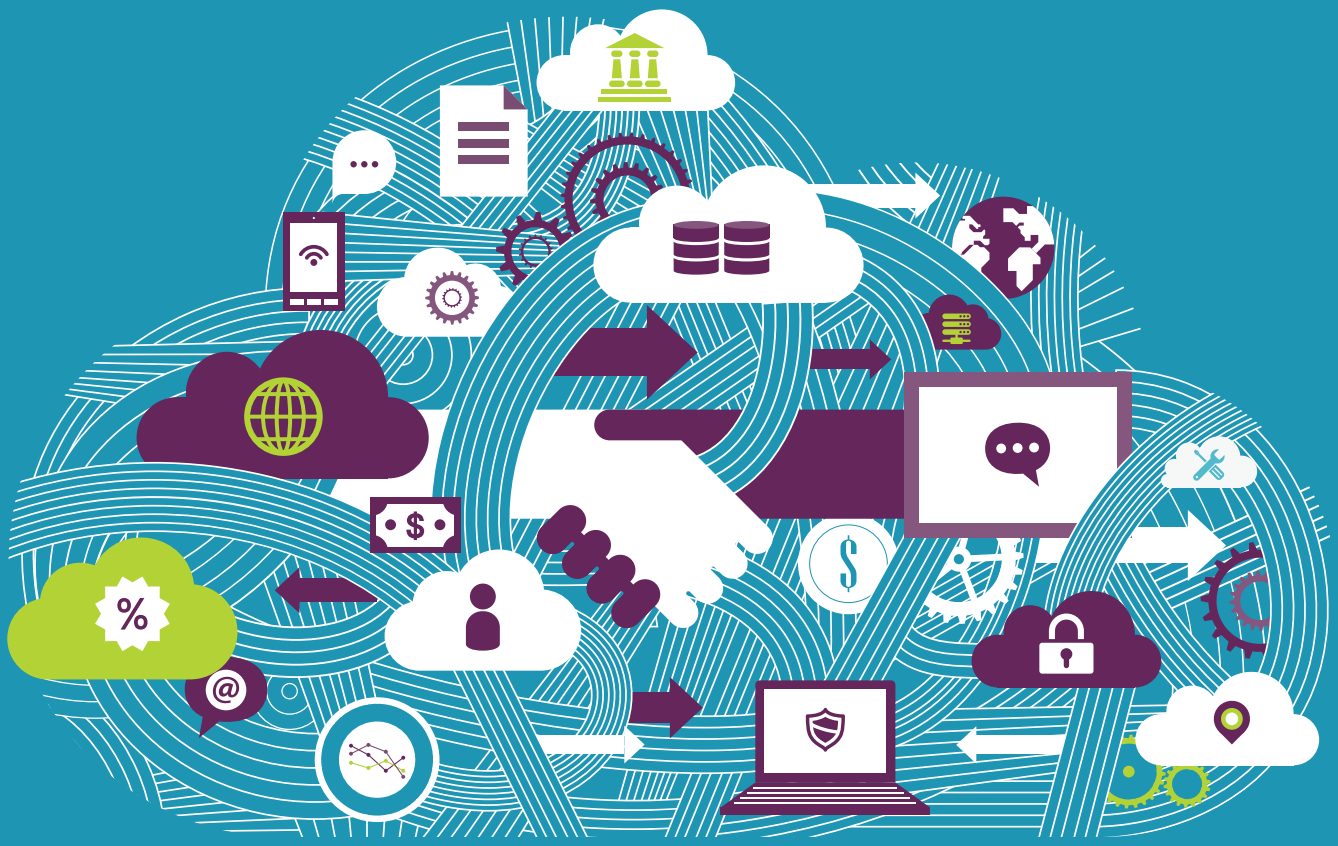
November/December 2020

The Bencher®

THE MAGAZINE OF THE AMERICAN INNS OF COURT®



Cybersecurity

www.innsofcourt.org

American Inns of Court®

PHOTO CREDIT: ©iStockphoto.com/akindo.

Ethical Issues in a Cyberworld

By Michael Hooker, Esquire, and Jason Pill, Esquire

Even if you are a relatively new lawyer, you probably will agree that the most significant change in the way attorneys practice law over the past couple of decades involves the use of and reliance on technology. Now, more than ever, documents are produced, modified, and stored electronically, greatly reducing the need for paper files and associated storage space. Email, laptops, smartphones, tablets, and social media enable lawyers to communicate more quickly and effectively with their clients. Services such as Zoom make it possible to conduct hearings, depositions, and conference calls remotely, frequently saving time and money for both lawyers and their clients.

But the ever-expanding use by lawyers of technology also raises new ethical issues. The Rules of Professional Conduct require lawyers to protect their clients' confidential information. Because lawyers obtain, store, and use highly sensitive client information, law firms increasingly are becoming attractive targets for phishing schemes, ransomware attacks, and other cybercrimes. What are the ethical implications of a lawyer's failure to adequately protect a client's electronically stored information from a cyber breach? What do the ethics rules require a lawyer to do in response to such an intrusion? Although these and related questions were foreign to the practice of law not that long ago, lawyers today need to understand that advances in technology bring with them new risks and ethical concerns.

Protection of Client Information from Cyberattacks

Traditionally, documents were kept in paper form in a lawyer's office. However, with advances in technology, lawyers have begun collecting and storing more and more client information in electronic form. Lawyers have long possessed the obligation to protect confidential client information under ethics rules like Rule 1.6 of the Model Rules of Professional Conduct. Because Rule 1.6 does not differentiate between paper versus electronic information, the duty to protect confidential client information applies equally to both hard copy and electronic information.

Recognizing the increasing impact of technology on the practice of law, the American Bar Association

(ABA) adopted in 2012 a series of "technology amendments" to the Model Rules. For instance, Comment [8] to Model Rule 1.1 was modified to require that lawyers keep abreast of the "benefits and risks associated with relevant technology" as part of their duty to maintain the requisite knowledge and skill required to competently represent their clients. Once the relevant technologies are understood, a lawyer must use and maintain the technologies in a manner that reasonably safeguards client information. This can be done either through the lawyer's own study and investigation or by employing or retaining a qualified lawyer and nonlawyer assistants.

The 2012 amendments also modified both Model Rule 1.6 and its commentary regarding the actions that lawyers must take to protect confidential client information. Rule 1.6(c) now requires a lawyer to "make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client." However, Comment [18] explains that unauthorized access to, or disclosure of, client information will not constitute an ethical violation if the lawyer has undertaken the requisite "reasonable efforts" to prevent unauthorized access or disclosure. In other words, lawyers are not guarantors that information they maintain will never be accessed or inadvertently disclosed, so long as they take reasonable steps to protect such information.

Because Model Rule 1.6 requires reasonable efforts to protect client information, an important question facing lawyers is what constitutes "reasonable efforts." In 2017, the ABA issued Formal Opinion 477R to address the role and risks of technology in the practice of law. Unfortunately, Opinion 477R did not provide definitive guidance regarding what protective measures are reasonable under the rule.

After concluding that the reasonable efforts question cannot be answered with "hard and fast rules," Opinion 477R outlined a series of factors that lawyers must consider in deciding what is needed to protect confidential information, including: (i) the sensitivity of the information; (ii) the likelihood of access or disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients. In short, Opinion 477R adopted a "fact-based" approach to security obligations that requires lawyers to assess risks, identify and implement appropriate security measures commensurate to those risks, verify that the measures are effectively implemented, and ensure that the measures are continually updated in response to new developments.

Opinion 477R also requires lawyers to constantly analyze how they communicate electronically about client matters and to determine what efforts are reasonable to protect such communications. Again, without providing concrete guidance concerning what is "reasonable," Opinion 477R outlined general steps that a lawyer should take to reasonably protect client-related communications, including: (i) understanding the nature of the threat; (ii) understanding how client confidential information is transmitted and where it is stored; (iii) understanding and using reasonable electronic security measures; (iv) determining how electronic communications about client matters should be protected; (v) labeling client information as confidential; (vi) training lawyers and nonlawyer assistants in technology and information security; and (vii) conducting due diligence regarding vendors providing communication technology. Importantly, even after a lawyer is satisfied that the security measures employed are sufficient, the lawyer must periodically reassess these factors to confirm that the protective measures continue to comply with ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

Significantly, Opinion 477R recognizes that a client might request or require a lawyer to implement specific client-mandated measures to protect confidential information that differ from what the lawyer otherwise might conclude is ethically required. Pursuant to Comment [19] to Rule 1.6, a "client may require the lawyer to implement special security measures not required by the Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule." Consequently, it is good practice to communicate with clients regarding appropriate methods of electronic communication and data storage, particularly if highly sensitive client information is involved, to ensure that everyone is on the same page about how such information should be handled by the lawyer.

Obligations after a Data Breach Occurs

In 2018, the ABA issued Formal Opinion 483 regarding the ethical obligations possessed by lawyers after electronic data breaches and cyberattacks. In Opinion 483, the ABA outlined steps that a lawyer must undertake to competently represent clients regarding potential and actual data breaches. For instance, lawyers are directed to employ reasonable

Continued on the next page.

efforts to monitor all relevant technologies so that breaches can be identified and determinations regarding further required action can be made.

In the event that a data breach occurs, the impacted lawyer or law firm must take prompt action to stop the breach. Indeed, Opinion 483 recommends that lawyers and law firms adopt an incident response plan before any data breach occurs so that preplanned and systematic action can be taken in the event of an intrusion. But whether or not such a plan exists, breached lawyers and law firms are required to take all reasonable steps necessary to restore computer operations so that the needs of their clients can be serviced.

Opinion 483 further mandates that lawyers undertake action to determine what occurred during a data breach if one is discovered. In conducting such a post-data breach investigation, a lawyer is required to gather sufficient information to ensure that the intrusion has been stopped, and, if possible, to evaluate what was lost or accessed. Such information is necessary to understand the scope of the breach and to permit an accurate disclosure of the breach to the lawyer's clients if disclosure is required by applicable ethical rules.

But importantly, as recognized in Opinion 477R and reiterated in Opinion 483, preserving client confidentiality is not a strict liability standard that requires lawyer-held data to be invulnerable or impenetrable. Again, the standard is one of "reasonable efforts," and no ethical violation occurs if the lawyer has implemented reasonable measures to prevent intrusion into clients' confidential information.

Obligation to Notify Clients of a Data Breach

After a lawyer discovers that a data breach has occurred, the lawyer must evaluate whether any clients need to be notified of the breach under applicable ethical rules. Pursuant to Model Rule 1.4(a)(3), a lawyer is required to keep clients reasonably informed about the status of their matters. Additionally, Model Rule 1.4(b) provides that a lawyer must explain a matter to the extent reasonably necessary to permit clients to make informed decisions about their representation.

Opinion 483 took the position that the foregoing rules create an obligation for lawyers to communicate with current clients about a data breach in at least certain circumstances. Specifically, the ABA concluded that lawyers possess the duty to notify current clients about a breach involving, or having a substantial likelihood of involving, material client confidential information. In the ABA's view, such notice is an integral part of keeping clients informed and affording clients an opportunity to make informed decisions about their representation. On the other hand, the ABA was "unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice." Because it is not clear what notice obligations, if any, exist between these two extremes, lawyers should carefully consider whether applicable ethics rules might still require notice to current or former clients even if not mandated by Opinion 483.

The nature and extent of the lawyer's notification to clients (if notice is required) will depend on the type of breach that occurred and the nature of the compromised data. In any event, the disclosure must be sufficient to provide enough information for clients to make an informed decision as to what, if anything, they should do in response to the breach.

Finally, lawyers cannot ignore that state and federal laws impose various (and often conflicting) obligations on businesses that have been victimized by a data breach. Thus, a lawyer experiencing a data breach must carefully analyze relevant laws and regulations to ensure that all necessary actions are taken after an intrusion, including, without limitation, timely compliance with all applicable notice requirements. Fulfillment of ethical obligations following a breach will not necessarily satisfy all state and federal law requirements or vice versa.

Conclusion

With data breaches and cyberattacks becoming almost routine, lawyers must implement adequate security measures to protect confidential client information and be prepared to respond appropriately after a data breach occurs. Although the ABA has provided some recent guidance regarding the ethical obligations of lawyers to protect and secure clients' electronic data, this area of legal ethics is likely to undergo further refinement and articulation in the future as both client and lawyer data becomes even more increasingly digital. ◆

Michael S. Hooker, Esquire, is a partner in the Tampa, Florida, office of Phelps Dunbar. He is a Master of the Bench member of the Tampa Bay American Inn of Court. Jason A. Pill, Esquire, is also a partner in the Tampa office of Phelps Dunbar and is a Barrister member of the Wm. Reece Smith Jr. Litigation American Inn of Court.