AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477

May 11, 2017

Securing Communication of Protected Client Information

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.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for e-mail communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: “Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation.”¹

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.²

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.³

In 2012 the ABA adopted “technology amendments” to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c)

---

and a new Comment to Rule 1.6, addressing a lawyer’s obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term “cybersecurity” has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of “when,” and not “if.” Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the “technology amendments” made to the Model Rules in 2012, identify some of the technology risks lawyers’ face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” The scope of this requirement was clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

4. “Cybersecurity” is defined as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” CYBERSECURITY, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/cybersecurity (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI’s Cyber Division, indicated that “[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm’s computer system is a really optimal way to obtain economic and personal security information.” Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.


7. Id. at 43.
Regarding the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.  

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise. The 2012 modification added a new duty in paragraph (c) 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.”

Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

---

8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

9. MODEL RULES OF PROF’L CONDUCT R. 1.6(a) (2016).

10. Id. at (c).
At the intersection of a lawyer's competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.\textsuperscript{11}

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

\dots rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.\textsuperscript{12}

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- 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).\textsuperscript{13}

\textsuperscript{11} The 20/20 Commission’s report emphasized that lawyers are not the guarantors of data safety. It wrote: "[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client’s confidences are subject to unauthorized access or disclosed inadvertently without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances.”

\textsuperscript{12} ABA CYBERSECURITY HANDBOOK, supra note 3, at 48-49.

\textsuperscript{13} MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2013). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.”
A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive 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 the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

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.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. **Understand the Nature of the Threat.**

Understanding the nature of the threat 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. “Reasonable efforts” in higher risk scenarios generally means that greater effort is warranted.

---

14. See item 3 below.
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. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer’s task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. **Understand and Use Reasonable Electronic Security Measures.**

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As comment [18] makes clear, what is deemed to be “reasonable” may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or 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. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm’s technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, “delete” usually does not mean information is permanently deleted, and “deleted” data may be subject to recovery. Therefore, a lawyer should consider
whether certain data should ever be stored in an unencrypted environment, or electronically transmitted at all.

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

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it, and 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.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client’s lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party. If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived, and the lawyer must determine whether it is prudent to warn a client of the dangers associated with such a method of communication.

---


18. some state bar ethics opinions have explored the circumstances under which e-mail communications should be afforded special security protections, See, e.g., Tex. Prof’l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer…;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
5. **Label Client Confidential Information.**

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” 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.¹⁹

Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has received an inadvertently sent “document or electronically stored information relating to the representation of the lawyer’s client” to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer’s duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

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

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, 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. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being

---

¹⁹ See Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).
implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. **Conduct Due Diligence on Vendors Providing Communication Technology.**

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may 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; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.\(^\text{20}\)

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including “using an Internet-based service to store client information.” Comment [3] provides that the “reasonable efforts” required by Model Rule 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.”21 If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.22

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer’s actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. 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.23 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. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [18] to Model Rule 1.6, “A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.”

---

21. The ABA’s catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer,” MODEL RULES OF PROF’L CONDUCT R. 5.3 cmt. [4] (2017). The concept of monitoring recognizes that although it may not be possible to “directly supervise” a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c Filed_may_2012.auth_checkdam.pdf.

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

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.
New York County Lawyers Association Professional Ethics Committee

Formal Opinion 749

February 21, 2017

TOPIC: A lawyer’s ethical duty of technological competence with respect to the duty to protect a client’s confidential information from cybersecurity risk and handling e-discovery when representing clients in a litigation or government investigation.

DIGEST: A lawyer’s ethical duty of competence extends to the manner in which he provides legal services to the client as well as the lawyer’s substantive knowledge of the pertinent areas of law. The duty of competence expands as technological developments become integrated into the practice of law. Lawyers should be aware of the disclosure risks associated with the transmission of client confidential information by electronic means, and should possess the technological knowledge necessary to exercise reasonable care with respect to maintaining client confidentiality and fulfilling e-discovery demands. Further, a lawyer’s duty of competence in a litigation or investigation requires that the lawyer have a sufficient understanding of issues relating to securing, transmitting, and producing electronically stored information ("ESI"). The duty of technological competence required in a specific engagement will vary depending on the nature of the ESI at issue and the level of technological knowledge required. A lawyer fulfills his or her duty of technological competence if the lawyer possesses the requisite knowledge personally, acquires the requisite knowledge before performance is required, or associates with one or more persons who possess the requisite technological knowledge.

RULES OF PROFESSIONAL CONDUCT: 1.1, 1.6, 5.1, 5.3

OPINION

A lawyer has a duty to “provide competent representation to a client,” which requires that the lawyer demonstrate “the legal knowledge, skill, thoroughness and preparation necessary for the representation.” New York Rules of Professional Conduct ("RPCs"), RPC 1.1. A comment to the rule notes that “[t]o maintain the requisite knowledge and skill, a lawyer should . . . (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information.” RPC 1.1, Cmt. [8]. RPC 1.6 provides that a lawyer “shall not knowingly reveal confidential information, as defined in this RPC, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person.” RPC 1.6(c) further requires a lawyer to “exercise reasonable care to prevent disclosure of information related to the representation by employees, associates and others whose services are utilized in connection with the representation.”

Duty of Competence and Protection of Electronically Transmitted Client

949112v.5 2189/00001
Information

Compliance with RPC 1.6 requires that lawyers who use technology to store or transmit a client’s confidential information, or to communicate with clients, use reasonable care with respect to those uses. The lawyer must assess the risks associated with the use of that technology to determine if the use is appropriate under the circumstances. See, e.g., N.Y. State 709 (1998) (“an attorney must use reasonable care to protect confidences and secrets”); N.Y. City 94-11 (lawyer must take reasonable steps to secure client confidences and secrets). Lawyers should be aware that the storage and transmission of a client’s confidential information electronically carries a risk of disclosure if the stored or transmitted data is hacked, or if human, software or hardware error results in an inadvertent disclosure.

Attacks on computer systems by those trying to gain confidential, proprietary, or other sensitive information for personal or political gain (including so-called “hacktivists”) are reported with alarming frequency. Corporate clients have become proactive in attempting to ensure that its outside vendors—including lawyers—who have access to sensitive corporate information sufficiently protect that information from disclosure through inadvertence or cyber-attack. Individual clients are increasingly sensitive to the potential harm from widely reported data breaches, and similarly expect their lawyers to use appropriate measures to avoid unauthorized disclosure of personal data. In response to these concerns, at least 25 states have adopted rules regarding maintaining technological competence, including most recently Florida’s rule, which mandates continuing legal education on the subject. See, e.g., Florida Rules of Professional Conduct, Rule 6-10.3(b) (effective January 1, 2017, a Florida lawyer’s CLE requirements will include 3 credit hours in approved technology programs); California Standing Committee on Professional Responsibility and Conduct Formal Op. 2015-193 (concluding that an attorney lacking the required e-discovery competence must either acquire the requisite skill before performance is required, associate with technical consultants or competent counsel, or decline the representation). An overwhelming majority of lawyers recently surveyed who work in firms ranging from solo practitioners to over 500 attorneys believed training in the firm’s technology is important.¹

Additionally, lawyers who represent clients who are located outside of New York may, in certain instances, be subject to laws in those other states that require a heightened level of protection of electronic communications. See, e.g., Mass. Gen. L. Ch. 93H, 201 C.M.R. 17 (requiring, where technically feasible, the encryption of personal information stored on portable devices and personal information transmitted across public networks or wirelessly); Nevada Senate Bill 227 (amending Nev. Rev. Stat. § 597.970 and requiring that data collectors who conduct business in the state encrypt data storage devices—including computers, cell phones and thumb drives—that contain personal information that are moved outside the secured physical and logical boundaries of the data collecting

entity).

Lawyers must have a sufficient understanding of the technology — either directly or through associating with persons possessing such knowledge — to determine how to satisfy the lawyer’s duty of reasonable care. Reasonable care will vary depending on the circumstances, including the subject matter, the sensitivity of the information, the likelihood that the information is sought by others, and the potential harm from disclosure. See NYCLA Op. 738 (2008) (lawyer may not ethically search metadata made available through an adversary’s inadvertent disclosure of client confidential information through metadata); N.Y. State 782 (2004) (addressing the exercise of reasonable care to prevent the disclosure of client confidential information through metadata).

**Duty of Competence and Electronically Stored Information**

Lawyers who represent client in litigations, or in government or regulatory investigations, are well aware that often a significant aspect of the representation of the client is the collection, preservation and production of ESI. The ethical duty of competence requires an attorney to assess at the outset of e-discovery issues that may arise in the course of the representation, including the likelihood that e-discovery will or should be sought by either side, identification of likely electronic document custodians, and preservation and collection of potentially relevant ESI in an appropriate database that will permit the lawyer to search for responsive ESI during e-discovery.

A lawyer’s obligations with respect to ESI will be governed by applicable state or federal law. See, e.g., Fed. R. Civ. P. Rules 16, 26 and 37 (outlining a federal court litigant’s obligations with respect to the presentation and production of ESI); Rules 202.12(b) and 202.70(g) of New York’s Uniform Trial Court Rules (requiring all attorneys be sufficiently versed in matters relating to their client’s technological systems to be competent to discuss all issues relating to electronic discovery at preliminary conferences). In addition, a lawyer’s ethical duty of competence requires the lawyer to assess his or her own e-discovery skills and resources in order to meet these ESI demands. E-discovery needs in a particular matter may include (i) assessing e-discovery needs and ESI preservation procedures; (ii) identifying custodians of potentially relevant ESI; (iii) understanding the client’s ESI system and storage; (iii) determining and advising the client on alternatives for the collection and preservation of ESI and associated costs; and (v) ensuring that the collection procedures, software and/or databases created will permit the lawyer to provide responsive ESI in an appropriate manner. If a lawyer lacks the requisite skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate with another attorney or expert who possess these skills. RPC 1.1 (b) & Cmt., 1,Cmt. 8.

Where a lawyer satisfies his or her duty of technological competence by associating with another lawyer or expert, the lawyer remains responsible for fulfilling the duty of
competence, and must satisfy himself or herself that the work of the associated lawyer or expert is being done properly. The lawyer must understand the pertinent legal issues and the e-discovery obligations imposed by law or court order and the relevant risks associated with the e-discovery tasks at hand, and satisfy himself or herself that everyone involved in the e-discovery process on behalf of the client is conducting themselves accordingly. See RPCs 5.1, 5.3.

CONCLUSION

A lawyer’s ethical duty of competence extends to the manner in which he or she provides legal services to the client as well as the lawyer’s substantive knowledge of the relevant areas of law. Lawyers must be responsive to technological developments as they become integrated into the practice of law. A lawyer cannot knowingly reveal client confidential information, and must exercise reasonable care to ensure that the lawyer’s employees, associates and others whose services are utilized by the lawyer not disclose or use client confidential information. The risks associated with transmission of client confidential information electronically include disclosure through hacking or technological inadvertence. A lawyer’s duty of technological competence may include having the requisite technological knowledge to reduce the risk of disclosure of client information through hacking or errors in technology where the practice requires the use of technology to competently represent the client.

A lawyer’s competence with respect to litigation requires that the lawyer possesses a sufficient understanding of issues relating to securing, transmitting, and producing ESI. The duty of competence in a specific engagement will vary depending on the nature of the ESI at issue and the level of technological knowledge required. A lawyer fulfills his or her duty of competence with respect to technology if the lawyer possesses the requisite knowledge personally, acquires the requisite knowledge in a timely manner and before performance is required, or associates with one or more persons who possess the requisite technological knowledge. If a lawyer is unable to satisfy the duty of technological competence associated with a matter, the lawyer should decline the representation.
Formal Opinion 483

Lawyers’ Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients “reasonably informed” about the status of a matter and to explain matters “to the extent reasonably necessary to permit a client to make an informed decision regarding the representation.” Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.

In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet. This

---

1 This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

2 See, e.g., Dan Steiner, Hackers Are Aggressively Targeting Law Firms’ Data (Aug. 3, 2017), https://www.cio.com (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”); See also Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).


opinion picks up where Opinion 477R left off, and discusses an attorney’s ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney’s ethical obligations after a data breach, and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules per se represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney’s roles, level of authority, and responsibility in the law firm’s operations.7

---

6 The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a “firm.” A “firm” is defined in Rule 1.0(c) as “a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization.” How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer’s position in the firm. See MODEL RULES OF PROF’L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF’L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyer); and MODEL RULES OF PROF’L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

7 In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.”) See also, e.g., Cybersecurity Resources, ABA Task Force on Cybersecurity, https://www.americanbar.org/groups/cybersecurity/resources.html (last visited Oct. 5, 2018).
I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

In recommending the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to ‘keep abreast of changes in the law and its practice.’ The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.

---

10 ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”
In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.11

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that “such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.”

Applying this reasoning, and based on lawyers’ obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data. Without such a requirement, a lawyer’s recognition of any data breach could be relegated to happenstance — and the lawyer might not identify whether a breach has occurred, whether further action is warranted, whether employees are adhering to the law firm’s cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties, and how and when the lawyer must take further action under other regulatory and legal provisions. Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

---

14 MODEL RULES OF PROF’L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF’L CONDUCT R. 1.15 (2018).
15 See also MODEL RULES OF PROF’L CONDUCT R. 5.1 & 5.3 (2018).
16 The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, https://www.us-cert.gov/ais (last visited Oct. 5, 2018); See also National Cyber Security Centre “Ten Steps to Cyber Security” [Step 8: Monitoring] (Aug. 9, 2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.\(^{18}\) The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. “One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents.”\(^{19}\) While every lawyer’s response plan should be tailored to the lawyer’s or the law firm’s specific practice, as a general matter incident response plans share common features:

The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm’s network.

Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

\(^{18}\) See ABA Cybersecurity Handbook, supra note 11, at 202 (explaining the utility of large law firms adopting “an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.”).

define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.\textsuperscript{20}

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer’s clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client.”\textsuperscript{21} These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer’s office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer’s duty of communication and honesty under


\textsuperscript{21} We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer’s computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.
Model Rules 1.4 and 8.4(c).\textsuperscript{22} Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer’s efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise.\textsuperscript{23} The 2012 modification added a duty in paragraph (c) 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.”\textsuperscript{24}

Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a “reasonable efforts” determination. Those factors include:

- 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

\textsuperscript{22} The rules against dishonesty and deceit may apply, for example, where the lawyer’s failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. See, e.g., MODEL RULES OF PROF’L CONDUCT R. 4.1 cmt. [1] (2018) (“Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.”).

\textsuperscript{23} MODEL RULES OF PROF’L CONDUCT R. 1.6(a) (2018).

\textsuperscript{24} Id. at (c).
• 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).  

As this Committee recognized in ABA Formal Opinion 477R:

At the intersection of a lawyer’s competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney’s competence in preserving a client’s confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable. Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access. As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

Although security is relative, a legal standard for “reasonable” security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.

---

25 MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2018). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, supra note 9, at 5.

26 ABA CYBERSECURITY HANDBOOK, supra note 11, at 122.

27 MODEL RULES OF PROF’L CONDUCT R. 1.6, cmt. [18] (2018) (“The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”)

28 ABA CYBERSECURITY HANDBOOK, supra note 11, at 73.
Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely. In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer’s Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client. We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must “keep the client reasonably informed about the status of the matter.” Rule 1.4(b) provides: “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.” Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.

30 This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.
31 Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass’n Op. 842 (2010) (Question 10: “If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients’ confidential information,
Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a “serious breach.”\[32\] The Committee advised:

Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client’s legal matter, disclosure of the breach would be required under Rule 1.4(b).\[33\]

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer’s ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client’s interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a “client reasonably informed about the status of the matter” and the lawyer should provide information as would be “reasonably necessary to permit the client to make informed decisions regarding the representation” within the meaning of Model Rule 1.4.\[34\]

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4’s requirement to keep clients “reasonably informed about the status” of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

\[33\] Id.
\[34\] MODEL RULES OF PROF’L CONDUCT R. 1.4(b) (2018).
Model Rule 1.15(a) provides that a lawyer shall hold “property” of clients “in connection with a representation separate from the lawyer’s own property.” Funds must be kept in a separate account, and “[o]ther property shall be identified as such and appropriately safeguarded.” Model Rule 1.15(a) also provides that, “Complete records of such account funds and other property shall be kept by the lawyer . . . .” Comment [1] to Model Rule 1.15 states:

A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer’s business and personal property.

An open question exists whether Model Rule 1.15’s reference to “property” includes information stored in electronic form. Comment [1] uses as examples “securities” and “property” that should be kept separate from the lawyer’s “business and personal property.” That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15’s safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, “Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information.”

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.
2. Former Client

Model Rule 1.9(c) requires that “A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.” When electronic “information relating to the representation” of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer’s obligation to notify the former client. Rule 1.9(c) provides that a lawyer “shall not . . . reveal” the former client’s information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is 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.

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9. We also note that Rule 1.16(d) directs that lawyers should return “papers and property” to clients at the conclusion of the representation, which has commonly been understood to include the client’s file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely. Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client’s electronic information that is in the lawyer’s possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

---

36 See Discipline of Feland, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent’s argument that the court should engraft an additional element of proof in a disciplinary charge because “such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.”).
the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.\(^\text{39}\)

3. Breach Notification Requirements

The nature and extent of the lawyer’s communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the “safe harbor” provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer’s office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer’s plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients’

\(^{39}\) Cf. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).
information. Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data breach, the lawyer should evaluate the lawyer’s obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws. Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information. Most breach notification laws specify who must comply with the law, define “personal information,” define what constitutes a breach, and provide requirements for notice. Many federal and state agencies also have confidentiality and breach notification requirements. These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual’s relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer’s possession that was accessed by an unauthorized user.

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make “reasonable efforts to prevent the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

---

42 Id.
43 Id.
44 ABA CYBERSECURITY HANDBOOK, supra note 11, at 65.
45 Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.
breach under Model Rule 1.4 in sufficient detail to keep clients “reasonably informed” and with an explanation “to the extent necessary to permit the client to make informed decisions regarding the representation.”
Compentence

Must a Lawyer Protect Client Confidences From Cyber Attacks?

By James Q. Walker

Technology is integral to a lawyer's ability to engage in the practice of law. Whether we are scheduling meetings with clients by email or text message, conducting due diligence in an electronic data room, using a database to produce electronic discovery in a litigation or government investigation, or filing pleadings in court, transactional and litigation lawyers alike rely on technology to represent clients. As a result, law firms are attractive targets for hackers who seek the information lawyers regularly maintain on behalf of clients, including documents and communications relating to confidential financial data, contemplated business transactions, trade secrets, litigation strategy, and business strategy.

Increasingly corporate clients are auditing their outside law firms to assess their cybersecurity preparedness and ensure that their firms have implemented security measures that adequately mitigate the risk of a data breach. See Law Firm Cyber Security Scorecard, LogicForce (Q4 2017) (48 percent of law firms had their data security practices audited by at least one corporate client in the past year). These audits typically require detailed information about IT systems, data management policies, and e-discovery practices.

Lawyers are ethically bound to provide competent representation to their clients, and must demonstrate the legal knowledge, skill, thoroughness and preparation reasonably necessary for each client representation. This means lawyers must be competent in their use of technology to carry out the representation of each client, and must take appropriate measures to protect each client’s confidential information. As explained by the New York County Lawyer’s Association’s ethics committee, “[l]awyers should be aware of disclosure risks associated with the transmission of client confidential information by electronic means, and should possess the technological knowledge necessary to exercise reasonable care with respect to maintaining client confidentiality” to avoid inadvertent disclosure through interception or misdirection. New York County Ethics Op. 749 (emphasis added).

“Reasonable care” may differ from one law firm to the next based, in part, on the clients serviced by the firm. For example, lawyers who represent clients in the financial industry are under additional pressure to ensure that they have implemented adequate cybersecurity regimes. The two most recent nominees to the U.S. Securities and Exchange Commission both said they want to help the SEC increase its oversight of cybersecurity efforts at firms the commission regulates.

Moreover, as of March 2017, any institution covered by the New York Banking Law, Insurance Law or Financial Services Law must comply with the New York Department of Financial Services (“DFS”) Cybersecurity rules. The DFS Cybersecurity rules require covered institutions to develop a cybersecurity program, to meet certain reporting and certification requirements, to design procedures to ensure the security of the institution’s systems and nonpublic information that is accessible to third party service providers (such as their lawyers), and to make a risk assessment regarding appropriate controls for third party service procedures based on the specific facts and circumstances pre-

James Walker concentrates his practice in government investigations, complex commercial litigation, professional liability and legal ethics. Mr. Walker represents directors, officers, and lawyers in government and internal investigations of potential criminal, regulatory and/or professional misconduct, and in related criminal and civil litigation and regulatory proceedings. Mr. Walker is the Chair of the New York County Lawyer’s Association Professional Ethics Committee, and has served on the New York City Bar’s Professional Discipline, Professional and Judicial Ethics, Professional Responsibility, and Securities Regulation Committees, and on the New York State Bar Association Committee on Professional Ethics. He frequently lectures on legal ethics, internal investigations and corporate governance. Mr. Walker also serves as the General Counsel of Richards Kibbe & Orbe LLP.
sented. 23 NYCRR 500, et seq. (2017). Law firms that currently represent, or wish to represent, institutions covered by the DFS Cybersecurity regulations will need to ensure that their internal cybersecurity regimes are responsive to their DFS-covered client’s cybersecurity needs.

**Cyber Attacks Against Law Firms**

Understanding past cyber-attacks that have involved law firms may help law firms to identify the current risk of interception and to mitigate exposure to a cyber-attack. Reported cyber-attacks against law firms typically have involved the use of malware to gain access to a law firm’s computer systems in order to (1) hold data hostage until a ransom is paid; (2) obtain nonpublic material information about pending business transactions for personal financial gain; or (3) obtain and disclose compromising information concerning clients and/or the firm as a form of activism (or “hacktivism”).

“Ransomware” describes malware that installs on a device without the user’s knowledge, encrypts files, and holds the user’s data hostage unless the ransom is paid, typically in the form of a cryptocurrency payment (e.g., bitcoin). See Casey Sullivan, DLA Piper’s Cyber Attack and Why it Matters, Big Law Business (June 28, 2017).

Wiperware is similar to ransomware, except that rather than seeking financial gain the hacker seeks to destroy data and/or disable systems. See Jun Du, How NotPetya is So Very Different from WannaCry, (June 30, 2017).

The hack of Moses Afonso Ryan (“MAR”) illustrates a typical ransomware attack. On May 22, 2015, a lawyer at MAR, a 10-person Rhode Island law firm, clicked on an email that contained an encrypted virus that disabled the firm’s computer network for three months, during which time the firm negotiated a ransom and obtained the decryption tools to regain control of the system.

The hacker extorted over $25,000 in payments from the firm in exchange for release of encrypted documents and information. To add to the firm’s woes, its insurer paid only $20,000 under a sublimit in its business interruption policy. MAR sued the insurer for $700,000, which the firm alleged represented the reduction in year-to-year billing that the firm attributed to the hack. The case is still pending. See Complaint, Moses Afonso Ryan Ltd. v. Sentinel Ins. Co., No. 1:17-CV-00157-5-PAS (D.R.I. 2017).

“Hacktivism” was behind the widely reported hack of Mossack Fonseca (“MF”), a Panamanian law firm, in April 2016. MF suffered a hack that affected 2.6 terabytes of data – including 4.8 million email messages and 2.2 million pdfs – and resulted in the disclosure of confidential documents dating from the 1970s through late 2015. As part of this “Panama Papers” hack, the hackers sought to expose high-ranking politicians who had hired the law firm to create offshore companies, which had the effect of avoiding certain taxes. The law firm had not updated its Outlook Web Access login since 2009 or its client login portal since 2013, leaving the firm vulnerable to a cyber-attack that exploited obsolete login protocols. See Matt Burgess and James Tempton, The security flaws at the heart of the Panama Papers, Wired (Apr. 6, 2016). A similar motivation may have been behind the 2016 hack of Appleby, a Bermuda-based law firm that announced some of its data had been “compromised” by a hack. See Appleby, Media coverage of the offshore sector (Oct. 24, 2017).

On October 13, 2016, the U.S. Attorney’s Office for the Southern District of New York charged three Chinese nationals with theft of data from at least two law firms over a period of 18 months. The defendants were accused of hacking into law firm networks and servers, targeting partners who worked on mergers and acquisitions, and buying stock in publicly traded companies that the hacked data revealed were the targets of deals. U.S. Attorney’s Office Southern District of New York, Press Release, “Manhattan U.S. Attorney Announces Arrest of Macau Resident and Unsealing of Charges Against Three Individuals for Insider Trading Based on Information Hacked from Prominent U.S. Law Firms.”

In June 2017, businesses across the globe – including Rosneft, A.P. Moller-Maersk, Merck & Co., Heritage Valley Health Systems, Cadbury, and certain DLA Piper law offices (excluding offices that were segmented from the rest of the firm’s system) – were the victim of a cyber-attack that was dubbed “NotPetya” or “Nyeta” by commentators. Nyeta appears to have originated from a Ukrainian software company that developed accounting software to assist with processing taxes. The company’s servers – which had not been updated since 2013 – were hacked by an employee, permitting a hacker to inject a backdoor into the software and exploit automatic updates of the software to further spread the Nyeta malware. The firm warned that all computers sharing a network with its infected accounting software had been compromised by hackers. See Jack Stubbs and Matthias Williams, How NotPetya’s cyber attack spread from Ukraine, and why it may still be a threat (Oct. 18, 2017).

Simultaneously, other malware called “FakeCry” spread through the software firm’s servers, and was similar to the May 2017 WannaCry ransomware that infected the British National Health Service and over 200,000 systems in 150 countries. Scott, M.E.Doc Servicess Found Responsible for Spreading NotPetya Ransomware (July 7, 2017). WannaCry and Nyeta are both believed to have spread so widely because users had failed to install a Microsoft patch, or installed it incorrectly, or were operating outdated operating systems that were no longer supported by Microsoft. See Robert Hutton et al., Extortionists Mount Global Hacking Attack Seeking Ransom, Bloomberg (May 13, 2017).

“Lawyers should be aware of disclosure risks associated with the transmission of client confidential information by electronic means, and should possess the technological knowledge necessary to exercise reasonable care with respect to maintaining client confidentiality.”

**New York County Ethics Op. 749**
These are just examples of reported hacks in the last two years. They demonstrate that firm or company size, revenue, practice and geography are not predictors of which firms will be targeted by hackers. Moreover, these examples suggest a range of vulnerabilities—failure to install software patches, outdated systems, inadequate insurance, and system accessibility across jurisdictions and extending to outside business partners—that law firms should review and consider addressing to mitigate the firm’s exposure to a cyber-attack.

What Determines the Reasonableness of a Law Firm’s Protective Measures?

Lawyers are not expected to guarantee the security of client information that is transmitted to or by the lawyer. Instead, they are expected to exercise “reasonable care” and employ reasonable protective measures, on a case-by-case basis, to mitigate the risk of disclosure through misdirection or interception. The American Bar Association concluded that the use of unencrypted email remains an acceptable method of attorney-client communication, but noted that with the proliferation of cyber-threats and fact sensitive requirements under the Model Rules, “particularly strong protective measures, like encryption, are warranted in some circumstances.” See ABA Formal Ethics Op. 477R.

“Reasonable care” – the standard of care required to fulfill a lawyer’s duty of technological competence in a specific engagement—will vary depending on (i) the client’s request to implement specific security measures; (ii) the sensitivity of the client’s information; (iii) the client’s risk tolerance for cyber intrusion; (iv) the means by which client information is transmitted; (v) the security measures available to protect the transmissions; (vi) the determination of which information constitutes confidential client information; (vii) the measures taken to protect any transmission of client information to other vendors; and (viii) the training of lawyers and staff in cybersecurity measures and breach response. The challenge for lawyers is establishing security protocols that reasonably protect client data based on the client’s cyber-risk profile, and ensuring that the firm remains vigilant in enforcing and updating its security measures.

How Can Law Firms Meet Their Duty of Technological Competence?

There is no one-size-fits-all approach to law firm data security, nor any requirement that law firms implement every possible security feature and preventive measure currently available in the market. Security measures that may be prudent in a large firm that regularly handles matters requiring the collection of a large volume of personally identifiable information, or that has clients that must comply with DFS cybersecurity regulations or similar, may not be feasible or sensible for a small boutique firm with a different type of law practice. When developing internal data security policies and procedures, law firms should identify measures that will increase the security of client information and meet their client’s specific security needs without compromising the lawyers’ ability to competently represent clients.

Accordingly, although there are a range of cybersecurity measures that a firm could implement, breach response plans that could be formulated, and cybersecurity insurance that could be purchased, there is nothing to suggest that any or all of these measures are reasonably necessary to meet a lawyer’s duty of technological competence in the firm’s particular circumstances. There are, however, general guidelines and steps that each lawyer or law firm should consider.

■ Address pertinent cybersecurity issues in the initial client meeting, and possibly in the engagement letter. For example, if the potential client has requested communications occur through a specific means, use of shared files, or other means of transmitting data electronically during the representation, make reference to that request in the engagement letter and obtain the client’s acknowledgement and consent to the transmission protocols to be used.

■ If the firm has received NIST Framework or ISO 27001 certification or similar, reference the certification in the engagement letter, and consider having the client acknowledge the certification obtained. The NIST Cybersecurity Framework provides a set of industry standards and best practices to manage cybersecurity risks. ISO 27001 provides an international model for creating, operating and maintaining an information security management system. See Phillip Yannella, Law Firms Are Seeking Data Security Certification, Big Law Business (Aug. 19, 2016).

■ Develop policies and procedures governing how information is handled at the firm. Comprehensive information handling procedures should reflect the range of features and protocols defining data management at the firm—including identification of the systems used, archived systems, users, the nature of the information retained, classification of data as it is saved in the firm’s system, pertinent document retention and destruction policies and litigation holds, and storage in other media (e.g., storage in personal devices pursuant to firm “Bring Your Own Device” policies, storage with third-party vendors, and shared drives). This information will help determine reasonable security measures. For example, if the firm regularly receives personally identifiable information or personal health information from its clients, it may wish to segregate those records from other client files.

■ Implement a cybersecurity program (including a breach response plan) to mitigate the threat of a data breach, meet applicable regulatory requirements, and ensure the firm can respond quickly and effectively to a data breach such that it can return to normal functioning and service of clients quickly. The program should include training employees in cyber-hack prevention.

■ Consider whether the firm should invest time and money into a security assessment, penetration testing, or other assessment of the firm’s cybersecurity preparedness, and consider scheduling practice breach response exercises.

■ In multi-office law firms, weigh the costs and benefits of segmenting networks and limiting file access to necessary personnel. Contemplate implementing different layers of access for different segments of the network in order to stem the ability of malware to spread.
Also consider segmentation by employee group (for example, have contract attorneys operate in a limited environment with limited access).

- Obtain appropriate cybersecurity insurance, carefully reviewing coverage triggers and sublimits and the apportionment of coverage between the cyber policy, professional liability policy and any property loss policies. For example, if the cyber coverage broadly excludes claims arising from a failure to render professional services, consider that based on a lawyer's duty to protect a client's confidential information, a data breach could be deemed a failure to fulfill the duty to protect confidential information and arguably excluded under this broad policy language.

- Be vigilant about updating operating systems to ensure that they remain supported, watch closely for patch updates, and deploy fixes immediately and correctly.

A lawyer's duty of reasonable care requires that they consider the security of technology used in their practice. Where a lawyer has a direct or indirect duty to comply with specific cybersecurity measures, the lawyer should identify the client information subject to the enhanced security and consider additional security measures to mitigate the risk of interception and improve the firm's ability to respond if a breach occurs. Moreover, lawyers must consistently assess and reassess their cybersecurity preparedness, particularly as the use of technological applications in their law practices increases and hackers become even more adept at stealing information.
Technology Assisted Review

What's Artificial About Intelligence? The Ethical and Practical Considerations When Lawyers Use AI Technology

By James Q. Walker

The legal profession is constantly changing, often prompted by new technology. Typically lawyers will not adopt new technology until market forces make doing so necessary to effectively represent clients. Under pressure to manage costs and work efficiently, lawyers must continue to adopt smarter and more efficient technological solutions that assist in delivering legal services.

Analytical tools that rely on artificial intelligence-powered software can assist lawyers in a wide range of document-intensive tasks that are critical to negotiating a transaction, conducting an internal investigation, or determining the evidence relevant to the prosecution or defense of a claim. AI uses algorithms to (1) identify and process patterns in data, increasing the accuracy and quality of the identification as more queries are processed (machine-based learning); (2) comprehend and respond to human language patterns (natural language processing); and/or (3) make predictions based on patterns found in sample data (predictive analytics).

In everyday life we are comfortable enjoying the benefits of AI tools: we ask Siri, Alexa, or Google Now to help us find the best nearby diner; we seek service assistance from AI-driven "chatbot" customer service representatives; we use smart home devices to adjust thermostats and lighting; and we trust Spotify, Pandora, and Google Home to select a playlist of songs based on a single request. Yet lawyers are reluctant to integrate AI analytical tools into legal practice, concerned that tools that rely on AI will lead to "artificial" and unreliable results, or may improperly replace a lawyer's professional judgment for computer-manipulated results.

James Walker concentrates his practice in government investigations, complex commercial litigation, professional liability and legal ethics. Mr. Walker represents directors, officers, and lawyers in government and internal investigations of potential criminal, regulatory and/or professional misconduct, and in related criminal and civil litigation and regulatory proceedings. Mr. Walker is the Chair of the New York County Lawyer's Association Professional Ethics Committee, and has served on the New York City Bar's Professional Discipline, Professional and Judicial Ethics, Professional Responsibility, and Securities Regulation Committees, and on the New York State Bar Association Committee on Professional Ethics. He frequently lectures on legal ethics, internal investigations and corporate governance. Mr. Walker also serves as the General Counsel of Richards Kibbe & Orbe LLP.
Intersection of Artificial Intelligence and the Practice of Law

There are AI tools to assist many areas of practice.

1. Contract Review and Analysis

Kira and eBrevia have software that extracts data from contracts to enhance due diligence. Kira can flag particular contract provisions (e.g., cooperation clauses) in a large collection of agreements and generate a “heat map” to show deviations from form. The eBrevia “Contract Analyzer” software converts collections of contracts into searchable text, extracts information based on user specifications, reveals deviations from “playbook,” and classifies documents by language and type.

2. Compliance and Threat Prediction

Several AI applications enable companies to monitor compliance and flag potential threats. For example, NexLP, Inc. offers “Story Engine,” which can review email and other communications in investigations to determine the timeline of key events, identify the participants and the relationships among these key players, and construct the context for communications. RAVN, from iManage, can read large volumes of documents and identify, classify, and extract information quickly and efficiently.

3. Research

ROSS Intelligence has software that permits lawyers to ask a legal research question in natural language, reviews more than a million pages of case law per second, and constructs an answer. ROSS also offers EVA, which analyzes briefs, checks cites, and identifies similar cases.

4. Brief and memo drafting

IBM Watson Debater scans a database (e.g., Wikipedia) for relevant content, identifies the strongest arguments, and constructs arguments on both sides of the issue in natural language.

5. Outcome predictors

Lex Machina applies natural language processing and mines court dockets to predict decision outcomes, favorable jurisdictions in which to bring a lawsuit, and successful motions and arguments before particular judges.

6. E-discovery

Technology assisted review (TAR) provides a means of sorting documents into categories to achieve a more efficient document review. Brainspace reviews documents at rates up to one million per hour and identifies key phrases and clusters in related documents.

The Legal Industry’s Vetting of TAR

TAR’s employment of AI tools is the example most familiar to lawyers, even though lawyers are slow to adopt TAR for even the larger document reviews where it can be most helpful. As with a manual document review, lawyers using TAR first identify the pertinent document custodians and download their documents to a review database to create the “master” collection that will be the source for all future searches.

Rather than relying on a team of temporary attorneys and/or paralegals conducting a manual review of documents that were responsive to search terms, TAR relies on one attorney to guide the review process through interactive testing. The lawyer may use search terms or establish criteria for judgmental sampling to create a seed set. The entire collection of electronically stored information is compared to the seed set. The computer determines a responsiveness score for each document in the ESI collection based on the review algorithm, which tests the similarity of seed set documents to the ESI collection.

The responsiveness metric identifies the success or failure of the TAR. For example, if TAR identifies 100 documents and 90 are responsive, the precision metric is 90 percent; if only 20 are responsive, the precision metric is 20 percent. A low precision metric means the produced documents are highly overinclusive, suggesting the lack of a pattern or a pattern that is not recognizable to the TAR algorithm. Documents that score above the chosen responsiveness threshold are marked as responsive. The lawyer checks the adequacy of the scoring by reviewing a sample of the documents tagged as responsive or unresponsive, and will re-code documents as needed.

This expanded set of attorney-reviewed documents provides the basis for the computer to automatically learn filtering rules, which will be applied to generate a new set of responsiveness scores. This process is repeated until the adequacy is acceptable to the lawyer. The resulting set of documents can be produced, subject to a privilege review.

Alternatively, a firm may wish to do additional quality control prior to production, possibly sampling the responsive and non-responsive documents and running manual searches over those populations to exclude individual documents or document categories that may have been missed in the review process. Computer-assisted review can substantially reduce the number of attorneys and paralegals involved in the review process.

Litigants have challenged the accuracy of TAR algorithms or argued that the seed set was not representative of the entire ESI collection, but several factors typically weigh heavily in favor of the conclusion that TAR satisfies the “reasonable inquiry” standard under Fed. R. Civ. P. Rule 26(g). See Timothy T. Lau and Emery G. Lee III, Federal Judicial Center, Technology-Assisted Review for Discovery Requests: A Pocket Guide for Judges 6 (2017).

- With a sufficiently large volume of documents, “reasonable inquiry” is satisfied if the responding party is enabled to produce a higher volume of responsive material more quickly than otherwise would be possible, especially if the cost of the production is substantially lower because of the need for fewer attorney reviewers.

- The larger the review, the more likely that humans faced with the monotonous task of reviewing thousands of documents electronically will make errors. By comparison, the computer never tires of reviewing thousands of documents, and is consistent in its approach.

- The scientific approach to TAR, which involves iterative quality-checking of search results to establish the responsive document set, compares favorably to a document-by-document manual review, where quick and possibly inconsistent judgments are made by multiple reviewers.
Indeed, courts have consistently lauded the advantages of TAR (or predictive coding) over manual review. See, e.g., Winfield v. City of New York, 15-CV-05236 (LTS)(KHP), 2017 BL 423037, at *5 (S.D.N.Y. Nov. 27, 2017) (court ordered TAR, which “hasten[ed] the identification, review, and production” of responsive documents and allows parties to “prioritize and/or categorize documents for purposes of document review and has been shown to produce more accurate results than manual review.”); Rabin v. PriceWaterHouseCoopers LLP, Case No. 16-cv-02276-JST, 22017 BL 277017, at *2 (N.D. Cal. Aug. 8, 2017) (court accepted respondents’ argument that “TAR process is capable of achieving an exceptionally high level of accuracy” and that its use would expedite discovery); In re Actos (Pioglitazone) Products Liability Litig., 274 F. Supp. 3d 485, 499 (W.D. La. July 17, 2017) (court noted that “[d]espite the initial ‘front loaded’ investment of time, although not perfect or fully realized, [predictive coding] provided an innovative efficiency to the discovery process when compared to the existing, prevailing methods of review.”); Hykes v. New York City, 10 Civ. 3119 (AT)(AJP), 2016 BL 248010, at *2 (S.D.N.Y Aug. 1, 2016) (concluded that generally TAR is “cheaper, more efficient and superior to keyword searching”); see also Maura R. Grossman & Gordon Cormack, Technology – Assisted Review in E-Discovery can be more Effective and More Efficient Thank Exhaustive Manual Review, XVII Richmond J. L. & Tech. 1, 37 (2011) (observed that manual reviews identified 25 to 80 percent of responsive documents, and TAR identified 67 to 86 percent of responsive documents).

At the same time, the benefits of TAR should not be exaggerated. As the first court that validated the use of predictive coding cautioned, predictive coding is neither required nor appropriate in all cases. Da Silva Moore v. Publicis Groupe & MSL Grp., 287 F.R.D. 182, 193 (S.D.N.Y. 2012) (magistrate judge’s ruling), adopted by 2012 BL 101971 (S.D.N.Y. Apr. 26, 2012).

Moreover, neither manual review nor TAR should be expected to achieve perfection. Judge Denise Cote, after permitting a defendant to use predictive coding over the plaintiff’s objection, made the following observation:

“...the production of documents in litigation ... is a herculean undertaking, requiring an army of personnel and the production of an extraordinary volume of documents. Clients pay counsel vast sums of money in the course of this undertaking, both to produce documents and to review documents received from others. Despite the commitment of these resources, no one would or should expect perfection from this process.” Federal Housing Finance Agency v. HSBC North America Holdings, 2014 BL 40542 (S.D.N.Y. Feb. 14, 2014).

Indeed, TAR cannot displace lawyers in the discovery process because a lawyer’s professional judgment is a necessary part of the TAR review. Attorneys must classify the sample of documents and provide the parameters for the computer’s search. Lawyers who understand the case, the implicated documents, and technology-assisted review must select the most appropriate protocols for the review and may need to defend those choices in court. If a pertinent document custodian is vague or uses coded language in emails discussing a topic of interest, a lawyer will need to correct the review by training the computer on a sample of responsive documents. Finally, the typical algorithm assigns each document a probability of responsiveness. Lawyers may have to hand-classify documents for which the responsiveness probability is too low.

The Ethics of Using AI Software in Legal Practice

The ethics rules support reliance on vendors who supply AI tools to assist in the practice of law provided that the tools are compatible with a lawyer’s professional obligations and assist lawyers to competently represent their clients. In 2012, Comment 3 to ABA Model Rule 5.3 was amended to acknowledge that lawyers “may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client” provided that the lawyer “make[s] reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer’s professional obligations.” Cmt. 3, ABA Model Rule 5.3. Ethics opinions and rule changes have made plain that a lawyer’s duty of competence in a client representation extends to the technology used in a representation. See New York County Ethics Op. 749 (2017); ABA Model Rules of Professional Conduct, Rule 1.1; see also ABA Commission on Ethics 20/20 Report (“in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology”); Erika Kubik, Tennessee Becomes 27th State to Adopt Ethical Duty of Technology Competence (Mar. 22, 2017).

Moreover, Comment 8 to Rule 1.1 provides that “[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology” (emphasis added). The practical significance of this duty is two-fold: lawyers have an affirmative duty (1) to be proficient in the technology they use in the representation of a client (either directly or through those who assist in the representation); and (2) to consider technological advances that may improve the professional services they provide to their clients. The first requires that lawyers who use technology during a client representation (e.g., produce documents using a discovery vendor’s search and storage software) understand the technology well enough to ensure compliance with the lawyer’s ethical duties. Lawyers must also supervise nonlawyers who are involved in e-discovery, and they remain liable for e-discovery vendor errors. See In Re Seroquel Products Liability Litig., 244 F.R.D. 648 (M.D. Fla. Aug. 21, 2007) (a party is responsible for the errors of its vendors, citing Sedona Principle 6: “Ultimate responsibility for ensuring the preservation, collection, processing, and production of electronically stored information rests with the party and its counsel, not with the nonparty consultant or vendor.”). Thus, if a lawyer uses AI in her legal practice, the lawyer must either directly possess the competence to use the technology or hire competent vendors, in which event the lawyer must conduct sufficient due diligence before hiring the vendor and during the vendor relationship.

The second leg of the duty suggests that a lawyer has an ethical responsibility to consider whether she may provide better service using technological tools—including AI software. Currently there may be no instance in which AI software represents the standard of care in an area of legal practice such that its use is necessary to a representation. See, e.g., New York Ethics Op. 1053
(2015) ("if a lawyer needs a sign language interpreter to communicate effectively with a client, then, unless the lawyer utilizes such an interpreter, the lawyer would be unable to provide 'competent representation' to the client, as required by Rule 1.1."). A lawyer has an affirmative duty, however, not only to determine if certain technology is necessary to a client representation, but also to consider whether technological tools will improve service to the client.

Assessing When AI Tools Should be Used in Legal Practice

AI technology and other new technology has already allowed lawyers to provide more efficient services to their clients in several ways. Legal research that previously took days may be accomplished in hours, and large computer networks and files may be reviewed in a fraction of the time. Innovations have reduced, and will continue to reduce, the overall number of lawyers and staff necessary to review and process documents critical to each engagement.

Lawyers can assess whether to use AI tools or other technology by considering the following questions:

1. Is the technology recognized in the industry as a means of facilitating the pertinent aspect of practice?

2. Is the technology priced competitively as compared to manual or old software approaches?

3. Is the technology easily supported by current technology at the firm or will the firm need to invest in outside technology support, and if so, is the outside technological support cost-effective?

4. Is there a foreseeable benefit to the client based on the cost, scope, accuracy, efficiency, or some other important factor relevant to the specific project?

5. Does the new technology have the potential to create greater efficiencies in the management of the workstreams?

Conclusion Use of AI tools and other new technology in legal practice is ethically appropriate and eventually may be required in order for a lawyer to discharge her duty of competence and remain abreast of relevant technology. Lawyers remain responsible for determining when AI tools should be used in their practice, and ensure that such usage is appropriately supervised. Clients may begin to require the use of these tools to reduce costs. Use of AI technology will free lawyers from more routine tasks and focus them on issues requiring professional judgment – those areas of practice that remain squarely in the lawyer's domain.