By Daniel A. Cotter

Technology and Data Security

The Use of Technology by Lawyers and the Rules of Professional Conduct

Like everyone else, lawyers live in an environment where technology is constantly evolving. Attorneys and firms are increasingly the targets of hacking and phishing scams, and some law firms have been sued, facing allegations that the firms' data security practices were insufficient to protect confidential client information. On October 15, 2015, the Illinois Supreme Court amended Rule 1.6(e) of the Illinois Rules of Professional Conduct ("RPC") to require that lawyers make reasonable efforts to prevent unauthorized access to client data, and imposing an affirmative duty on lawyers to understand the relevant technology.

This article discusses some of the relevant rules of professional conduct, recent changes to those rules, and some considerations for lawyers in protecting their clients' and firms' data in specific areas of technology usage. On April 4, 2016, the Office of Court Administration for the New York State Unified Court System released amendments proposed by the New York State Bar Association to the New York Rules of Professional Conduct, which would make the New York RPCs consistent with both the ABA Model Rules and the Illinois RPCs.

Relevant RPCs for Illinois Lawyers

The Illinois RPCs contain a number of rules that affect an attorney's obligations of confidentiality and security of information, including Illinois Rule 1.1 (Competence) and Illinois Rule 1.6 (Confidentiality of Information).

The duty of competence under Illinois Rule 1.1 includes competence in the selection and use of technology. Comment 8 to Illinois Rule 1.1 provides:

> 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.

Lawyers should understand the risks presented when they access data through practices such as cloud computing or "bring your own device" ("BYOD") policies, and when their acceptance of credit card payments may involve confidential client information.

Illinois Rule 1.6(e) was amended on October 15, 2015 (with an effective date of January 1, 2016) to adopt the ABA Model Rules change already in place and incorporate into the RPC an affirmative requirement for Illinois lawyers to guard against inadvertent or unauthorized disclosure. Rule 1.6(e) provides:

> (e) 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.

(Emphasis added.)

Comment 18 to Illinois Rule 1.6 was also amended and substantially revised, providing in pertinent part (tracked changes kept to reflect the extent of the changes to the comment):

> [18~~6~~] Paragraph (e) requires a ~~A~~ lawyer ~~must~~ 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 (e) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal

laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Finally, Comment 19 to RPC 1.6(e) directly addresses the use of technology, providing:

> [19] When *transmitting* a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, *does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions.* Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the *sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.* 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

(Emphasis added.)

What measures are "reasonable" will depend on the facts and circumstances facing a particular lawyer or law firm, including the types of information collected and the cost of employing such additional safeguards.

A lawyer must also keep in mind a number of other RPCs when considering the security of client sensitive or confidential information. Rule 1.15(a) requires that a lawyer safeguard client property (including data) even after termination of representation under RPC 1.16(d). An attorney also has an obligation to supervise third party vendors providing technology services, including the vendor's storage and backup of data in the cloud. Finally, a lawyer has an obligation to warn clients about the risk of using electronic communications where there is a significant risk that a third party may gain access.

The New York Amendments

The New York Unified Court System recently issued its request for public comments to proposed amendments to the New York RPCs. The proposed amendments include changes to New York Rule 1.6(c) that would require lawyers to make "reasonable efforts" to safeguard confidential information, making the language substantially identical to the amended Illinois Rule 1.6(e) by converting the New York RPC 1.6(c) to an affirmative duty. New comments to New York RPC 1.6(c) (if the amendment is adopted) also are consistent with Illinois Comment 18 to Illinois Rule 1.6(e).

Practical Considerations–Encrypting Emails

One issue to consider with the revised Illinois rules and accompanying comments is whether attorneys are required to encrypt emails containing client data. With one exception, no bar association (including the American Bar Association) has addressed the question in some time. This may change in the near future.

Encryption of emails generally can take place at two stages: 1) data at rest and 2) data in transit. Data at rest is data that is stored physically in any digital form that is located within the lawyer's control and once transmitted to the client, in the client's control. Data in transit is data that is flowing over the Internet or within the confines of a privacy network such as a Local Area Network ("LAN"). Encrypting data in transit provides some protection from being obtained by unintended third parties, but hackers will still have an ability to hack into the data at rest.

The Illinois State Bar Association considered the question of sending unencrypted emails in ISBA Advisory Opinion 96-10 (reaffirmed in 2010), available at https://www.isba.org/sites/default/files/ethicsopinions/96-10.pdf, which advised that unencrypted email is acceptable:

> Because (1) the expectation of privacy for electronic mail is no less reasonable than the expectation of privacy for ordinary telephone calls, and (2) the unauthorized interception of an electronic message subject to the [Electronic Communications Privacy Act].

The Electronic Communications Privacy Act was passed by the United States Congress in 1986 and was designed to prohibit access to stored electronic communications and to prevent the unauthorized access by government to private electronic communications. The ABA concluded similarly to the ISBA, in Formal

Opinion No. 99-413, issued on March 10, 1999 (available at http://cryptome.org/jya/fo99-413.htm) that:

> 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.
>
> Although earlier state bar ethics opinions on the use of Internet e-mail tended to find a violation of the state analogues of Rule 1.6 because of the susceptibility to interception by unauthorized persons and, therefore, required express client consent to the use of e-mail, more recent opinions reflecting lawyers' greater understanding of the technology involved approve the use of unencrypted Internet e-mail without express client consent.

Both of the above-referenced opinions were issued in the late 1990s. Since that time, privacy and data laws on various levels have been passed, including Gramm-Leach Bliley, HIPAA, and Sarbanes-Oxley on the federal level. Accordingly, some in the legal arena, including Catherine Sanders Reach, Director, Law Practice Management & Technology at the Chicago Bar Association, have recommended that the ABA revisit its 1999 ethics opinion. At the very least, given the changed RPCs and the need to try to prevent unauthorized access to client information, lawyers should revisit encryption of emails and determine whether it makes sense to consider requiring encryption both for data at rest and data in transit.

While most state bar ethics opinions relevant to the attorney email question date to the late 1990s, the State Bar of Texas recently revisited the issue. Texas Opinion 648, available at http://legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648.aspx, reaffirmed that email may continue to be used for communicating with clients, but that "some circumstances" may require the lawyer to advise her client "regarding risks incident to the sending or receiving of emails" and "to consider whether it is prudent to use encrypted email or another form of communication." Given the changes to the Model Rules and the amendments being adopted by states such as Illinois and Texas, lawyers should assess encryption of their emails.

Practical Considerations–Use of Public Wi-Fi

Another consideration for lawyers to address is the use of public Wi-Fi. Lawyers who travel or are out of the office frequently may be tempted to use the public Wi-Fi offered in airport lounges, hotels, or coffee shops. In light of the Illinois RPCs, including the comments revisions, lawyers should revisit this issue as well. Not many ethics opinions have been issued to date in this area, but given the changing technology and the reality that lawyers are increasingly the targets of hacking and phishing scams, lawyers should make sure they understand the technology and consider more secure alternatives.

The Standing Committee on Professional Responsibility and Conduct of the State Bar of California (The "Standing Committee") issued Formal Opinion No. 2010-179, available at http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=837, 2010 to address the question. The Standing Committee determined that use of public Wi-Fi presented security risks when used without other technologies, concluding:

> With regard to the use of a public wireless connection, the Committee believes that, *due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection* at the coffee shop to work on Client's matter *unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.* Depending on the sensitivity of the matter, Attorney may need to *avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use* of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client

Illinois Lieutenant Governor to Keynote Alliance for Women Kick-Off

Join the Alliance for Women at their annual kick-off reception on Wednesday, October 5, 2016, from 5:00-7:00 p.m., at the CBA Building, 321 S Plymouth Court. Lieutenant Governor Evelyn Sanguinetti will be the guest speaker. Thank you to our generous sponsor Schiff Hardin. RSVP at www.chicagobar.org.

About Evelyn Sanguinetti

Evelyn Sanguinetti (born in Miami, Florida) is the 47th and current Lieutenant Governor of Illinois. Sanguinetti is the first Hispanic and first Latina lieutenant governor in Illinois history. Before becoming lieutenant governor, Sanguinetti served as a member of the Wheaton City Council, was an assistant attorney general under former Illinois Attorney General James E. Ryan, and practiced at a private law firm in Chicago. She has also worked as an adjunct professor at John Marshall Law School, her alma mater.

> privilege or work product protections, and seek her informed consent to do so.

(Emphasis added.)

The Standing Committee also addressed the question of a lawyer using her laptop or accessing data while on her personal wireless system at home. The Standing Committee advised that the attorney will not violate her duties of confidentiality and competency if the personal wireless system "has been configured with appropriate security features."

One challenge of public Wi-Fi is that hackers are using Wi-Fi "pineapples" and other tools to intercept key strokes, obtain passwords, and gain access to unsuspecting users' data. Many hackers are creating Wi-Fi connections that appear to be the Wi-Fi provided by the hotel, coffee shop or other provider, but are set up to easily obtain data of those using the connection. Lawyers should consider the issues raised by the California Standing Committee and whether public Wi-Fi affords them a "reasonable expectation of privacy." One way to address the issue is through the use of services such as Citrix to provide an enhanced layer of protection to the lawyer and law firm.

Practical Considerations–Using the Cloud

As noted above, Comment 8 to Rule 1.1 of the Illinois RPCs requires lawyers to understand the risks and benefits of technology, including the use of the cloud. Cloud computing is the Internet-based computing that provides shared computer processing and storage resources. A number of ethics opinions have looked at the issue and have generally found that with appropriate safeguards and consideration, lawyers may store their data with an offsite third party vendor.

For example, the ISBA issued Opinion No. 10-01 in July 2009, available at https://www.isba.org/sites/default/files/ethicsopinions/10-01.pdf, addressing the issue and concluding:

> [A] law firm may retain or work with a private vendor to monitor the firm's computer server and network, either on-site or remotely, and may allow the vendor to access it as needed for maintenance, updating, troubleshooting and similar purposes. Before doing so, however, the law firm must take reasonable steps to ensure that the vendor protects the confidentiality of the clients' information on the server.

As with the opinions on encryption and use of public and private Wi-Fi, the opinions on cloud computing are dated. Given the ongoing technological advances relating to cloud computing, the ABA and other state bars may also revisit this issue, especially in light of the changing rules of professional conduct and the imposition of affirmative duties upon lawyers to understand and be conversant in technology relating to client information.

Conclusion

As technology changes, lawyers' obligations to protect client information continue to evolve. The ABA and state bars have yet to opine on many of the issues relating to the use of technology by lawyers and whether attorney and firm practices violate the rules of professional conduct. Lawyers must review their firm's policies and practices and make "reasonable efforts" in their information security practices to "keep abreast of changes in the law and its practice." Illinois and other states RPCs impose affirmative duties on lawyers to take steps to ensure security of client data. Failure to take reasonable steps to ensure data safety and to understand the relevant technology may result in an ethical violation or lawsuit for an unsuspecting lawyer. ■

Daniel A. Cotter is a Partner at Butler Rubin Saltarelli & Boyd LLP, where he chairs the Insurance Regulatory and Transactions practice and is a member of the Cyber and Privacy practice, and is a member of the **CBA Record** *Editorial Board.* *Special thanks to CBA Director of Legal Practice Management, Catherine Sanders Reach, for her discussions with me in the privacy arena.*

Numerous ethical opinions relevant to the topic of cloud computing include:

- ISBA Ethics Op. 10-01 (July 2009)
- Pennsylvania Formal Opinion 2011-200
- North Carolina 2011 Formal Op. 6
- New York State Bar Ethics Opinion 842
- Alabama Ethics Opinion 2010-2
- Washington State Bar Advisory Opinion 2215
- Iowa Bar Ethic Opinion 11-01
- Vermont Ethics Opinion 2010-6
- Massachusetts Bar Ethics Opinion 12-03
- New Hampshire Ethics Committee Advisory Op. #2012-13/4