Technology Competence, Cybersecurity, Blogging, "Self-Defense, and When Does Client Information Become "Generally Known"

Annual Bench and Bar CLE
June 26, 2019

Technology Competence

Formal Statutory and Ethical Opinion Guidance:

> The Kentucky Rules of Professional Conduct, together with interpretations of relevant Professional Ethics Rules through the Formal Ethics Opinions of the Kentucky Bar Association and the American Bar Association, provide a guidance in compliance with electronic communications and electronic storage of client files and materials.

Technology Competence Is Now Required In the Practice of Law:

SCR 3.130 (Rule 1.1):

> **Competence**
>
> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Supreme Court Commentary 1990

> **Maintaining Competence**
>
> [6] To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances.

"Ethics 2000" Review and the 2009 Amendments[1]

> Comment:

[1] Order of Kentucky Supreme Court No. 2009-05, effective July 1, 2009. The 2009 Amendments also used the "Comment" in place of "Supreme Court Commentary", but "Supreme Court Commentary" still is used in published sources and in the later Orders.

Maintaining Competence

(6) To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Maintaining Competence

(6) To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education~~. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances.~~ and comply with all continuing legal education requirements to which the lawyer is subject.

Kentucky Supreme Court Order 2017-18, effective January 1, 2018:

Maintaining Competence

(6) 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 to newly adopted language in Comment 6.)

Relevant Formal Opinions include:

1. Kentucky Bar Association:
   a. KBA Ethics Opinion 446, "*Cybersecurity*", July 20, 2018;
   b. KBA Ethics Opinion 437, "*Use of Cloud Computing*", March 21, 2014;
   c. KBA Ethics Opinion 434, "*Ethical Considerations Relating to a Lawyer's Use of Social Network Sites to Benefit a Client*", November 17, 2012;
   d. KBA Ethics Opinion 403, "*Use of electronic mail services to Communicate With Clients*", March 1998.

2. American Bar Association:
   a. ABA Formal Opinion 483, "*Lawyers' Obligations After an Electronic Data Breach or Cyberattack*",
   b. ABA Formal Opinion 477R, "*Securing Communication of Protected Client Information*", May 11, 2017, Revised May 22, 2017;
   c. ABA Formal Opinion 99-413, "*Confidentiality Obligations for E-mail Communications with Clients*, March 10, 1999.

What does "including the benefits and risks associated with relevant technology," mean to the practicing bar?

From the Field Examples:

A. Spam Filters/Junk Mail:

Emerald Coast Util. Auth. v. Bear Marcus Pointe, LLC, 227 So. 3d 752 (Ct. App. Fla. 2017): Court issued opinion awarding $600,000 in fees against a party that was not discovered because the spam filter rejected the email. The Court of Appeals held the law firm "made a conscious decision to use a defective email system without any safeguards or oversight in order to save money. Such a decision cannot constitute excusable neglect." *Id*. at 757.

The Court went on to state:

> Counsel has a duty to have sufficient procedures and protocols in place to ensure timely notice of appealable orders. This includes use of an email spam filter with adequate safeguards and independent monitoring of the court's electronic docket. In cases where rendition of an appealable order has been delayed for a significant period of time, it might also include the filing of a joint motion for a case management conference to ensure that the order has not slipped through the cracks.

Pace v. United Services Automobile Association, No. 05-cv-01562-LTB-MJW, 2007 U.S. Dist. LEXIS 49425; 2007 WL 2022059 (D. Colo. July 9, 2007). Plaintiff's counsel failed to appear at a court ordered settlement conference because the newly installed (but not properly configured) "Barracuda Spam Firewall Whitelist" determined the ECF emailed order was spam. The Court awarded the fees and expenses of the other counsel as a sanction, stating:

> It is incumbent upon attorneys to adopt internal office procedures that ensure the court's notices and orders are brought to their attention once they have been received. *In re Schlosser*, 100 B.R. 348, 350 (Bankr. S.D. Ohio 1989); *Greene v. Union Mut. Life Ins. Co.*, 102 F.R.D. 598, 603 (D. Maine 1984). This is just as true in these days of electronic noticing as it was when documents were sent by first class mail. *To rely on procedures that treat the court's electronic notices as the functional equivalent of junk mail is not acceptable. Furthermore, it is counsels' responsibility to monitor the progress of their cases and the court's docket*

Slip Op. at 9-10 (emphasis added).

Can't happen to me? Consider:

> *See Yeschick v. Mineta*, 675 F.3d 622, 629-30 (6th Cir. 2012)—affirmative duty to check the electronic docket. Email issues are not an excuse.

CR 5.02(2) Election to receive service of documents from other counsel by email;

U.S. Bankruptcy Court practice;

Federal e-FILING—(CM-ECF).

B. "Reply All" Email—What if the sender shows a copy to his/her client?

KBA Ethics Opinion 442, "*Email Replies*", November 17, 2017:

If a lawyer (Lawyer A) sends an email to another lawyer (Lawyer B), who is not affiliated with Lawyer A, and copies Lawyer A's client by using "cc," Lawyer B should not correspond directly with Lawyer A's client by use of the "reply all" key. A lawyer who, without consent, takes advantage of "reply all" to correspond directly with a represented party violates Rule 4.2. Further, showing "cc" to a client on an email, without more, cannot reasonably be regarded as consent to communicate directly with the client.

SCR 3.130 (Rule 4.2):

Communication with person represented by counsel.

In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order**.**

C. Redaction—Is it really redacted?

1. **Suppose you use Adobe Acrobat for redaction, marked, but fail to "apply redactions"; or**
2. **Suppose you use a marker, but the copying picks up and reproduces the redacted language.**
3. **Suppose, etc.—use your imagination.**

Consider SCR 3.130(Rule 4.4)

Respect for rights of third persons.

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) *A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall:*

(1) *refrain from reading the document*,

(2) promptly notify the sender, and

(3) abide by the instructions of the sender regarding its disposition.

(Emphasis Added)

Comment 2. Paragraph (b) recognizes that lawyers sometimes receive *documents or other communications that were mistakenly sent or produced by opposing parties* or their lawyers. If it is clear from the circumstances that the document was not intended for the receiving lawyer, that lawyer must avoid reading the substance of the communication, notify the sender of the mistake, and comply with any reasonable request of the sender, allowing for protective measures (e.g. returning to sender, deleting or otherwise destroying the communication). The question whether the privileged status of such a document has been waived is a matter of law beyond the scope of these Rules. Similarly, this Rule does not address the legal duties of a lawyer who received a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person. For purposes of this Rule, "document" includes e-mail or other electronic modes of transmission subject to being read or put into readable form. (Emphasis Added)

D. "I Don't Want An Email Address"

Retired lawyer, had not represented clients in many years, but a compulsory email address rule was in effect:

In re Collie, 406 S.C. 181, 749 S.E.2d 522 (2013):

> Although the attorney may have considered herself retired from the practice of law since she had not represented clients in many years, she was nevertheless classified as a regular member of the South Carolina Bar and, therefore, pursuant to S.C. App. Ct. R. 410(g), was required to provide a valid email address;
>
> The attorney repeatedly refused to comply with the explicit directives, orders, and rules of the court and of requests by the clerk of court by refusing to maintain and monitor an operational email account;
>
> *The attorney posed a substantial threat of serious harm to the public and to the administration of justice*;
>
> Pursuant to S.C. App. Ct. R. 413:17(b) and (c), the attorney was placed on interim suspension**.**

(The attorney had sent her responses relating to the disciplinary proceeding to the Supreme Court by facsimile.)

E. "I don't (want to) (can't) use computers and email for court filings"

State ex rel. Okla. Bar Ass'n v. Oliver, 2016 OK 37, 369 P.3d 1074 (2016)

Lawyer had been practicing law since 1967; had practiced before the bankruptcy courts for twenty-eight to thirty years; was admitted in the Eastern, Western, and Northern districts of the federal court, and the U.S. Tax Court--no previous complaints or disciplinary actions.

Lawyer acknowledged that his problems with the bankruptcy court were caused by his lack of expertise in computer skills and his frustration in trying to meet the federal court's expectations with electronic pleading requirements. No testimony nor any documents showed an insufficiency in the lawyer's knowledge of substantive bankruptcy law.

The bankruptcy judge gave the lawyer a brief suspension, gave him "homework", and then informed him of the errors that he made in filing nine "homework" documents that she had assigned to him.

The lawyer stated he had an attorney friend who would be willing to assist him with all of the filings for the next few weeks. The judge gave him 30 days to "have a lawyer on board," and one who was well-versed in the local rules and guidelines, but the lawyer had to "resubmit the homework without any errors, neither rules errors nor even any typographical errors."

The judge memorialized her instructions from the show cause hearing. In her instructions he was required to refile the nine documents he previously presented, which had to be "error free." She ended that paragraph with the sentence, "In doing so, [the lawyer] may not seek or obtain assistance from this Court's law clerk, the staff of the Court Clerk's office or any other person." The next paragraph requires him to file a document certified under oath from a bankruptcy attorney agreeing to associate with [the lawyer] and assist him in the preparation and filing of "documents with this Court" and that he or she was well versed in the Local Rules and Guidelines of the court and the Federal Rules of Bankruptcy Procedure.

Final outcome: Permanent disbarment from the bankruptcy court and public censure by Oklahoma Supreme Court for failure to report discipline and for failure to learn the system in which he practiced.

F. "I don't want to learn"

Corporate Counsel, in response to inadequate discovery search told the Court:

"I have to confess to this Court, I am not computer literate. I have not found presence in the cybernetic revolution. I need a secretary to help me turn on the computer. This was out of my bailiwick."

James v. National Financial. LLC, 2014 Del. Ch. LEXIS 254 *; 2014 WL 6845560.

Cybersecurity

I. Outline of Formal Statutory and Ethical Opinion Guidance:

A. "*Whether an attorney uses email to communicate with clients; e-files documents with the courts; stores client information electronically; shares files with others; employs mobile devices and/or accesses the internet, care must be taken to avoid disclosure of confidential client information*."

KBA Ethics Opinion 446 (Emphasis Added).

B "'At the beginning of the client-lawyer relationship, *the lawyer and the 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 communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required.*'"

KBA Ethics Opinion 446 *quoting* ABA Formal Opinion 477R at 7. (Emphasis Added).

C "Due to the constant changing of technology, it is impossible to give specific requirements of what constitutes 'reasonable efforts' by an attorney to prevent cybersecurity breaches. *What is 'reasonable' depends upon the facts and circumstances taken to prevent access or disclosure of confidential information*."

KBA Ethics Opinion 446. (Emphasis Added).

Comment 18 to Model Rule 1.6 provides some guidance[2]:

[2] Comment 18 to Model Rule 1.6 has not been adopted in Kentucky. The corresponding commentary to SCR 3.130(Rule 1.6) is Comment 15 which reads:

> 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.* (Emphasis added.)

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).

D "SCR 3.130(1.4) does not mandate the disclosure to a client about general cyber attacks against the law firm, or breaches of security within an attorney's computer systems. However, if there is a disclosure of the client's specific confidential and/or privileged information to third parties, which we believe would constitute a 'significant development' affecting the client's representation, then a disclosure must be made to the client about this development."

KBA Ethics Opinion 446.

E "Due to the rapid change of cybersecurity options, an attorney may determine that taking 'reasonable measures' to avoid a theft or loss of confidential client information includes contracting with a professional to create and/or maintain the cybersecurity plan for the law firm. "When a lawyer selects a provider of any support services, the duty of competence, the duty to protect a client's property, and the duty of confidentiality require the lawyer to investigate the qualifications, competence and diligence of the provider. *A lawyer who does not investigate whether a warehouse he or she is considering for the storage of files had adequate security to safeguard client files fails in his or her confidentiality and competence obligations to the client. Likewise, an attorney selecting an online provider of storage or other services must investigate the provider to be sure that client information is reasonably sure to remain confidential and secure.*"

KBA Ethics Opinion 446 *quoting* ABA Formal Opinion 477R at 9. (Emphasis Added).

II. KRS §365.732. Notification to affected persons of computer security breach involving their unencrypted personally identifiable information:

(1) As used in this section, unless the context otherwise requires:

(c) "Personally identifiable information" means an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted:

1. Social Security number;

2. Driver's license number; or

3. Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account

III. Neither the Kentucky Rules of Professional Conduct, nor the Formal Ethics Opinions of the Kentucky Bar Association and the American Bar Association "mandate the specific policies or procedures that an attorney must employ to have an effective data security program, nor does it contend that there is a 'one shoe fits all' solution for every attorney for cybersecurity."

[E]ach attorney must understand what devices the law firm uses that are connected to the office network or the internet; *how client information is exchanged or stored through that system and who has access to the data, and make 'reasonable efforts' to combat cyber threats.* An attorney's policies will thus depend upon an attorney's use of electronics; the method used to communicate with clients and the nature of the client's information. "These requirements are as applicable to electronic practices as they are to comparable office procedures."

> KBA Ethics Opinion 446 *quoting* ABA Formal Opinion 477R at 7. (Emphasis Added).

SCR 3.130 (Rule 1.1):

Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

SCR 3.130 (Rule 1.4):

Communication.

(a) A lawyer shall:
(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;
(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;
(3) keep the client reasonably informed about the status of the matter;
(4) promptly comply with reasonable requests for information; and
(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.
(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

SCR 3.130 (Rule 1.6(a))

Confidentiality of information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
(b) * * * *

Relevant Formal Opinions include:

Kentucky Bar Association:

KBA Ethics Opinion 446, "*Cybersecurity*", July 20, 2018;

KBA Ethics Opinion 442, "*Email Replies*", November 17, 2017;

KBA Ethics Opinion 437, "*Use of Cloud Computing*", March 21, 2014;

KBA Ethics Opinion 403, "*Use of electronic mail services to Communicate With Clients*", March 1998.

American Bar Association:

ABA Formal Opinion 483, "*Lawyers' Obligations After an Electronic Data Breach or Cyberattack*";

ABA Formal Opinion 480, "*Confidentiality Obligations for Lawyer Blogging and Other Public Commentary*" March 6, 2018;

ABA Formal Opinion 477R, "*Securing Communication of Protected Client Information*", May 11, 2017, Revised May 22, 2017;

ABA Formal Opinion 99-413, "*Confidentiality Obligations for E-mail Communications with Clients*, March 10, 1999.

When Does Client Information Become "Generally Known"?

Formal Opinion 479, December 15, 2017

The "Generally Known" Exception to Former-Client Confidentiality

A lawyer's duty of confidentiality extends to former clients. Under Model Rule of Professional Conduct 1.9(c), a lawyer may not *use* information relating to the representation of a former client to the former client's disadvantage without informed consent, or except as otherwise permitted or required by the Rules of Professional Conduct, unless the information has become "generally known."

The "generally known" exception to the duty of former-client confidentiality is limited. It applies (1) only to the use, and not the disclosure or revelation, of former-client information; and (2) only if the information has become (a) widely recognized by members of the public in the relevant geographic area; or (b) widely recognized in the former client's industry, profession, or trade. *Information is not "generally known" simply because it has been discussed in open court, or is available in court records, in libraries, or in other public repositories of information.*

1. **Model Rule 1.9(c)(2) governs the *revelation* of former client confidential information;**

2. **Model Rule 1.9(c)(1) addresses the *use* of former client confidential information.**

3. **ABA Formal Opinion 479 addresses the "generally known" exception to Model Rule 1.9(c)(1)**

What Does It Mean to be "Generally Known"?

1. Most of us would equate "generally known" with "public record"

Restatement 3d of the Law Governing Lawyers, §59

Definition of "Confidential Client Information"

Confidential client information consists of information relating to representation of a client, other than information that is generally known.

Comment d:

Generally known information. ***Confidential client information does not include information that is generally known***. Such information may be employed by lawyer who possesses it in permissibly representing other clients (see § 60, Comments g & h) and in other contexts where there is a specific justification for doing so (compare Comment e

hereto). Information might be generally known at the time it is conveyed to the lawyer or might become generally known thereafter. At the same time, the fact that information has become known to some others does not deprive it of protection if it has not become generally known in the relevant sector of the public.

Whether information is generally known depends on all circumstances relevant in obtaining the information. ***Information contained in books or records in public libraries, public-record depositaries such as government offices, or in publicly accessible electronic-data storage is generally known if the particular information is obtainable through publicly available indexes and similar methods of access***. Information is not generally known when a person interested in knowing the information could obtain it only by means of special knowledge or substantial difficulty or expense. Special knowledge includes information about the whereabouts or identity of a person or other source from which the information can be acquired, if those facts are not themselves generally known.

A lawyer may not justify adverse use or disclosure of client information simply because the information has become known to third persons, if it is not otherwise generally known. Moreover, if a current client specifically requests that information of any kind not be used or disclosed in ways otherwise permissible, the lawyer must either honor that request or withdraw from the representation (see § 32; see also §§ 16(2) & 21(2)).

[Emphasis Added]

2. ABA Op. 479 rejects that standard out of hand.

"A number of courts and other authorities conclude that information is not generally known merely because it is publicly available or might qualify as a public record or as a matter of public record**.**

The opinion cites several examples at footnote 6 including;

See, e.g., Pallon v. Roggio, Civ. A. Nos. 04-3625(JAP), 06-1068(FLW), 2006 WL 2466854, at *7 (D. N.J. Aug. 24, 2006) ("'Generally known' does not only mean that the information is of public record. . . . The information must be within the basic understanding and knowledge of the public. The content of form pleadings, interrogatories and other discovery materials, as well as general litigation techniques that were widely available to the public through the internet or another source, such as continuing legal education classes, does not make that information 'generally known' within the meaning of Rule 1.9(c)." (citations omitted));

Steel v. Gen. Motors Corp., 912 F. Supp. 724, 739 (D. N.J. 1995) (in a discussion of Rule 1.9(c)(2), stating that the fact that information is publicly available does not make it 'generally known');

In re Gordon Props., LLC, 505 B.R. 703, 707 n.6 (Bankr. E.D. Va. 2013) ("'Generally known' does not mean information that someone can find.");

In re Anonymous, 932 N.E.2d 671, 674 (Ind. 2010) (stating in connection with a discussion of Rule 1.9(c)(2) that "the Rules contain no exception allowing revelation of information relating to a representation even if a diligent researcher could unearth it through public sources" (footnote omitted);

In re Tennant, 392 P.3d 143, 148 (Mont. 2017) (explaining that with respect to the Rule 1.9(c) analysis of when information is considered to be generally known, the fact that "the information at issue is generally available does not suffice; the information must be within the basic knowledge and understanding of the public;" protection of the client's information "'is not nullified by the fact that the circumstances to be disclosed are part of a public record, or that there are other available sources for such information, or by the fact that the lawyer received the same information from other sources'") (citations omitted));

Turner v. Commonwealth, 726 S.E.2d 325, 333 (Va. 2012) (Lemons, J., concurring) ("While testimony in a court proceeding may become a matter of public record even in a court denominated as a 'court not of record,' and may have been within the knowledge of anyone at the preliminary hearing, it does not mean that such testimony is 'generally known.' There is a significant difference between something being a public record and it also being 'generally known.'");

3. The ABA Suggested Definition:

A Workable Definition of Generally Known under Model Rule 1.9(c)(1)

Consistent with the foregoing, the Committee's view is that information is generally known within the meaning of Model Rule 1.9(c)(1) if (a) it is *widely recognized by members of the public in the relevant geographic area*; or (b) it is *widely recognized in the former client's industry, profession, or trade*. Information may become widely recognized and thus generally known as a result of publicity through traditional media sources, such as newspapers, magazines, radio, or television; through publication on internet web sites; or through social media. With respect to category (b), information should be treated as generally known if it is announced, discussed, or identified in what reasonable members of the industry, profession, or trade would consider a leading print or online publication or other resource in the particular field. Information may be widely recognized within a former client's industry, profession, or trade without being widely recognized by the public. For example, if a former client is in the insurance industry, information about the former client that is widely recognized by others in the insurance industry should be considered generally known within the meaning of Model Rule 1.9(c)(1) even if the public at large is unaware of the information.

Unless information has become widely recognized by the public (for example by having achieved public notoriety), or within the former client's industry, profession, or trade, *the fact that the information may have been discussed in open court, or may be available in court records, in public libraries, or in other public repositories does not, standing alone, mean that the information is generally known for Model Rule 1.9(c)(1) purposes. Information that is publicly available is not necessarily generally known.*

Certainly, if information is publicly available but requires specialized knowledge or expertise to locate, it is not generally known within the meaning of Model Rule 1.9(c)(1).

4. Use Judgment and Discretion:

A. The "Fact" of Representation May be Confidential, if the Client Desires it to be Kept Confidential.

B. The Client May Expect That the Lawyer Will Not Discuss the Matter, Even if Proceedings have been Filed

In re Anonymous, 932 N.E.2d 671, 674 (Ind. 2010)—gossiping at a cocktail party

C. CLE Presentations:

No immunity for a lawyer discussing clients at Continuing Legal Education Programs

D. Blogging

See KBA Blogging Opinion

References:

SCR 3.130 (Rule 1.6(a))

Confidentiality of information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) * * * *

SCR 3.130 (Rule 1.9)

Duties to former clients.

* * * *

(c) ***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:

(1) ***use information relating to the representation to the disadvantage of the former client except*** as these Rules would permit or require with respect to a client, or ***when the information has become generally known***; or

(2) ***reveal information relating to the representation*** except as these Rules would permit or require with respect to a client.

(Emphasis Added)

Relevant Formal Opinions include:

Kentucky Bar Association: Has Not Issued Any Opinion.

American Bar Association:

ABA Formal Opinion 479, "The 'Generally Known' Exception to Former-Client Confidentiality," December 15, 2017.

Vermont Law Review, Vol. 40, p. 69, Michael D. Chicchini, "On The Absurdity of Model Rule 1.9"

https://lawreview.vermontlaw.edu/wp-content/uploads/2016/01/Vol-40-1-Cicchini.pdf

Blogging

Disclosure of client confidential information in a blog or other social media

1) **In a blog or other social media, may a lawyer disclose information relating to the representation of a current or former client without the client's consent?**
Answer: No

2) **May an attorney reveal the identity of a current or former client in a blog or other social media without the client's consent?**
Answer: No.

3) **Is there an exception to (1) or (2) for information contained in a public record?**
Answer: No.

Essentially, this opinion covers the informal disclosure of client information, sometimes for a useful purpose such as a lawyers' exchange of information blog posting;

1. Unless one of the exceptions in Rule 1.6(b) applies, Rule 1.6(a) requires a lawyer to obtain client consent before disclosing any information relating to the client's representation.

2. KBA E-253, applying DR 4-101(C) absent consent, a lawyer may reveal names and addresses of clients only:

1) where the information is in the public record as a result of the attorney's representation; or

2) where the circumstances make it obvious that the client does not expect confidentiality as to the existence of the attorney client relationship, or
3) where the client has specifically authorized in writing the release of the information.

3. [T]here is no justification for revealing information, without consent, about past or present clients in a blog or other social media. In *Office of Lawyer Regulation v. Pershek*, 798 N.W.2d 879 (Wis. 2011), the attorney was suspended for blogging about her clients; in *In re Smith*, 991 N.E.2d 106 (Ind. 2013), the attorney was disbarred for writing a book about a former client. The disciplinary cases involve negative disclosures, but the rule against disclosure applies to all information, whether positive, neutral or negative.

4. Attorneys should be careful in using thinly disguised hypotheticals. "A violation of Rule 1.6(a) is not avoided by describing public commentary as a 'hypothetical' if there is a reasonable likelihood that a third party may ascertain the identity or situation of the client from the facts set forth in the hypothetical." ABA Formal Op. 480.

SCR 3.130 (Rule 1.6(a))

Confidentiality of information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
(b) * * * *

Relevant Formal Opinions include:

Kentucky Bar Association:
Disclosure of client confidential information in a blog or other social media

American Bar Association:
ABA Formal Opinion 480, "Confidentiality Obligations for Lawyer Blogging and Other Public Commentary" March 6, 2018.

"Self-Defense" From Unfair or False Public Postings

Self-defense opinion (March 14, 2019)

Question: May a lawyer reveal client confidential information reasonably necessary to respond to a former client's public criticism?

Answer: No

Question: How may a lawyer ethically respond to a former client's public criticism?

Answer: See Opinion

The self-defense exception to the duty of confidentiality (1.6(b)(3)is triggered by claims or disciplinary complaints against a lawyer. The exception does not encompass internet criticism. In Defending Against Internet Criticism: Silence is Golden, 26 South Carolina Law Review 12 (2014), Nathan Crystal uses the Betty Tsamis case to illustrate: After being fired a flight attendant hired Tsamis to seek unemployment benefits from the state. Apparently Tsamis learned after she was hired that the attendant had been fired because he beat up a female co-worker. After a hearing the claim was denied and the attendant complained about Tsamis on the internet. This eventually resulted in Tsamis being publicly reprimanded for posting the following:

> This is simply false. The person did not reveal all the facts of the situation up front in our first and second meetings. . . . Despite knowing he would likely lose he chose to go forward with a hearing to try to obtain benefits. I dislike it very much when my clients lose but I cannot invent positive facts for clients when they are not there. I fell badly for him but his own actions in beating up a female coworker are what caused the consequences he is now so upset about.

In most instances the best advice is to ignore the criticism. For the lawyer who wants to respond, the Committee recommends the following:

My professional and ethical responsibilities do not allow me to reveal confidential client information in response to _____

SCR 3.130 (Rule 1.6(a))

Confidentiality of information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(c) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

* * *

(3) *to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to*

> *respond to allegations in any proceeding, including a disciplinary proceeding, concerning the lawyer's representation of the client;* or * * * *

Public airing of client dissatisfaction with the lawyer is not a "controversy between the lawyer and the client."

KENTUCKY BAR ASSOCIATION
Ethics Opinion KBA E-403
Issued: March 1998

Since the adoption of the Rules of Professional Conduct in 1990, the Kentucky Supreme Court has made substantial revisions to the rules governing the advertisement of legal services. For example, Rule 7.30 was deleted and replaced with Rule 7.09, entitled "Direct contact with potential clients." Lawyers should consult the current version of the rules and comments, SCR 3.130 (available at http://www.kybar.org) and the Attorneys' Advertising Commission Regulations, before relying on this opinion.

Question 1: May a lawyer use electronic mail services including the Internet to communicate with clients without encryption?

Answer: Yes, unless unusual circumstances require enhanced security measures.

Question 2: Is the creation and use by a lawyer of an Internet "web site" containing information about the lawyer and the lawyer's services that may be accessed by Internet users, including prospective clients, a communication falling within KRPCs 7.09 [Prohibited Solicitation] or 7.30 [Direct Contact With Prospective Client]?

Answer: Qualified No. Unless the lawyer uses the Internet or other electronic mail service to direct messages to a specific recipient [in which case the rules governing solicitation would apply, only the general rules governing communications regarding a lawyer's services and advertising [KRPCs 7.10, 7.20, and the so-called advertising rules set forth at KRPCs 7.01-7.08] should apply to a lawyer's "web-site" on the Internet.

References: Illinois Op. 96-10 (1997); Kurt Metzmeier & Shaun Esposito, How to Avoid Losing your License on the Information Superhighway; Ethical Issues Raised by the Use of the Internet in The Practice of Law (1997-98).

OPINION

Despite widespread use of the Internet, the Committee has received few inquiries regarding its use. Still, the Committee is of the view that this opinion should be issued to provide some guidance and some comfort. The subject is addressed in a recent article cited in the references, which is available from the UK Law Library, and which has been submitted for publication in the Bench & Bar.

The Committee finds persuasive the comprehensive and thoughtful opinion of the Illinois State Bar Association, ISBA Advisory Opinion No. 96-10, excerpts of which we attach as an Appendix.

APPENDIX

ILLINOIS STATE BAR ASSOCIATION

ISBA Advisory Opinion on Professional Conduct

ISBA Advisory Opinions on Professional Conduct are prepared as an educational service to members of the ISBA. While the Opinions express the ISBA interpretation of the Illinois Rules of Professional Conduct and other relevant materials in response to a specific hypothesized fact situation, they do not have the weight of law and should not be relied upon as a substitute for individual legal advice.
Illinois Opinion No. 96-10

May 16, 1997

Topic: Electronic communications; confidentiality of client information; advertising and solicitation.

Digest: Lawyers may use electronic mail services, including the Internet, without encryption to communicate with clients unless unusual circumstances require enhanced security measures. The creation and use by a lawyer of an Internet "web site" containing information about the lawyer and the lawyer's services that may be accessed by Internet users, including prospective clients, is not "communication directed to a specific recipient" within the meaning of the rules, and therefore only the general rules governing communications concerning a lawyer's services and advertising should apply to a lawyer "web site" on the Internet. If a lawyer uses the Internet or other electronic mail service to direct messages to specific recipients, then the rules regarding solicitation would apply.

Ref.: Illinois Rules of Professional Conduct, Rules 1.6, 7.1, 7.2, 7.3 and 7.4; ISBA Opinion Nos. 90-07 and 94-11; Electronic Communications Privacy Act, 18 USC §2510, et seq.

QUESTIONS

The Committee has received various inquiries regarding ethical issues raised by use of electronic means of communication, including electronic mail and the "Internet," by lawyers. These inquiries usually involve two general areas of concern. The first is whether electronic mail may be used to communicate with clients regarding client matters in view of a lawyer's duty under the ethics rules to maintain the confidentiality of client information. The second is whether the creation and use of a "web site" and other forms of contract with prospective clients may be conducted by lawyers on the Internet, and if so, whether the rules regarding "in person" solicitation should apply to such contact.

Because of the technical nature of the discussion, the Committee will use the following commonly accepted definitions in this opinion. The Internet is a supernetwork of computers that links together individual computers and computer networks located at academic, commercial, government and military sites worldwide, generally by ordinary local telephone lines and long-distance transmission facilities. Communications between computers or individual networks on the Internet are achieved throughout he use of standard, nonproprietary protocols.

Electronic mail, commonly known as e-mail, is an electronic message that is sent from one computer to another, usually through a host computer on a network. E-mail messages can be sent through a private or local area network (within a single firm or organization), through an electronic mail service (such as America Online, CompuServ or MCI Mail), over the Internet, or through any combination of these methods.

A bulletin board service (sometimes called a "BBS") is an electronic bulletin board on a network where electronic messages may be posted and browsed by users or delivered to e-mail boxes. A "newsgroup" is a type of bulletin board service in which users can exchange information on a particular subject. A "chat" group is a simultaneous or "real time" bulletin board or newsgroup among users who send their questions or comments over the Internet.

The World Wide Web is that part of the Internet consisting of computer files written in a particular format (the "HTML" format) that includes "hyperlinks" (text or symbols that the user may click on to switch immediately to the item identified) as well as graphics and sound, to enable the creation of complex messages. A "home page" is a computer file containing text and graphics in the HTML format usually continuing information about its owner, which can be obtained over the Internet and viewed by transmitting it from the owner's computer to the user's terminal. A "web site" is a set of computer files containing text and graphics in the HTML format and organized around a central home page.

The Electronic Communications Privacy Act, 18 USC §2510, et seq. (the "ECPA"), is the federal codification of the intrusion arm of the common law tort of invasion of privacy applied to electronic communication and provides criminal and civil penalties for its violation. The ECPA is actually the 1986 revision of the federal wiretap statute originally enacted in 1968, but the term ECPA is now commonly used to refer to the entire statute, as amended.

OPINION

The first issue, whether a lawyer may use electronic mail services including the Internet to communicate with clients, arises out of a lawyer's duty to protect confidential client information. Rule 1.6(a) of the Illinois Rules of Professional Conduct provides that "...a lawyer shall not, during or after termination of the professional relationship with the client, use or reveal a confidence or secret of the client known to the lawyer unless the client consents after disclosure." AS the Terminology provisions of the Rules state, the information a lawyer must protect includes information covered by the lawyer-client privilege (a "confidence") as well as information that the client wishes to be held inviolate or the revelation of which would be embarrassing or detrimental to the client (a "secret").

The duty to maintain the confidentiality of client information implies the duty to use methods of communication with clients that provide reasonable assurance that messages will be and remain confidential. For that reason, the Committee concluded in Opinion No. 90-07 (November 1990) that a lawyer should not use cordless or other mobile telephones that were easily susceptible to interception when discussing confidential client matters. The Committee also opined that a lawyer conversing with a client over a cordless or mobile telephone should advise the client of the risk of the loss of confidentiality.

With the increased use of electronic mail, particularly electronic mail transmitted over the Internet, have come suggestions that electronic messages are not sufficiently secure to be used by lawyers communicating with clients. At least two state etches opinions have concluded that because it is possible for Internet or other electronic mail service providers to intercept electronic mail service providers to intercept electronic mail messages, lawyers should not use electronic mail for "sensitive" client communications unless the messages were encrypted or the client expressly consented to "non-secure" communication. South Carolina Bar Advisory Opinion 94-27 (January 1995); Iowa Supreme Court Board of Professional Ethics and Conduct Opinion 96-1 (August 29, 1996). After reviewing much of the available literature on this issue, the Committee disagrees with these opinions.

Among the numerous recent articles regarding a lawyer's use of electronic mail, the Committee found three to be particularly useful and informative. These are: Joan C. Rogers, "Malpractice Concerns Cloud E-Mail, On-Line Advice," ABA/BNA Lawyers' Manual on Professional Conduct (March 6, 1996); Peter R. Jarvis & Bradley F. Tellam, "High-Tech Ethics and Malpractice Issues," 1996 Symposium Issue of the Professional Lawyer, p. 51 (1996); David Hricik, "Confidentiality and Privilege in High-Tech Communications," 8 Professional Lawyer, p. 1 (February 1997). From these and other authorities, there is a clear consensus on two critical points. First, although interception of electronic messages is possible, it is certainly no less difficult than intercepting an ordinary telephone call. Second, intercepting an electronic mail message is illegal under the ECPA.

Courts and ethics committees have uniformly held that persons using ordinary telephones for confidential communications have a reasonable expectation of privacy. The three common types of electronic mail messages appear no less secure. For example, electronic messages that are carried on a local area or private network may only be accessed from within the organization owning the network. Such messages would therefore clearly appear subject to a reasonable expectation of privacy.

Other electronic messages are carried by commercial electronic mail services or networks such as America Online, CompuServ or MCI Mail. Typically, these services transmit e-mail messages from one subscriber's computer to another computer "mailbox" over a proprietary telephone network. Typically, the computer mailboxes involved are password-protected. Because it is possible for dishonest or careless personnel of the mail service provider to intercept or misdirect a message, this form of electronic mail is arguably less secure than messages sent over a private network. AS a practical matter, however, any ordinary telephone call may also be intercepted or misdirected by dishonest or careless employees of the telephone service provider. Again, this possibility has not compromised the reasonable expectation of privacy of ordinary telephone users. The result should be the same for electronic mail service subscribers.

The third type of electronic mail, that carried on the Internet, typically travels in another fashion. Rather than moving directly from the sender's host computer to the recipient's host computer, Internet messages are usually broken into separate "packets" of data that are transmitted individually and then re-assembled into a complete message at the recipient's host computer. Along the way, the packets travel through, and may be stored temporarily in, one or more other computers (called "routers") operated by third parties (usually called an "internet service provider" or "ISP") that help distribute electronic mail over the Internet.

Unlike a cordless cellular telephone message, for example, an Internet e-mail is not broadcast over the open air waves, but through ordinary telephone lines and the intermediate computers. When an Internet message is transmitted over an ordinary telephone line, it is subject to the same

protections and difficulties of interception as an ordinary telephone call. To intercept an Internet communication while it is in transit over telephone lines requires an illegal wiretap. Consequently, the real distinction between an Internet electronic message and an ordinary telephone call is that Internet messages may be temporarily stored in, and so can be accessed through, a router maintained by an ISP. It is possible that an employee of an ISP (as part of the maintenance of the router) could lawfully monitor the router and thereby read part or all of a confidential message. As in the case of telephone and proprietary electronic mail providers, it is also possible for dishonest employees of an ISP to intercept messages unlawfully. The Committee does not believe that the opportunity for illegal interception by personnel of an ISP makes it unreasonable to expect privacy of the message.

As noted above, it is also clear that unauthorized interception of an Internet message is a violation of the ECPA, which was amended in 1986 to extend the criminal wiretapping laws to cover Internet transmissions. As part of the 1986 amendments, Congress also treated the issue of privilege in 18 USCA §2517(4), as follows:

> No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

This provision demonstrates that Congress intended that Internet messages should be considered privileged communications just as ordinary telephone calls.

In summary, the Committee concludes that 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 ECPA is illegal, a lawyer does not violate Rule 1.6 by communicating with a client using electronic mail services, including the Internet, without encryption. Nor is it necessary, as some commentators have suggested, to seek specific client consent to the use of unencrypted e-mail. The Committee recognizes that there may be unusual circumstances involving an extraordinarily sensitive matter that might require enhanced security measures like encryption. These situations would, however, be of the nature that ordinary telephones and other normal means of communication would also be deemed inadequate.

With respect to the second general issue, the extent to which a lawyer may use Internet web site to communicate with clients and prospective clients, the Committee believes that the existing Rules of Professional Conduct governing advertising, solicitation and communication concerning a lawyer's services provide adequate and appropriate guidance to a lawyer using the Internet. For example, the Committee views an Internet home page as the electronic equivalent of a telephone directory "yellow pages" entry and other material included in the web site to be the functional equivalent of the firm brochures and similar materials that lawyers commonly prepare for clients and prospective clients. An Internet user who has gained access to a lawyer's home page, like a yellow pages user, has chosen to view the lawyer's message from all the messages available in that medium. Under these circumstances, such materials are not a "communication directed to a specific recipient" that would implicate Rule 7.3 and its provisions governing direct contact with prospective clients. Thus, with respect to a web site, Rule 7.1, prohibiting false or misleading statements concerning a lawyer's services, and Rule 7.2, regulating advertising in the public media, are sufficient to guide lawyers and to protect the public.

On the other hand, lawyer participation in an electronic bulletin board, chat group, or similar service, may implicate Rule 7.3, which governs solicitation, the direct contact with prospective clients. The Committee does not believe that merely posting general comments on a bulletin board or chat group should be considered solicitation. However, of a lawyer seeks to initiate an unrequested contact with a specific person or group as a result of participation in a bulletin board or chat group, then the lawyer would be subject to the requirements of Rule 7.3.

For example, if the lawyer sends unrequested electronic messages (including messages in response to inquiries posted in chat groups) to a targeted person or group, the messages should be plainly identified as advertising material.

Finally, lawyers participating in chat groups or other on-line services that could involve offering personalized legal advice to anyone who happens to be connected to the service should be mindful that the recipients of such advise are the lawyer's clients, with the benefits and burdens of that relationship. In Opinion No. 94-11 (November 1994), the Committee addressed an analogous situation arising out of a "call-in" legal advice service as follows:

> The committee believes that callers to the legal advice service are clients of the law firm who are entitled to the protection of clients afforded by the Rules of Professional Conduct. However, it does not appear that either the law firm or the cellular telephone service makes any effort to determine the identity of the callers and check for potential conflicts of interest prior to the time that the callers' questions are asked and the legal advice is given. (Presumably the callers' identities are revealed after the advice is rendered through the billing process. If the cellular telephone company handles the billing for the law firm, this procedure may also violate client confidences. See ISBA Opinion No. 93-04) Under these circumstances, it would be possible for the law firm to give legal advice to callers whose interest are directly adverse to other firm clients, including other callers, in violation of Rule 1.7(a), or whose interests are materially adverse to the firm's former clients, including other callers, concerning the same or a substantially related matter, in violation of Rule 1.9

Lawyers participating in similar activity over the Internet would be subject to the same concerns expressed in Opinion No. 94-11.

For these reasons, the Committee believes that Illinois lawyers may appropriately make use of the Internet in serving and communicating with clients and prospective clients subject to the existing rules governing confidentiality, advertising and solicitation.

Note to Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530 (or its predecessor rule). The Rule provides that formal opinions are advisory only.

KENTUCKY BAR ASSOCIATION
Ethics Opinion KBA E-427
Issued: March 23, 2007

OPINION

Subject: Lawyer and law firm domain names (web addresses)

Question I: May a lawyer or law firm use a domain name that does not identify the lawyer or firm, but links to a website that clearly identifies the sponsoring lawyer or law firm?

Answer: Qualified Yes

Question II: May a lawyer maintain a website that is identified by domain name only and does not identify an individual lawyer or law firm?

Answer: No

References: SCR 3.130 (7.01-7.60); KBA E-338 (1990); KBA E-302 (1985); Az. B. Ethics Op. 01-05 (2001) (available at www.myazbar.org/Ethics/opinionview); Ass'n of the City B. of N.Y. Op. 2003-01 (available at 2004 WL 837935); N. J. Comm. on Atty. Advt. Op. 32 (available at 2005 WL 3890570); S. C. B. Ethics Adv. Comm. Op. 04-06 (available at 2004 WL 1520110).

Introduction

The Attorneys' Advertising Commission is responsible for overseeing the regulation of lawyer advertising, which is governed by SCR 3.130 (7.01 - 7.60). Lawyer advertising on the internet raises a broad range of ethical issues, which are not specifically addressed by the rules. The Attorneys' Advertising Commission has asked the Ethics Committee to consider two of those issues; both are related to the use of domain names (web addresses). This opinion is designed to assist the Commission in its work and to alert members of the bar to some of the ethical issues associated with the use of domain names. Lawyers are reminded that Rule 7.05 provides that all advertisements must be filed with the Attorneys' Advertising Commission;[1] lawyers who have ethical questions about lawyer advertising should request an advisory opinion from the Commission, not the Ethics Committee. SCR 3.130 (7.06).

The Kentucky Rules of Professional Conduct contain extensive provisions regulating lawyer advertising. See SCR 3.130 (7.01 - 7.60). Rule 7.02(1) defines advertising as the furnishing of "any information or communication containing a lawyer's name or other identifying information…."[2] Rule 7.15 prohibits communications about the lawyer or the lawyer's service that are false, deceptive or misleading. These umbrella provisions are the foundation of lawyer advertising regulation and apply to all advertisements, no matter what form they take. In addition, Rule 7.50(1) prohibits the "use of a firm name, letterhead or other professional

[1] Lawyer websites are a form of advertising and are subject to the same rules, including the submission requirements, as other forms of advertising.
[2] The rule excludes certain basic kinds of communication, such as professional cards, professional directory listings and office signs, from the definition of advertising. SCR 3.130 (7.02 (1) (a)-(i)).

designation that violates Rule 7.15." It is against this backdrop that the Committee considers the ethical issues related to lawyer and law firm domain names.

I. Use of a domain name that does not identify the lawyer or law firm, but connects to a website that clearly identifies the sponsoring lawyer or law firm

Various electronic media, including the internet, have become important sources of information for the public, and lawyer websites have become a popular means of communicating with clients and potential clients. Typically, websites contain information about the lawyer or the firm members and the nature of the practice. They are designed to promote the lawyer or the firm and to attract clients. Websites are a form of advertising; they "furnish … information … containing a lawyer's name or other identifying information…." and are subject to regulation by the bar. SCR 3.130 (7.02(1)).

Just as websites are a type of advertising subject to the Rules of Professional Conduct, so are the domain names that are used to access those websites. Domain names are a form of communication about the lawyer's services. Like firm names, they contain "identifying information" and cannot be false, deceptive or misleading. SCR 3.130 (7.15).

Many lawyers use domain names that are related to their own name or that of their firm. Lawyer Joe W. Smith may use the domain name of www.jwsmithattorney.com or www.jwsmithandassociates.com. In the first example, the domain name is that of the lawyer; in the second example, the domain name is that of a law firm. These hypothetical domain names, standing alone, would not be false, deceptive or misleading advertising.[3] The webpages to which they link would, of course, be subject to a separate review under the rules.[4]

The issue becomes more complicated when the lawyer selects a domain name that is not related to his or her name, or that of the firm. Most ethics committees considering this issue have concluded that domain names that do not include the lawyers name are not per se unethical as long as they comply with the general advertising rules.[5]

A domain name must be analyzed under several provisions of the advertising rules. Again, the initial focus will be on whether the domain name is false, deceptive or misleading. Does the name contain a material misrepresentation of fact, create unjustified expectations or compare the lawyer's services with others? SCR 3.130 (7.15 (a) – (c)). The following examples of domain names, unrelated to the lawyer or the firm, may be helpful in understanding the application of the rules.

Some domain names are targeted to a particular group of potential clients by suggesting an area of concentration. For example, a lawyer who practices family law might use www.divorcelawyer.com. The mere fact that the domain name indicates a field of practice does not, in and of itself, make it false, deceptive or misleading. Although Kentucky does not recognize specialists, Rule 7.40 permits a lawyer to indicate his or her area of practice as long as

[3] In the above example, the domain name www.jwsmithandassociates.com would violate the rule if no legal entity actually exists. Rule 7.50(4) provides: "Lawyers may state or imply that they practice in a legal entity only if that is the fact."
[4] *See* SCR 3.130 (7.05) requiring all advertisements to be filed with the Commission.
[5] *See e.g.,* N.J. Comm. on Atty. Advert. Op. 32 (available at 2005 WL 3890570); Assn. of the B. of the City of N. Y. Formal Op. 2003-01 (available at 2004 WL 837935) (decided under the Code).

long as the advertisement otherwise conforms to the rules.[6] If a lawyer can state that he or she practices divorce law, there does not appear to be any reason why that same lawyer can not use a domain name that conveys the same information.

This is not to suggest that all domain names will withstand scrutiny under the rules. Just as a lawyer could not say she is the "greatest lawyer in Kentucky," because that is likely to create unjustified expectations (and compares her services with others), she could not use the domain name www.greatestlawyerinky.com for the same reason. Similarly, any domain name that suggests a connection with a governmental entity would violate Rule 7.15. For example, a private law firm that used a domain name of www.louisvillelegalclinic.com might lead a prospective client to believe that the lawyer is part of a governmental entity or a non-profit organization. Similarly, the Arizona Bar has concluded that the domain name www.countybar.com is misleading because it implies affiliation with a bar association and the domain name www.arizonalawyer.org is misleading because the use of the top level domain name "org" implied that the firm is a non-profit organization.[7] Finally, although a lawyer may use a domain name that indicates an area in which the lawyer practices, Rule 7.40 prohibits the use of any form of the words "certified," "specialists," "expert," or "authority."[8] Thus, a domain name of www.accidentspecialist.com, would violate Rule 7.40.

Finally, it is important to emphasize that Question I. assumes that the domain name links directly to the website of the lawyer or the law firm and that the site clearly identifies the lawyer or firm by name. This satisfies the requirement of Rule 7.20, which provides that "(a)ny communication made pursuant to these Rules shall include the name of at least one lawyer licensed in Kentucky, or law firm any of whose members are licensed in Kentucky, responsible for its contents." By clearly identifying the lawyer or the firm on the webpage, the user will not be misled about the identity of the lawyers and the services being offered.

II. Maintenance of a website that is identified by domain name only and does not include the name of an individual lawyer or law firm

The second question is a variation on the first. It assumes that the domain name does not include the lawyer's name or the name of the firm, that the website is identified by the domain name only and that the identity of the lawyer or law firm is unclear. In the first question, the domain name was a form of communication, but its primary purpose was to attract the user and connect him or her to the lawyer's website, where the lawyer or the firm was identified. In this question, the domain name is again used to attract the user but, because it connects to a website that does not identify the lawyer or the firm, the domain name becomes the identifier. The current Rules of Professional Conduct were developed long before the internet became a generally accepted means for exchanging information. Nevertheless, the rules contain a number of principles that are relevant to website communications. In applying those principles, it becomes immediately

[6] SCR 3.130 (7.40) provides:

> Communication of fields of practice.
> A lawyer may communicate the fact that the lawyer does or does not practice in particular field of law. A lawyer who concentrates in, limits his or her practice, or wishes to announce a willingness to accept cases in a particular field may so advertise or publicly state in any manner otherwise permitted by these Rules. Any such advertisement or statement shall be strictly factual and shall not contain any form of the words "certified", "specialist", or "authority."

[7] Az. B. Ethics Op. 01-05 (2001) (available at www.myazbar.org/Ethics/opinionview).

[8] SCR 3.130 (7.40), *supra* n. 6.

apparent that the practice of not prominently identifying the lawyer or the law firm on the website is problematic on several levels.

First, the overwhelming concern of the rules is that all advertisements be truthful; they cannot be deceptive or misleading. SCR 3.130 (7.15). By failing to identify the name of the firm or the lawyer involved, the public may be misled as to the identity, status and responsibility of those involved.

Second, Rule 7.20(3) requires that every communication made under the rule "shall include the name of at least one lawyer licensed in Kentucky, or law firm any of whose members are licensed in Kentucky, responsible for its contents." Failure to prominently identify the lawyer or the firm on the webpage violates this rule.

It has been suggested that when a lawyer maintains a website that does not identify the lawyer or the law firm, but uses the domain name as the identifier, the domain name becomes a tradename. Although the tradename issue may be an interesting one, the Committee is of the view that this question can be resolved on the basis of the two rules described above. It is the Committee's view that it is a violation of the Rules 7.15 and 7.20(3) to maintain a website that is identified by domain name only and does not include the name of an individual lawyer or law firm.

Conclusion

The Committee has concluded that it is not inherently unethical for a lawyer or a lawyer firm to adopt a domain name, unrelated to the name of the lawyer or the law firm, if the following conditions are met:

- The domain name complies with RPC 7.15; it is not false, deceptive or misleading.
- The website to which the domain name connects prominently identifies the name of the firm or the lawyers involved. The domain name cannot be used as a substitute identity for the lawyer or the firm.
- The domain name does not imply that the lawyer is a specialist, except as permitted by Rule 7.40.[9]

Note to Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. Note that the Rule provides: "Both informal and formal opinions shall be advisory only; however, no attorney shall be disciplined for any professional act performed by that attorney in compliance with an informal opinion furnished by the Ethics Committee member pursuant to such attorney's written request, provided that the written request clearly, fairly, accurately and completely states such attorney's contemplated professional act."

[9] Rule 7.50 generally prohibit communications which state or imply that the lawyer is "certified" or a "specialist" or "expert" in a particular area of practice. The rule contains a narrow exception for licensed patent lawyers, admiralty lawyers and those certified by national organizations qualifying under *Peel v. Attorney Registration and Disciplinary Commission of Illinois.*

KENTUCKY BAR ASSOCIATION

Ethics Opinion KBA E-434
Issued: November 17, 2012

The Rules of Professional Conduct are amended periodically. Lawyers should consult the current version of the rules and comments, SCR 3.130 (available at http://www.kybar.org/237), before relying on this opinion.

Subject: Ethical Considerations Relating to a Lawyer's Use of Social Network Sites[1] to Benefit a Client[2]

Question: May a lawyer access or otherwise use the social network site of a third-person to benefit a client?

Answer: A lawyer may access or otherwise use the social network site of a third-person to benefit a client, as long as the conduct does not violate the Rules of Professional Conduct.

References: SCR 3.130 (3.5), (4.1), (4.2), (4.3), (8.4) (a) and (c); Risk Managing Internet Social Network Investigations, 23 The Risk Manager (newsletter of Lawyers Mutual Ins. Co. of Ky.) (Spring 2012), www.lmick.com/resources/the-risk-manager-by-year/187-newsletter-2012.html; Journal of Computer-Mediated Communications (2007); San Diego Co. Bar Op. 2011-12 (2011); N.Y. State Bar Assn. Op. 843 (2010).

Introduction

The dramatic changes in information technology and the growth of social network sites such as Facebook have significantly changed the way people communicate. At the same time, these changes have made a wealth of personal information available over the internet. While many use these networks for social purposes, connecting with friends and family, they also can be used for business and professional purposes and may be a valuable resource for a practicing lawyer. Information posted on the social network site

[1] Social networks, as commonly understood at the time this opinion was written, include web-based services that allow individuals to build a public or semi-public bounded system; to identify users with whom they share a connections and view and traverse their list of connections and those made by others in the system. boyd, d. m. and Ellison, N. B., Social network sites: Definition, history, and scholarship, *Journal of Computer-Mediated Communications (2007)*, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

[2] This opinion only addresses ethical considerations relating to the lawyer's use of social network sites of third persons. It does not address the ethical restrictions on a lawyer's use of his or her own social network site for advertising or other purposes.

of an adverse party, a witness, juror or other third person could be very useful to the lawyer investigating a matter on behalf of a client.

The Committee has received several inquiries regarding the use of social network sites and the extent to which lawyers may go to obtain access to information from the site of an opponent or other third person. In addressing these issues, the Committee perceived two challenges. First, ethical issues raised by modern technology were not even imagined by the drafters of the Rules of Professional Conduct. However, after considerable discussion the Committee concluded that, despite the advances in technology, the core ethical principles upon which the profession has relied for generations – honesty and fairness --remain unchanged. In the final analysis, though social networking may appear to raise new ethical issues that might require new rules, the current rules adequately address those issues that have been brought to the attention of the Committee. For example, if the Rules of Professional Conduct prohibit lawyers from contacting jurors or communicating with represented parties in the non-technical world, they prohibit such conduct in the virtual world. The underlying principles of fairness and honesty are the same, regardless of context.

The second challenge related to the specific scenarios that the Committee was asked to address. We quickly realized that social networking is extraordinarily complex and is being modified constantly. In addition, new systems are being developed every day and it is beyond the Committee's capacity to imagine what might develop in the future. Because of this, it is not possible to draft an opinion with specific scenarios that would be comprehensive and enduring. Nevertheless, the Committee believes it would be helpful to address the basic Rules of Professional Conduct that might be implicated when a lawyer accesses or otherwise uses a social network site to benefit a client. Specifically, those rules are:

- SCR 3.130(4.1) Truthfulness in Statements to Others
- SCR 3.130 (4.2) Communication with Person Represented by Counsel
- SCR 3.130(4.3) Dealing with Unrepresented Person
- SCR 3.130(3.5) Impartiality and Decorum of the Tribunal
- SCR 3.130(8.4(a)(c)) Misconduct

Some inquiries have focused on whether a lawyer may access the site of a third person. If the site is "public," and accessible to all, then there does not appear to be any ethical issue.[3] If, however, access is limited, then there may be issues of what the lawyer can do to gain access. The Rules of Professional Conduct require truthfulness and honesty in dealing with others. Specifically, SCR 3.130 (4.1) prohibits a lawyer from making false statements.[4] Also relevant is SCR 3.130(8.4), which prohibits the lawyer from engaging in dishonest conduct.[5]

[3] See, San Diego Co. Bar Op. 2011-2 (2011). See also, N.Y. Bar Assn. Op. 843 (2010).

[4] SCR 3.130(4.1) provides: "In the course of representing a client a lawyer:(a) shall not knowingly make a false statement of material fact or law to a third person; and (b) if a false statement of material fact or law has been made, shall take reasonable remedial

Social network sites generally permit certain people to send messages to others. A lawyer's communication with someone represented by counsel is addressed by SCR 3.130(4.2), which generally prohibits direct contact.[6] To the extent that someone is represented by counsel, it would apply. The Commentary to Rule 4.2 explains that the rule is to protect against uncounseled disclosures and applies even though the represented person initiates or consents to the contact.[7] If a person with whom the lawyer is communicating is unrepresented, such as a witness, then SCR 3.130 (4.3) would apply.[8] The Rules of Professional Conduct,[9] as well as various statutes and court rules, prohibit improper contact with jurors. Those prohibitions would apply in the social network context as well.

Finally, questions have arisen as to whether a lawyer may request a third person, such as a paraprofessional, investigator or other non-lawyer staff member, to obtain information through means that the lawyer could not ethically use. SCR 3.130 (8.4)[10] and the Comments[11] normally would prohibit such conduct. As a general rule, a lawyer cannot use another to do that which the lawyer is prohibited from doing.

Conclusion

Social networking and other technological advances have provided, and will continue to provide, endless possibilities for obtaining information that may be useful in the representation of a client. These systems are extraordinarily complicated and constantly changing, and thus it would be impossible to address every possible ethical consideration that might arise in conjunction with the use of social network sites. Several core

measures to avoid assisting a fraudulent or criminal act by a client including, if necessary, disclosure of a material fact, unless prohibited by Rule 1.6."

[5] SCR 3.130(8.4(a),(b),(c)) provides: "It is professional misconduct for a lawyer to:(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;(b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation…."

[6] SCR 3.130(4.2) provides: "In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order."

[7] *See* Comments 1 and 3 to Rule 4.2.

[8] SCR 3.130(4.3) provides: "In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding. The lawyer shall not give legal advice to an unrepresented person. The lawyer may suggest that the unrepresented person secure counsel."

[9] SCR 3.130(3.5) provides: "A lawyer shall not: (a) seek to influence a judge, juror, prospective juror or other official by means prohibited by law; (b) communicate ex parte with such a person as to the merits of the cause except as permitted by law or court order; (c) communicate with a juror or prospective juror after discharge of the jury if: (1) the communication is prohibited by law, local rule, or court order; (2) the juror has made known to the lawyer a desire not to communicate; or (3) the communication involves misrepresentation, coercion, duress or harassment; or (d) engage in conduct intended to disrupt the tribunal."

[10] SCR 3.130(8.4) provides that it is "professional misconduct for a lawyer to assist or induce another to engage in conduct that violates the Rules of Professional Conduct."

[11] Comment 1 to Rule 8.4 provides: "Lawyers are subject to discipline when they violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so or do so through the acts of another, as when they request or instruct an agent to do so on the lawyer's behalf."

principles are clear. Every lawyer is bound by the Rules of Professional Conduct. Those rules prohibit a lawyer from misrepresenting material facts, or engaging in conduct involving dishonesty, fraud, deceit or misrepresentation. They also provide that a lawyer may not communicate with persons represented by counsel or state or imply disinterest in dealing with unrepresented persons. In addition, the rules prohibit improper contact with jurors. Finally, Rule 8.4(a) prohibits a lawyer from using a third person to engage in conduct that would violate the Rules of Professional Conduct, if done by a lawyer. A lawyer must keep all of these rules in mind when deciding the appropriate use of social network sites.

Note to Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. The Rule provides that formal opinions are advisory only.

Formal Ethics Opinion

KENTUCKY BAR ASSOCIATION

Ethics Opinion KBA E-437
Issued: March 21, 2014

The Rules of Professional Conduct are amended periodically. Lawyers should consult the current version of the rule and comments, SCR 3.130 (available at http://www.kybar.org/237), before relying on this opinion.

Use of Cloud Computing[1]

Question

May lawyers use cloud computing with clients' confidential information?

Answer

Yes. Lawyers may use cloud computing with clients' confidential information. In so doing, lawyers must follow the Rules of Professional Conduct with regard to

safeguarding client confidential information,
acting competently in using cloud computing,
properly supervising the provider of the cloud service, and
communicating with the client about cloud computing when such communication is necessary due to the nature of the representation.

References

SCR 3.130[Kentucky Rules of Professional Conduct] (1.1 & cmt. 6), (1.4(a) & (b)), (1.6(a) & cmt. 14, 15, & 16), (1.9(c)), (1.15(a)), (1.16), (1.18(b)), (5.3(a) & (b)); ABA Model Rules of Professional Conduct Rule 1.1, cmt. 8, Rule 1.6(c) & cmt. 18, Rule 5.3 cmt. 3; Fla. Eth. Op. 12-3(2013); Iowa Eth. Op. 11-10(2012); Me. Eth. Op. 207(2013); Mass. Eth. Op. 12-03(2012); N.H. Eth. Op. 2012-13/4(2012); N.Y. Eth. Op. 842 (2010); N.C. Eth. Op. 6 (2011); Ohio Informal Adv. Op. 2013-03(2013); Pa. Eth. Op. 2011-200(2011); Vt. Eth. Op. 2010-6(2010); Wash. Eth. Op. 2215(2012); *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations,* New York City Bar Ass'n, Committee on Small Law Firms (Nov. 2013), available at http://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf; Robert Ambrogi, *High in the Cloud: Firm Central Emphasizes Integration—At a Cost,* ABA Journal p. 30(Nov. 2013); Nicole Black & Matt Spiegel, *Breaking Down Cloud Computing,* available at http://apps.americanbar.org/litigation/committees/solo/articles/winter2013-0213-breaking-down-cloud-computing.html; Sharon D. Nelson & John W. Simek, *Have Attorneys Read the iCloud Terms and Conditions?,* Slaw(Jan. 30, 2012), available at http://www.slaw.ca/2012/01/30/have-attorneys-read-the-icloud-terms-and-conditions/.

Discussion

Technology provides an ever-changing environment in which to apply the Rules of Professional Conduct. Cloud computing is technology that allows a lawyer to store and access software or data though the software or data is stored and/or operated in the cloud—that is, a remote location that is not under the control of the lawyer but is controlled by a third party who provides the storage or other service. The service may be long-term storage of confidential client information or may be shorter-term storage or services to enable data processing or web-based email.[2]

Lawyers long have had "a duty to make reasonable judgments when protecting client property and information." Pa. Eth. Op. 2011-200(2011). This duty is the same whether the lawyer is selecting a security system to protect a bricks-and-mortar law office, selecting an offsite warehouse for the storing of client files, or selecting a provider of a service such as online storage for confidential client information.

Because technology evolves every day, we decline to mandate in this opinion specific practices regarding the protection of confidential client information in the world of the cloud. The reality is that such practices soon would be obsolete—and our opinion would be obsolete as well. Rather, we choose to guide lawyers in the exercise of reasonable judgment regarding the use of cloud technology. *See* Vt. Eth. Op. 2010-6(2010) (constantly changing nature of cloud technology makes establishing "specific conditions precedent" to use not appropriate); Ohio Informal Adv. Op. 2013-03(2013) ("applying existing principles to new technological advances while refraining from mandating specific practices—is a practical one").

Use of this technology by a lawyer is ethically proper if the lawyer abides by the Rules of Professional Conduct by safeguarding client confidential information, by acting competently in using cloud computing services, by properly supervising the provider of

[1] As another opinion states, cloud computing is "merely 'a fancy way of saying stuff's not on your computer.'" Pa. Eth. Op. 2011-200 (2011) (quoting Quinn Norton, *Byte Rights,* Maximum PC, Sept. 2012)). The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." See Nicole Black & Matt Spiegel, *Breaking Down Cloud Computing,* available at http://apps.americanbar.org/litigation/committees/solo/articles/winter2013-0213-breaking-down-cloud-computing.html.

[2] *See* Robert Ambrogi, *High in the Cloud: Firm Central Emphasizes Integration—At a Cost,* ABA Journal p. 30(Nov. 2013)(discussing cloud-based practice management products which allow the management of cases, clients, contacts, and calendars).

the cloud service, and by communicating with the client about use of cloud services when such communication is necessary given the nature of the representation.[3]

Confidential Information and Competence

Lawyers have a duty to protect confidential client information. SCR 3.130(1.6(a)) states the basic rule that "[a] lawyer shall not reveal information relating to the representation of the client unless the client gives informed consent, the disclosure is impliedly authorized or the disclosure is permitted by paragraph (b)." The permitted disclosures of paragraph (b) are not relevant here. SCR 3.130(1.9(c)) and SCR 3.130(1.18)(b)) make clear that the duty not to reveal information relating to the representation continues to apply when the client becomes a former client and applies to prospective clients as well, even after the prospective client has moved on. *See also* SCR 3.130(1.6 cmt.16) ("The duty of confidentiality continues after the client-lawyer relationship has terminated.").

Lawyers also have a duty to act with competence. SCR 3.130(1.1) states:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment six to SCR 3.130(1.1) states in part that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice." While Kentucky's competence rule, SCR 3.130(1.1) has not been modified since 2009, the ABA, in August of 2012, amended its version of this comment to state specifically that the duty of competence includes the duty to "keep abreast" of technology.[4] While the ABA comment is not controlling, it is helpful.

Comment fourteen to SCR 3.130(1.6) clarifies that a part of the lawyer's duty of competence is to "safeguard information relating to the representation of a client 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." As with storage of files in a bricks-and-mortar law office or in an off-site warehouse, client information stored in the cloud cannot be protected absolutely. Burglars can break into law offices and warehouses despite the utmost care to protect against such happenings. Likewise, sophisticated hackers can access online information despite the utmost care to protect confidential client information.

[3] Many jurisdictions have issued ethics opinions dealing with cloud computing. All of them approve of lawyer use of cloud computing but provide cautionary advice. *See, e.g.,* Fla. Eth. Op. 12-3(2013); Me. Eth. Op. 207(2013); Ohio Informal Adv. Op. 2013-03(2013); Iowa Eth. Op. 11-10(2012); Mass. Eth. Op. 12-03(2012); N.H. Eth. Op. 2012-13/4(2012); Wash. Eth. Op. 2215(2012); N.C. Eth. Op. 6(2011); Pa. Eth. Op. 2011-200(2011); N.Y. Eth. Op. 842(2010); Vt. Eth. Op. 2010-6(2010).

[4] The comment to ABA Model Rule of Professional Conduct Rule 1.1 states: "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." ABA Model Rules of Professional Conduct Rule 1.1 cmt. 8.

Comment fifteen to SCR 3.130(1.6) provides:

> 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.[5]

From these statements it is clear that a lawyer has a duty to take reasonable measures to protect confidential client information in any setting: bricks-and-mortar law office, offsite warehouse, or online storage or service site in the cloud.

Taking such reasonable measures is also consistent with the duty, as stated in SCR 3.130(1.15(a)), to "appropriately safeguard[]" the client's property.

When a lawyer selects a provider of any support service, the duty of competence, the duty to protect a client's property, and the duty of confidentiality require the lawyer to investigate the qualifications, competence, and diligence of the provider. A lawyer who

[5] The ABA amended its version of Rule 1.6 to state 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 the client." *See* ABA Model Rules of Professional Conduct Rule 1.6(c). The supporting comment language added by the ABA in August of 2012 states, in part:

> 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. 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. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

ABA Model Rules of Professional Conduct Rule 1.6 cmt. 18.

does not investigate whether a warehouse he or she is considering for the storage of files has adequate security to safeguard client files fails in his or her confidentiality and competence obligations to the client. Likewise, an attorney selecting an online provider of storage or other service must investigate the provider to be sure that client information is reasonably sure to remain confidential and secure.

Supervision

A lawyer has a duty to supervise nonlawyers engaged by the lawyer to assist the lawyer in practicing law. SCR 3.130(5.3(a)) states that with regard to a nonlawyer assistant, "[a] partner, 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 the person's conduct is compatible with the professional obligations of the lawyer." SCR 3.130(5.3(b)) states that a lawyer with "direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."

These rules require supervision of a provider of online storage just as they require supervision of an offsite provider of services such as a storage warehouse operator and just as they require supervision of a paralegal working within a bricks-and-mortar law firm. A lawyer must make "reasonable efforts" to ensure that the online storage provider's conduct "is compatible with the professional obligations of the lawyer." SCR 3.130(5.3(a)). This duty, though ongoing, is extremely important at the point that the lawyer selects the provider because it is at that point the lawyer must determine whether the provider is capable of conduct compatible with the lawyer's ethical responsibilities.[6]

Communication

SCR 3.130(1.4(a)) states that a lawyer must "reasonably consult with the client about the means by which the client's objectives are to be accomplished." While cloud computing does not always require client consultation, there may be situations in which consulting with the client may be proper. A lawyer must exercise judgment to determine if a particular client matter involves highly sensitive information such that the lawyer should consult with the client about the use of the cloud. *See also* Mass. Eth. Op. 12-03(2012)(lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so"); N.H. Eth. Op. 2012-13/4(2012) (informing the client "may become necessary" if particularly sensitive data is at issue); Pa. Eth. Op. 2011-200(2011) (communication with client may be necessary depending on the sensitivity of the information involved and the scope of the representation).

Issues to Consider in Light of the Lawyers Responsibilities

[6] Comment three to ABA Model Rules of Professional Conduct Rule 5.3, added in August 2012, specifically notes use of "an Internet-based service to store client information" as the kind of assistance a lawyer may have.

In order to abide by these duties a lawyer owes a client, a lawyer should investigate the provider's qualifications, the provider's reputation, and the provider's longevity as well as understand the nature of the service provided. Just as a lawyer should review the terms of storage for a warehouse for storage of client files, so too should a lawyer review the terms of the arrangement[7] regarding online storage or treatment of confidential client information or other cloud-based service. Some questions that a lawyer should consider[8] in this regard include the following:

What protections does the provider have to prevent disclosure of confidential client information?

Is the provider contractually obligated to protect the security and confidentiality of information stored with it?

Does the service agreement state that the provider "owns" the data stored by the provider?[9]

What procedures, including notice procedures to the lawyer, does the provider use when responding to governmental or judicial attempts to obtain confidential client information?

[7] The terms often are found in the "Service Level Agreement." *See* Sharon D. Nelson & John W. Simek, *Have Attorneys Read the iCloud Terms and Conditions?,* Slaw(Jan. 30, 2012), available at http://www.slaw.ca/2012/01/30/have-attorneys-read-the-icloud-terms-and-conditions/.

[8] This list is based on a list provided by the Ohio State Bar Association. *See* Ohio Informal Adv. Op. 2013-03(2013). Florida Ethics Opinion 12-3(2013) sets forth other issues to consider:

> As suggested by the Iowa opinion, lawyers must be able to access the lawyer's own information without limit, others should not be able to access the information, but lawyers must be able to provide limited access to third parties to specific information, yet must be able to restrict their access to only that information. Iowa Ethics Opinion 11-01 also recommends considering the reputation of the service provider to be used, its location, its user agreement and whether it chooses the law or forum in which any dispute will be decided, whether it limits the service provider's liability, whether the service provider retains the information in the event the lawyer terminates the relationship with the service provider, what access the lawyer has to the data on termination of the relationship with the service provider, and whether the agreement creates "any proprietary or user rights" over the data the lawyer stores with the service provider. It also suggests that the lawyer determine whether the information is password protected, whether the information is encrypted, and whether the lawyer will have the ability to further encrypt the information if additional security measures are required because of the special nature of a particular matter or piece of information. It further suggests that the lawyer consider whether the information stored
> via cloud computing is also stored elsewhere by the lawyer in the event the lawyer cannot access the information via "the cloud."

Fla. Eth. Op. 12-3 (2013) (referring to Iowa Eth. Op. 11-10(2012)). Me. Eth. Op. 207 (2013), N.C. Eth. Op. 6 (2011), and Pa. Eth. Op. 2011-200 (2011) have other lists.

[9] SCR 3.130(1.15(a)) provides that client property must be "identified as such and appropriately safeguarded." Any statement that the service provider owns the information is inconsistent with the demands of this rule.

At the conclusion of the relationship between the lawyer or law firm and the provider, will the provider return all information to the lawyer or law firm?

Does the provider keep copies of the confidential client information after the relationship is concluded or the lawyer or law firm has removed particular client information from the provider?

What are the provider's policies and procedures regarding emergency situations such as natural disasters and power interruption?

Where, geographically, is the server used by the provider for long-term or short-term storage or other service located?[10]

Conclusion

A lawyer may use cloud-based services with regard to confidential client information. In using cloud-based services, a lawyer must use reasonable care to assure that client confidentiality is protected and client property is safeguarded. *See* SCR 3.130(1.6(a)) & (1.15(a)). A lawyer must act consistent with his or her duty of competence in selecting and monitoring the providers of cloud-based services. *See* SCR 3.130(1.1). A lawyer must use "reasonable efforts" to ensure that the conduct of providers of cloud-based services assisting him or her is compatible with ethical obligations of the lawyer, and, if the lawyer is a partner or otherwise has managerial authority in a law firm, the lawyer must use "reasonable efforts" to make sure that the firm has measures in place to assure that providers of cloud-based services engage in conduct compatible with ethical obligations of the lawyer. *See* 3.130(5.3(a) & (b)). Finally, a lawyer must consult with the client about the use of the cloud if the matter is sufficiently sensitive such that the duty to "reasonably consult with the client about the means by which the client's objectives are to be accomplished" is implicated. *See* SCR 3.130(1.4(b)).[11]

---

[10] Lawyers should be aware that search and seizure law as well as the law relating to ownership of information stored electronically on a server may vary greatly by country.

[11] For an in-depth but practitioner-oriented discussion of cloud use, see *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations,* New York City Bar Ass'n, Committee on Small Law Firms (Nov. 2013), available at http://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf.

Note to Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. This Rule provides that formal opinions are advisory only.

Formal Ethics Opinion
KENTUCKY BAR ASSOCIATION

Ethics Opinion KBA E-442
Issued: November 17, 2017

The Rules of Professional Conduct are amended periodically. Lawyers should consult the current version of the rule and comments, SCR 3.130 (available at http://www.kybar.org/237), before relying on this opinion.

Question 1: When an attorney (Lawyer A) sends an email to another lawyer (Lawyer B) and Lawyer A sends a copy of such communication to Lawyer A's client, should Lawyer A's action be regarded as giving Lawyer B consent to use the "reply all" function when replying to Lawyer A?

Answer: No

Authorities: SCR 3.530 (4.2), North Carolina State Bar Formal Ethics Opinion 7 (2013), Association of the Bar of the City of New York Formal Opinion 2009-1, Restatement of the Law Governing Lawyers, section 99, comment j.

Question 2: When Lawyer A sends an email to Lawyer B with copy of such email being sent to Lawyer A's client, does the act of sending the client a copy of the email reveal "information relating to the representation of the client?"

Answer: Yes

Authority: SCR 3.530 (1.6(a))

Question 3: What precautions should an attorney take in using the "reply all" button?

Answer: See opinion

Discussion

1) If a lawyer (Lawyer A) sends an email to another lawyer (Lawyer B), who is not affiliated with Lawyer A, and copies Lawyer A's client by using "cc," Lawyer B should not correspond directly with Lawyer A's client by use of the "reply all" key. A lawyer who, without consent, takes advantage of "reply all" to correspond directly with a represented party violates Rule 4.2.

Further, showing "cc" to a client on an email, without more, cannot reasonably be regarded as consent to communicate directly with the client. In North Carolina State Bar Formal Ethics Opinion 7 (2013), the Committee opined:

> There are scenarios where the necessary consent may be implied by the totality of the facts and circumstances. However, the fact that a lawyer copies his own client on an electronic communication does not, in and of itself, constitute implied consent to a "reply to all" responsive electronic communication. Other factors need to be considered before a lawyer can reasonably rely on implied consent. These factors include, but are not limited to: (1) how the communication is initiated; (2) the nature of the matter (transactional or adversarial); (3) the prior course of conduct of the lawyers and their clients; and (4) the extent to which the communication might interfere with the client-lawyer relationship.

In Formal Opinion 2009-1 the Association of The Bar of The City Of New York, Committee on Professional and Judicial Ethics opined that the no-contact rule (DR 7-104(A) (1)) prohibits a lawyer from sending a letter or email directly to a represented person and simultaneously to her counsel, without first obtaining "prior consent" to the direct communication or unless otherwise authorized by law. Further, prior consent to the communication means actual consent. The New York Bar advised that while consent may be inferred from the conduct of the represented person's lawyer, a lawyer communicating with a represented person without first securing the other lawyer's express consent runs the risk of violating the no-contact rule. (Emphasis added.) This Committee agrees with the opinions of North Carolina and New York and endorses their use for Kentucky lawyers.

2) Showing another lawyer that a copy of an email is being sent to a lawyer's client reveals the following information relating to the lawyer's representation: 1) the identity of the client; 2) the client received the email including attachments, and 3) in the case of a corporate client, the individuals the lawyer believes are connected to the matters and the corporate client's decision makers. Hence, it is best to avoid a problematic result by not sending and showing a copy of the sending lawyer's email to the sending lawyer's client. Of course, "cc"ing a client does not violate Rule 1.6, if the client expressly or impliedly consents to the limited disclosure of "information related to the representation."

3) To avoid the problems identified in (1) and (2), attorneys should either forward their emails to their client or use their system's blind carbon copy feature ("bcc"), after first assuring that the "reply all" feature is limited to those in the "cc" line. Sending a blind copy to the client ("bcc) or forwarding the email to the client protects a confidential communication (sending the copy to client), avoids inappropriate confusion, and forecloses an implied consent argument. If Lawyer A wants Lawyer B to know that Lawyer A's client has been informed of the communication, then Lawyer A may either so advise Lawyer B of such fact or, if deemed necessary, show that a copy of the email communication is being made to Lawyer A's client, while at the same time giving clear written notice to Lawyer B that Lawyer B is not authorized to respond or communicate with Lawyer A's client.

Avoiding use of "cc" also prevents the client to inadvertently communicate with opposing counsel by hitting the "reply all." key. A proposed (2017) amendment to comment 6 to Rule 1.7 would add "the risks and benefits of technology" to lawyers' obligations to maintain the requisite knowledge and skill. The "reply all" button presents a dangerous risk to the sending lawyer because the sender might inadvertently send an embarrassing or harmful email to unintended recipients. The web contains many examples of funny, embarrassing or harmful uses of "reply all." In addition to "think before you reply," the Wall Street Journal suggests:

> If the system allows customization of the toolbar. "Reply All" can be made more difficult to use accidentally by moving it away from the Reply button. Organizations can also install add-ons for Outlook which prompt people when they are using Reply All. Similar to the helpful, "Are you sure you want to delete this?" or the "is the attachment actually attached" pop-ups, this add-on wants confirmation before enabling Reply All, giving senders the chance to reconsider whether that's really their intention. (Let's Make it Harder to Use "Reply All," Wall Street Journal, November 13, 2016).

Note To Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. This Rule provides that formal opinions are advisory only.

Formal Ethics Opinion
KENTUCKY BAR ASSOCIATION

Ethics Opinion KBA E-446
Issued: July 20, 2018

The Rules of Professional Conduct are amended periodically. Lawyers should consult the current version of the rule and comments, SCR 3.130 (available at http://www.kybar.org/237), before relying on this opinion.

Subject: Cybersecurity

Question #1: Does an attorney have an ethical responsibility to implement cybersecurity measures to protect clients' information?

Answer: Yes

Question #2: Does an attorney have an ethical responsibility to advise clients about cyberattacks against the law practice and/or breaches of security?

Answer: Qualified Yes.

Question #3: Can an attorney utilize third parties and/or non-lawyers to plan and implement cybersecurity measures?

Answer: Yes.

Question #4: Does an attorney have an ethical responsibility to ensure that law firm employees, as well as third parties employed by, retained by, or associated with the lawyer, comply with the attorney's cybersecurity measures?

Answer: Yes.

INTRODUCTION

An attorney's use of technology in the practice of law has evolved considerably since this Committee first addressed communicating with clients through electronic mail services in 1998.[1] Since that time, Ethics Opinions have discussed the use of domain names,[2] cloud computing,[3] and most recently, communications between attorneys by email.[4] As noted previously, "Technology provides an ever-changing environment in which to apply the Rules of Professional Conduct."[5] Whether an attorney uses email to communicate with clients; e-files documents with the courts; stores client information electronically; shares files with others; employs mobile devices and/or accesses the internet, care must be taken to avoid disclosure of confidential client information.

As technology has evolved, so has the ability of third parties to attack or 'hack' a lawyer's electronic systems, not only to obtain confidential client information, but also to disrupt the law firm's operations by threatening to destroy client files to collect ransom payments. "Creating, using, communicating, and storing information in electronic form greatly increases the potential for unauthorized access, use, disclosure and alteration, as well as the risk of loss or destruction (of client information)."[6] Attorneys must therefore be cognizant of cybersecurity measures that can be employed to preserve their client's information.

Unfortunately attorneys are consider 'easy targets' for cyberattacks.[7] If 'techno-challenged', or even 'technophobic', the lawyer may not appreciate the cyber risk of electronically communicating with clients, and/or storing collected client information on the law firm's computer systems. Further, the technology employed by an attorney to protect from unauthorized access, theft, or destruction of client information may not be as sophisticated as the client's own cyber defenses. Moreover, while solo practitioners or small law firms may think they are immune to cyber attacks, the size of a law firm doesn't matter when it comes to cyberattacks. Instead, the 'sophistication or lack thereof' of the attorney's computer system becomes the issue. As learned from the 'Panama Papers' breach, even the largest of law firms whom one would believe would have tech-savy security in place to prevent 'hacks', are not exempt from cyber attacks.[8]

In 2012, the American Bar Association ("ABA") established a "Cybersecurity Legal Task Force" that recommended 'technology amendments' to the Model Rules of Professional Conduct ("Model Rules") 1.0; 1.6; and 4.4. Those amendments were subsequently approved by the ABA House of Delegates to specifically provide information and guidance to attorneys on use of electronic communications; intrusions on a law firm's systems and networks; and ethical obligations to protect a client's confidential information. The ABA Standing Committee on Ethics and Professional Responsibility subsequently issued Formal Opinion 477R on May 22, 2017, that

---

[1] KBA Ethics Opinion KBA E-403.

[2] KBA Ethics Opinion KBA E-427.

[3] KBA Ethics Opinion KBA E-437.

[4] KBA Ethics Opinion E-442.

[5] Id.

[6] ABA Cybersecurity Legal Task Force & Section of Science & Technology Law, Report to the House of Delegates: Resolution 109 A.B.A. 4 (August 2014) ("Cybersecurity Resolution").

[7] Jane LeClaire & Gregory Keeley, Cybersecurity in Our Digital Lives (2013) at 128.

[8] "... (T)he Mossack Fonseca (law firm) attack was *dead simple*. So simple, in fact, that a teenager with no hacking knowledge other than basic googling skills could have done it... Furthermore, the security mistakes Mossack Fonesca made were *appallingly common.* So common, in fact, that it's fair to say most of the readers of this article work for organizations that are making at least one of the same mistakes." Jason Bloomberg, "Cybersecurity Lessons Learned from 'Panama Papers' Breach, Forbes Tech Journal (April 21, 2016).

interpreted these amendments to the Model Rules to further explain ethical issues involving the use of electronic means to communicate regarding client matters.[9] While the Kentucky Supreme Court did not adopt the ABA Model Rules, nor has it amended the Kentucky Rules of Professional Conduct ("Rules") [10] to discuss technology issues as the ABA has done, the discussion in Formal Opinion 477R provides a background to an attorney seeking guidance on technology issues impacting confidentiality of client communications.

DISCUSSION

Question 1: An attorney's ethical responsibility to implement cybersecurity measures to protect clients' information is founded upon four (4) separate requirements of the Rules as they relate to competence (SCR 1.1(6)); communications (1.4); confidentiality of information (1.6) and safekeeping of client's property (1.15). Paramount among these ethical obligations is the requirement to "... not reveal information relating to the representation of a client unless the client gives informed consent."[11] The Commission has previously acknowledged that this provision not only applies to traditional paper communications, but it also applies to the use of emails with clients and opposing counsel, as well as the storing of client information 'in the cloud'. Above all, the attorney must use 'reasonable care' to ensure that the client's confidential information is protected, and that the client's property is safeguarded.[12]

Comment (8) to ABA Model Rule 1.1 states that for an attorney to maintain the 'requisite knowledge and skill' required by this provision of the Model Rule, the attorney must keep abreast of the changing risks and benefits of relevant technology[13]. Effective January 1, 2018, the Kentucky Supreme Court similarly revised its "Maintaining Competence" Commentary (6) of SCR 3.130 (1.1) to include "... the benefits and risks associated with relevant technology...." Further, KBA Opinion E-437 makes it clear that Kentucky lawyers should be competent in the use of technology in their law practices. This 'competence requirement' includes the knowledge of traditional cyber defense tools to protect client data. Thus, "(b)ecause the protection of confidentiality is an element of competent lawyering, a lawyer should not use any particular mode of technology to store or transmit confidential information before considering how secure it is, and whether reasonable precautions such as firewalls, encryption, or password protection could make it more secure."[14]

It should be noted that the type of communication with a client, and/or the method of storing a client's data may require different levels of security. "At the beginning of the client-lawyer relationship, the lawyer and the 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 communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required."[15]

Due to the constant changing of technology, it is impossible to give specific requirements of what constitutes 'reasonable efforts' by an attorney to prevent cybersecurity breaches.[16] What is 'reasonable' depends upon the facts and circumstances taken to prevent access or disclosure of confidential information. Comment 18 to the Model Rules provides some guidance:

> "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 (eg. By making a device or important piece of software excessively difficult to use)"

By no means, however, is an attorney ethically held to a 'strict liability' standard in efforts to prevent cyber attacks. Nor do we mandate specific measures or suggested safeguards that an attorney must take to avoid 'hacks' in order to satisfy this ethical responsibility.[17] Instead, this Opinion updates historically held ethics guidelines for keeping client information confidential in light of the ever-changing use of technology in the practice of law.

Furthermore, as an attorney is under a continuing obligation pursuant to SCR 3.130

---

[9] For an extensive discussion of this topic, refer to the ABA Cyberscurity Handbook: A Resource for attorneys, law firms, and business professionals (2nd Edition) by Jill D. Rhodes and Robert S. Litt (2018)

[10] SCR 3.130 et seq.

[11] SCR 3.130 (1.6).

[12] See, KBA Ethics Opinion E-437; For a discussion of this Opinion and its practical application to the practice of law, see "Ethics Still Apply: Even When Your Head Is In The Cloud", Lawyers Mutual Insurance Company of Kentucky Risk Management (2016).

[13] The ABA stated that the change to Model Rule 1.1 did not create a 'new requirement' for an attorney, but instead made explicit what was previously considered 'implicit' in the Model Rule; See also, "Andrew Perlman, "The Twenty First Century Lawyer's Evolving Ethical Duty of Competence", The Professional Lawyer, Vol. 22, No. 4.

[14] California State Bar Opinion 2010-179 (undated).

[15] ABA Formal Opinion 477R at 7.

[16] For a discussion of Data Breach Cyber Security Risk Management see "Attorney's Liability for Data Breaches" Lawyers Mutual Insurance Company of Kentucky Risk Management (2016).

[17] See, Arizona State Bar Opinion 09-04 (2009) which tells attorneys who store client information to consider firewalls, password protection schemes, encryption, certain anti-virus measures, etc.

(1.1) to "... keep abreast of changes in the law and its practice ..."[18] so too is the attorney to undertake continuing technology education to increase cyber-preparedness, and to continually reevaluate policies and procedures in place to minimize data breaches of a client's confidential information.

Question 2: An attorney is required to "... reasonably consult with the client about the **means** by which the client's objectives are to be accomplished."[19] The 'means' employed by the attorney includes discussing the use of technology in client communications, the handling of confidential client information within the law firm, and the storage of that information.[20]

Further, an attorney is required to " . . . keep the client reasonably informed about the status of the matter (that the attorney is handling for the client."[21] The Commentary to this Rule[22] explains that this includes telling the client about 'significant developments' affecting the time or the substance of the representation. While an attorney is allowed to withhold certain information from the client in limited circumstances, "(a) lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person."[23]

SCR 3.130(1.4) does not mandate the disclosure to a client about general cyber attacks against the law firm, or breaches of security within an attorney's computer systems. However, if there is a disclosure of the client's specific confidential and/or privileged information to third parties, which we believe would constitute a 'significant development' affecting the client's representation, then a disclosure must be made to the client about this development.

We are further mindful of KRS 365.732 which imposes a statutory duty upon an 'information holder'[24] to give written notice to persons affected by a computer security 'breach' involving their unencrypted 'personally identifiable information'. While this statute does not establish a cause of action for a violation, KRS 446.070 allows a person injured by the violation of any Kentucky statute to recover damages sustained as a result of that violation. Thus, if an attorney failed to disclose to the client a breach involving the client's unencrypted personally identifiable information then the attorney may be unethically withholding that information to protect the lawyer's own interest to avoid a lawsuit or an ethical charge by the client.

Similarly, the duty imposed by SCR 3.130 (1.15) to 'safekeep' a client's 'property' not only applies to a trust account in which a client's funds are maintained, but also to the client's files; client data stored on the law firm's computer system or 'the cloud'; and the client's intellectual property retained by the attorney because of pending matters. The Commentary to this Rule explains: "A lawyer should hold property of others with the care required of a professional fiduciary." Accordingly, the theft or loss of a client's funds or property as a result of a cyberattack must also be disclosed to the client.

Question 3: An attorney may not delegate ethical responsibilities to third parties. However, when the attorney lacks sufficient information, education and/or training to comply with the Rules, then the attorney should seek assistance from others, including nonlawyers and/or support services. "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."[25]

Due to the rapid change of cybersecurity options, an attorney may determine that taking 'reasonable measurers' to avoid a theft or loss of confidential client information includes contracting with a professional to create and/or maintain the cybersecurity plan for the law firm. "When a lawyer selects a provider of any support services, the duty of competence, the duty to protect a client's property, and the duty of confidentiality require the lawyer to investigate the qualifications, competence and diligence of the provider.[26] A lawyer who does not investigate whether a warehouse he or she is considering for the storage of files had adequate security to safeguard client files fails in his or her confidentiality and competence obligations to the client. Likewise, an attorney selecting an online provider of storage or other services must investigate the provider to be sure that client information is reasonably sure to remain confidential and secure."[27]

Notably, each attorney within a law firm does not need to personally have all of the requisite technology competencies to meet this ethical responsibility. The lawyer can utilize another attorney within the law firm, the expertise of the law firm's nonlawyer staff, and/or outside experts to comply. "Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this[28] subject."

Question 4: Partners or managers of attorneys, as well as supervisory lawyers, are required under the Rules to make 'reasonable efforts' to ensure that those lawyers that they manage or supervise

---

[18]Supreme Court Commentary (6).

[19]SCR 3.130 (1.4)(a)(2).

[20]See, KBA Opinion E-437 discussing with a client the attorney's use of the cloud if the client's matter is sufficiently sensitive.

[21]SCR 3.130(1.4).

[22]Commentary (3) to SCR 3.130 (1.4).

[23]Commentary (7) to SCR 3.130 (1.4).

[24]KRS 365.732(1) (b) defines an 'information holder' as "... any person or business entity that conducts business in this state."

[25]ABA Formal Opinion 477R at 9.

[26]For a discussion of what information lawyers should consider in this regard, refer to KBA Opinion E-437 at 6; See also, ABA Formal Opinion 08-451 regarding outsourcing legal and nonlegal services.

[27]Id. at 4-5.

[28]ABA Cybersecurity Handbook, supra at 66.

conform to the Rules.[29] That requirement extends to nonlawyers or assistants employed or retained by, or associated with, a lawyer . Thus, the attorney who has direct supervisory over the nonlawyer must ensure their conduct complies with the Rules.[30]

At the same time, lawyers who have managerial authority within a law firm are required to make " ... reasonable efforts to establish internal policies and procedures designed to provide reasonable assurances that nonlawyers in the firm will act in a way compatible with the Rules...." [31] While all lawyers have a duty to evaluate their client data and systems and take reasonable steps to secure confidential information, attorneys who have managerial roles have the added duty of evaluating and correcting security issues within the law firm and prescribing policies and procedures to reduce cyber threats. Having an effective data security program will reduce the risk of confidential client information being disclosed for all lawyers in the law firm.

The Opinion does not mandate the specific policies or procedures that an attorney must employ to have an effective data security program, nor does it contend that there is a 'one shoe fits all' solution for every attorney for cybersecurity. Instead, each attorney must understand what devices the law firm uses that are connected to the office network or the internet; how client information is exchanged or stored through that system and who has access to the data, and make 'reasonable efforts' to combat cyber threats. An attorney's policies will thus depend upon an attorney's use of electronics; the method used to communicate with clients and the nature of the client's information.[32] "These requirements are as applicable to electronic practices as they are to comparable office procedures."[33]

Establishing policies and procedures for cybersecurity alone, however, does not end the partner, attorney manager or supervising attorney's responsibility under the Rules. Implementation of the policies and procedures, specific training for employees on those policies and ongoing supervision is warranted. Because a law firm's data security practices are only as strong as its weakest link " (all lawyers) must make sure that subordinate attorneys, interns, paralegals, case managers, administrative assistants, and external business partners all understand necessary data security practices and the critical role that all parties play in ensuring the protection of client information."[34]

---

[29]SCR 3.130 (5.1).

[30]SCR 3.130 (5.3).

[31]Commentary (2) to SCR 3.130 (5.3); See also Commentary (2) to SCR 3.130 (5.1).

[32]For a thorough discussion of this topic, refer to the Cybersecurity For The Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security by John Bandler (American Bar Association Section of Science & Technology, 2017).

[33]ABA Formal Opinion 477R at 9.

[34]Drew T. Simshaw, "Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data", 38 Am. J. Trial Advocacy, 549, 550, 554 (2015).

Note To Reader

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. This Rule provides that formal opinions are advisory only.

Disclosure of client confidential information in a blog or other social media

1) In a blog or other social media, may a lawyer disclose information relating to the representation of a current or former client without the client's consent?

Answer: No

Authority: SCR 3.130 (1.9 (c)(2)) and comment 16; KBA E-253; SCR 3.130(1.6(a)) and comment 4; KBA E-253; Hudson, Client Consent is Key, May 2018 ABA Journal, p. 24; *In re Smith*, 991 N.E.2d 106 (Ind. 2013); *Office of Lawyer Regulation v. Pershek*, 798 NW2d 879 (Wis. 2011);

2) May an attorney reveal the identity of a current or former client in a blog or other social media without the client's consent?

Answer: No. See opinion

Authority: E-253.

3) Is there an exception to (1) or (2) for information contained in a public record?

Answer: No. See opinion.

Authority: SCR 3.130(1.6(a)) and comment 4; KBA E-253; Hudson, *Client Consent is Key*, May 2018 ABA Journal, p. 24.

Discussion:

SCR 3.130(1.6(a)) defines confidential information as "information relating to the representation of a client," a broader definition than is found in the ABA Model Code of Professional Responsibility and the Restatement of the Law Governing Lawyers. The Model Code (DR 4-101) and the Restatement (sec. 60) limit lawyers' duty of non-disclosure to communications protected by the attorney-client privilege and information that might work to clients' disadvantage. Rule 1.6(a) of the ABA Model Rules of Professional Conduct, on which SCR 3.130(1.6)(a) is based, is not so limited. Unless one of the exceptions in Rule 1.6(b) applies, Rule 1.6(a) requires a lawyer to obtain client consent before disclosing *any* information relating to the client's representation.

In KBA E-253, applying DR 4-101(C) of the Model Code of Professional Responsibility, the Committee opined that, absent consent, a lawyer may reveal names and addresses of clients only: 1) where the information is in the public record as a result of the attorney's representation; or 2) where the circumstances make it obvious that the client does not expect confidentiality as to the existence of the attorney client relationship, or 3) where the client has specifically authorized in writing the release of the information.

In E-253, the Committee opined that a lawyer may reveal a client's name and address if it is *obvious* that the client does not expect name and address to be confidential. Clients' names and addresses should be presumed to be confidential. While decided under the old Code, E-253 is sensible and, we believe, consistent with prevailing practice.

Without client consent, Attorneys may reveal names and addresses (and the nature of the representation) where *necessary* to facilitate a firm merger or lateral transfer (KBA E-443), and there may be other situations in which attorneys should be permitted to reveal client information. As examples, in comment h to Section 60 of the Restatement, the American Law Institution cited cooperating with other lawyers with similar issues, for example personal injury lawyers with products liability claims, and "cooperating with reasonable efforts to obtain information about clients and law practice for public purposes such as historical research," for example a biography of a deceased client.

However, there is no justification for revealing information, without consent, about past or present clients in a blog or other social media. In *Office of Lawyer Regulation v. Pershek*, 798 N.W.2d 879 (Wis. 2011), the attorney was suspended for blogging about her clients; in *In re Smith*, 991 N.E.2d 106 (Ind. 2013), the attorney was disbarred for writing a book about a former client. The disciplinary cases involve negative disclosures, but the rule against disclosure applies to all information, whether positive, neutral or negative.

Attorneys should be careful in using thinly disguised hypotheticals. "A violation of Rule 1.6(a) is not avoided by describing public commentary as a 'hypothetical' if there is a reasonable likelihood that a third party may ascertain the identity or situation of the client from the facts set forth in the hypothetical." ABA Formal Op. 480.

A lawyer's duty of confidentiality extends to both current and former clients. SCR 3.130(1.9)(c)(2) requires that a lawyer not reveal information relating to the lawyer's representation of a client except as the Rules would permit or require with respect to a client. Hence, a lawyer may not reveal confidential client information even though such information may be contained in a public record. However, a lawyer may use information relating to the representation of a former client if the information has become "generally known." See SCR 3.130(1.9)(c)(1) and ABA Formal Opinion 479.

Proposed self-defense opinion (March 2019)

Question: May a lawyer reveal client confidential information reasonably necessary to respond to a former client's public criticism?

Answer: No

Authorities: Rule 1.6 (b)(3),Crystal, Defending Against Internet Criticism: "Silence is Golden, 26 South Carolina Lawyer 12 (2014); Fucile, Discretion in the Bette Part of Valor: Rebutting Negative Online Client interviews, 83 Defense Counsel J. 84 (2016); People v. Issac, 2016 WL 6124510 (Col. 2016); State ex rel Counsel for the Nebraska Supreme Court v. Tonderum, 840 N.W. 487 (Nebraska 2013).

Question: How may a lawyer ethically respond to a former client's public criticism?

Answer: See Opinion

The self-defense exception to the duty of confidentiality (1.6(b)(3)is triggered by claims or disciplinary complaints against a lawyer. The exception does not encompass internet criticism. In Defending Against Internet Criticism: Silence is Golden, 26 South Carolina Law Review 12(2014), Nathan Crystal uses the Betty Tsamis case to illustrate: After being fired a flight attendant hired Tsamis to seek unemployment benefits from the state. Apparently Tsamis learned after she was hired that the attendant had been fired because he beat up a female co-worker. After a hearing the claim was denied and the attendant complained about Tsamis on the internet. This eventually resulted in Tsamis being publicly reprimanded for posting the following:

> This is simply false. The person did not reveal all the facts of the situation up front in our first and second meetings. . . . Despite knowing he would likely lose he chose to go forward with a hearing to try to obtain benefits. I dislike it very much when my clients lose but I cannot invent positive facts for clients when they are not there. I fell badly for him but his own actions in beating up a female coworker are what caused the consequences he is now so upset about.

In most instances the best advice is to ignore the criticism. For the lawyer who wants to respond, the Committee recommends the following:

> My professional and ethical responsibilities do not allow me to reveal confidential client information in response to _____

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion No. 99-413
March 10, 1999

Protecting the Confidentiality of Unencrypted E-Mail

A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail. A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation.

The Committee addresses in this opinion the obligations of lawyers under the Model Rules of Professional Conduct (1998) when using unencrypted electronic mail to communicate with clients or others about client matters. The Committee (1) analyzes the general standards that lawyers must follow under the Model Rules in protecting "confidential client information"[1] from inadvertent disclosure; (2) compares the risk of interception of unencrypted e-mail with the risk of interception of other forms of communication; and (3) reviews the various forms of e-mail transmission, the associated risks of unauthorized disclosure, and the laws affecting unauthorized interception and disclosure of electronic communications.

The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy. The level of legal protection accorded e-mail transmissions, like that accorded other modes of electronic communication, also supports the reasonableness of an expectation of privacy for unencrypted e-mail transmissions. The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law.[2]

The Committee concludes, based upon current technology and law as we are informed of it, that a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a) in choosing that mode to communicate. This is principally because there is a reasonable expectation of privacy in its use.

The conclusions reached in this opinion do not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of e-mail,[3] just as they would warrant the avoidance of the telephone, fax, and mail. See Model Rule 1.1 and 1.4(b). The lawyer must, of course, abide by the client's wishes regarding the means of transmitting client information. See Model Rule 1.2(a).

A. Lawyers' Duties Under Model Rule 1.6

The prohibition in Model Rule 1.6(a) against revealing confidential client information absent client consent after consultation imposes a duty on a lawyer to take reasonable steps in the circumstances to protect such information against unauthorized use or disclosure.[4] Reasonable steps include choosing a means of communication in which the lawyer has a reasonable expectation of privacy.[5] In order to comply with the duty of confidentiality under Model Rule 1.6, a lawyer's expectation of privacy in a communication medium need not be absolute; it must merely be reasonable.

It uniformly is accepted that a lawyer's reliance on land-line telephone, fax machine, and mail to communicate with clients does not violate the duty of confidentiality because in the use of each medium, the lawyer is presumed to have a reasonable expectation of privacy.[6] The Committee now considers whether a lawyer's expectation of privacy is any less reasonable when she communicates by e-mail.

B. Communications Alternatives To E-Mail

In order to understand what level of risk may exist without destroying the reasonable expectation of privacy, this Section evaluates the risks inherent in the use of alternative means of communication in which lawyers nonetheless are presumed to have such an expectation. These include ordinary U.S. mail; land-line, cordless, and cellular telephones; and facsimile transmissions.

1. U.S. and Commercial Mail

It uniformly is agreed that lawyers have a reasonable expectation of privacy in communications made by mail (both U.S. Postal Service and commercial). This is despite risks that letters may be lost, stolen or misplaced at several points between sender and recipient. Further, like telephone companies, Internet service providers (ISPs), and on-line service providers (OSPs), mail services often reserve the right to inspect the contents of any letters or packages handled by the service. Like e-mail, U.S. and commercial mail can be intercepted and disseminated illegally. But, unlike unencrypted e-mail, letters are sealed and therefore arguably more secure than e-mail.[7]

2. Land-Line Telephones

It is undisputed that a lawyer has a reasonable expectation of privacy in the use of a telephone.[8]

For this reason, the protection against unreasonable search and seizure guaranteed by the Fourth Amendment applies to telephone conversations.[9] It also is recognized widely that the attorney-client privilege applies to conversations over the telephone as long as the other elements of the

privilege are present.[10] However, this expectation of privacy in communications by telephone must be considered in light of the substantial risk of interception and disclosure inherent in its use. Tapping a telephone line does not require great technical sophistication or equipment, nor is the know-how difficult to obtain.[11]

Multiple extensions provide opportunities for eavesdropping without the knowledge of the speakers. Technical errors by the phone company may result in third parties listening to private conversations. Lastly, phone companies are permitted by law to monitor phone calls under limited conditions.

Despite this lack of absolute security in the medium, using a telephone is considered to be consistent with the duty to take reasonable precautions to maintain confidentiality.[12]

3. Cordless and Cellular Phones

Authority is divided as to whether users have a reasonable expectation of privacy in conversations made over cordless and cellular phones.[13] Some court decisions reached the conclusion that there is no reasonable expectation of privacy in cordless phones in part because of the absence, at the time, of federal law equivalent to that which protects traditional telephone communications.[14] After the 1994 amendment to the Wiretap Statute, which extended the same legal protections afforded regular telephone communications to cordless phone conversations,[15] at least one ethics opinion addressed the advisability of using cordless phones to communicate with clients and concluded that their use does not violate the duty of confidentiality.[16]

The nature of cordless and cellular phone technology exposes it to certain risks that are absent from e-mail communication. E-mail messages are not "broadcast" over public airwaves.[17] Cordless phones, by contrast, rely on FM and AM radio waves to broadcast signals to the phone's base unit, which feeds the signals into land-based phone lines. Therefore, in addition to the risks inherent in the use of a regular telephone, cordless phones also are subject to risks of interception due to their broadcast on radio signals that may be picked up by mass-marketed devices such as radios, baby monitors, and other cordless phones within range.[18] Further, the intercepted signals of cordless and analog cellular telephones are in an instantly comprehensible form (oral speech), unlike the digital format of e-mail communications.

Similarly, cellular phones transmit radio signals to a local base station that feeds the signals into land-based phone lines. The broadcast area from the phone to the station is larger than that of a cordless phone, and receivers and scanners within range may intercept and overhear the conversation. Although the Committee does not here express an opinion regarding the use of cellular or cordless telephone, it notes that the concerns about the expectation of privacy in the use of cordless and cellular telephones do not apply to e-mail transmitted over land-based phone lines.[19]

4. Facsimile

Authority specifically stating that the use of fax machines is consistent with the duty of confidentiality is absent, perhaps because, according to some commentators, courts assume the conclusion to be self-evident.[20] Nonetheless, there are significant risks of interception and disclosure in the use of fax machines. Misdirection may result merely by entering one of ten digits incorrectly. Further, unlike e-mail, faxes often are in the hands of one or more intermediaries before reaching their intended recipient, including, for example, secretaries, runners, and mailroom employees. In light of these risks, prudent lawyers faxing highly sensitive information should take heightened measures to preserve the communication's confidentiality.

C. Characteristics Of E-Mail Systems

The reasonableness of a lawyer's use of any medium to communicate with or about clients depends both on the objective level of security it affords and the existence of laws intended to protect the privacy of the information communicated. We here examine the four most common types of e-mail and compare the risks inherent in their use with those of alternative means of communication, including the telephone (regular, cordless and cellular), fax, and mail.

Like many earlier technologies, "e-mail" has become a generic term that presently encompasses a variety of systems allowing communication among computer users. Because the security of these e-mail systems is not uniform, the Committee here evaluates separately the degree of privacy afforded by each. As set forth below, we conclude that a lawyer has a reasonable expectation of privacy in such use.

1. "Direct" E-Mail[21]

Lawyers may e-mail their clients directly (and vice versa) by programming their computer's modem to dial their client's. The modem simply converts the content of the e-mail into digital information that is carried on land-based phone lines to the recipient's modem, where it is reassembled back into the message. This is virtually indistinguishable from the process of sending a fax: a fax machine dials the number of the recipient fax machine and digitally transmits information to it through land-based phone lines. Because the information travels in digital form, tapping a telephone line to intercept an e-mail message would require more effort and technical sophistication than would eavesdropping on a telephone conversation by telephone tap.

Based on the difficulty of intercepting direct e-mail, several state bar ethics opinions and many commentators recognize a reasonable expectation o privacy in this form of e-mail.[22] Further, in two recent federal court decisions, the attorney-client and work-product privileges were considered applicable to e-mail communications.[23] The Committee agrees that there is a reasonable expectation of privacy in this mode of communication.

2. "Private System" E-Mail

A "private system" includes typical internal corporate e-mail systems and so-called "extranet" networks in which one internal system directly dials another private system. The only relevant distinction between "private system" and "direct" e-mail is the greater risk of misdirected e-mails in a private system. Messages mistakenly may be sent throughout a law firm or to unintended recipients within the client's organization. However, all members of a firm owe a duty of

confidentiality to each of the firm's clients.[24] Further, unintended disclosures to individuals within a client's private e-mail network are unlikely to be harmful to the client.

The reliance of "private system" e-mail on land-based phone lines and its non-use of any publicly accessible network renders this system as secure as direct e-mail, regular phone calls, and faxes. As a result, there is a widespread consensus that confidentiality is not threatened by its use,[25] and the Committee concurs.

3. On-line Service Providers

E-mail also may be provided by third-party on-line service providers or "OSPs."[26] Users typically are provided a password-protected mailbox from which they may send and retrieve e-mail.

There are two features of this system that distinguish it from direct and private-system e-mail. First, user mailboxes, although private, exist in a public forum consisting of other fee-paying users. The added risk caused by the existence of other public users on the same network is that misdirected e-mails may be sent to unknown users. Unlike users of private system e-mail networks who, as agents of their employers, owe a duty of confidentiality to them and, in the case of a law firm, to all firm clients, the inadvertent user owes no similar duties.[27] The risk of misdirection is, however, no different from that which exists when sending a fax. Further, the misdirection of an e-mail to another OSP can be avoided with reasonable care.[28]

The second distinctive feature of e-mail administered by an OSP is that the relative security and confidentiality of user e-mail largely depends on the adequacy of the particular OSP's security measures meant to limit external access and its formal policy regarding the confidentiality of user e-mail. Together, they will determine whether a user has a reasonable expectation of privacy in this type of e-mail.

The denial of external access ordinarily is ensured by the use of password-protected mailboxes or encryption[29]. The threat to confidentiality caused by the potential inspection of users' e-mail by OSP system administrators who must access the e-mail for administrative and compliance purposes is overcome by the adoption of a formal policy that narrowly restricts the bases on which system administrators[30] and OSP agents[31] [32] are permitted to examine user e-mail.

Moreover, federal law imposes limits on the ability of OSP administrators to inspect user e-mail, irrespective of the OSP's formal policy. Inspection is limited by the ECPA to purposes "necessary to the rendition of services" or to the protection of "rights or property."[33] Further, even if an OSP administrator lawfully inspects user e-mail within the narrow limits defined by the ECPA, the disclosure of those communications for purposes other than those provided by the statute is prohibited.[34]

Accordingly, the Committee concludes that lawyers have a reasonable expectation of privacy when communicating by e-mail maintained by an OSP, a conclusion that also has been reached by at least one case as well as state bar ethics committees and commentators.[35]

4. Internet E-Mail

E-mail may be sent over the Internet between service users without interposition of OSPs. Internet e-mail typically uses land-based phone lines and a number of intermediate computers randomly selected to travel from sender to recipient. The intermediate computers consist of various Internet service providers or "routers" that maintain software designed to help the message reach its final destination.

Because Internet e-mail typically travels through land-based phone lines, the only points of unique vulnerability consist of the third party-owned Internet services providers or "ISPs," each capable of copying messages passing through its network. Confidentiality may be compromised by (1) the ISP's legal, though qualified, right to monitor e-mail passing through or temporarily stored in its network, and (2) the illegal interception of e-mail by ISPs or "hackers."[36]

The ISPs' qualified inspection rights are identical to those of OSPs.[37] The same limits described above therefore apply to ISPs. In addition, the provider of an electronic communications service may by law conduct random monitoring only for mechanical or service quality control checks.[38]

The second threat to confidentiality is the illegal interception of e-mail, either by ISPs exceeding their qualified monitoring rights or making unauthorized disclosures, or by third party hackers who use ISPs as a means of intercepting e-mail. Although it is difficult to quantify precisely the frequency of either practice, the interception or disclosure of e-mail in transit or in storage (whether passing through an ISP or in any other medium) is a crime and also may result in civil liability.[39]

In addition to criminalization, practical constraints on the ability of third parties and ISPs to capture and read Internet e-mail lead to the conclusion that the user of Internet e-mail has a reasonable expectation of privacy. An enormous volume of data travelling at an extremely high rate passes through ISPs every hour. Further, during the passage of Internet e-mail between sender and recipient, the message ordinarily is split into fragments or "packets" of information. Therefore, only parts of individual messages customarily pass through ISPs, limiting the extent of any potential disclosure. Because the specific route taken by each e-mail message through the labyrinth of phone lines and ISPs is random, it would be very difficult consistently to intercept more than a segment of a message by the same author.

Together, these characteristics of Internet e-mail further support the Committee's conclusion that an expectation of privacy in this medium of communication is reasonable. The fact that ISP administrators or hackers are capable of intercepting Internet e-mail - albeit with great difficulty and in violation of federal law - should not render the expectation of privacy in this medium any the less reasonable, just as the risk of illegal telephone taps does not erode the reasonable expectation of privacy in a telephone call.[40]

CONCLUSION

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.

Even so, when the lawyer reasonably believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted, the lawyer should consult the client as to whether another mode of transmission, such as special messenger delivery, is warranted. The lawyer then must follow the client's instructions as to the mode of transmission. See Model Rule 1.2(a).

ENDNOTES

1 As used in this opinion, "confidential client information" denotes "information relating to the representation of a client" under Model Rule 1.6(a), which states:

(a) a lawyer shall not reveal information relating to representation of a client unless a client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation.

2 The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), amended the Federal Wiretap Statute of 1968 by extending its scope to include "electronic communications." 18 U.S.C.A. (2510, et seq. (1998) (the "ECPA"). The ECPA now commonly refers to the amended statute in its entirety. The ECPA provides criminal and civil penalties for the unauthorized interception or disclosure of any wire, oral, or electronic communication. 18 U.S.C.A. (2511.

3 Options other than abandoning e-mail include using encryption or seeking client consent after apprising the client of the risks and consequences of disclosure.

4 See also RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS (112 cmt. d (Proposed Official Draft 1998), which provides that confidential client information must be "acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality."

5 Whether a lawyer or a client has a reasonable expectation of privacy also governs whether a communication is "in confidence" for purposes of the attorney-client privilege. As a result, analysis under the attorney-client privilege is often relevant to this opinion's discussion of e-mail and the duty of confidentiality. The relevance of privilege is not exhaustive, however, because of its more restrictive application in prohibiting the introduction of privileged communications between a lawyer and client in any official proceeding. In contrast to the requirement imposed by the duty of confidentiality to avoid disclosing any information "relating to the representation" of the client, see Model Rule 1.6(a), supra n.1, the attorney-client privilege applies only to actual "communications" made "in confidence" by the client to the lawyer. See JOHN H. WIGMORE, 8 EVIDENCE § 2295 (McNaughton rev. 1961).

6 See infra Section B. It should be noted that a lawyer's negligent use of any medium - including the telephone, mail and fax - may breach the duty of confidentiality. The relevant issue here, however, is whether, despite otherwise reasonable efforts to ensure confidentiality, breach occurs solely by virtue of the lawyer's use of e-mail.

7 A.C.L.U. v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), aff'd 521 U.S. 844 (1997) ("Unlike postal mail, simple e-mail is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted.").

8 Frequently, what we understand to be regular or land-line telephone conversations are transmitted in part by microwave. For example, many corporate telephone networks are hard-wired within a building and transmitted by microwave among buildings within a corporate campus to a central switch connected by land-line or microwave to a local or interstate carrier.

9 It should be noted that the ECPA preserves the privileged character of any unlawfully intercepted "wire, oral, or electronic communication." 18 U.S.C.A. (2517(4). The inclusion of e-mail in this provision is important for two reasons. First, implicit in this provision is the assumption that electronic communications are capable of transmitting privileged material. To argue that the use of e-mail never is "in confidence" or constitutes an automatic waiver of otherwise privileged communications therefore appears to be inconsistent with an assumption of this provision of federal law. Second, the identical federal treatment of e-mail with other means of communication long assumed consistent with the maintenance of privilege likewise is inconsistent with the assertion that the use of e-mail poses unique threats to privileged communications.

10 See Peter R. Jarvis & Bradley F. Tellam, High-Tech Ethics and Malpractice Issues 7 (1996) (paper delivered at the 22nd National Conference on Professional Responsibility, May 30, 1996, in Chicago, Illinois) (on file with its author), reported in 1996 SYMPOSIUM ISSUE OF THE PROFESSIONAL LAWYER, 51, 55 (1996) (hereafter "Jarvis & Bradley"); David Hricik, E-mail and Client Confidentiality: Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail, 11 GEO. J. LEGAL ETHICS 459, 479 (1999) (hereafter "Hricik").

11 See Jarvis & Tellam supra n.10, at 57; Hricik supra n.10, at 480.

12 See Hricik supra n.10, at 481.

13 See, e.g., Jarvis & Tellam supra n.10, at 59-61; Hricik supra n.10, at 481-85. Compare Mass. Ethics Opinion 94-5 (1994) (if risk of disclosure to third party is "nontrivial," lawyer should not use cellular phone); N.C. Ethics Op. 215 (1995) (advising lawyers to use the mode of communication that best will maintain confidential information); State Bar of Arizona Advisory Op. 95-11 (1995) (lawyers should exercise caution before using cellular phones to communicate client confidences) with United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992) (finding that there may be reasonable expectation of privacy in cordless phone communications for Fourth Amendment purposes).

14 McKarney v. Roach, 55 F.3d 1236, 1238-9 (6th Cir. 1995), cert. denied, 576 U.S. 944 (1995); Askin v. United States, 47 F.3d 100, 103-04 (4th Cir. 1995).

15 By 1986, the protection under federal law for cellular phone communications was equal to traditional land-line telephone communications. The Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 202(a), 108 Stat. 4279 (1994), deleted previous exceptions under the Federal Wiretap Act that limited the legal protections afforded cordless phone communications under 18 U.S.C.A. ((2510(1), 2510(12) (A). Existing law criminalizes the intentional and unauthorized interception of both cordless and cellular phone communications, 18 U.S.C.A. (2511; the privileged status of the communication preserves in the event of intentional interception, 18 U.S.C.A. (2517(4); and bars the introduction of the unlawful interception as evidence at trial even if it is not privileged, 18 U.S.C.A. (2515.

16 State Bar of Arizona Advisory Op. 95-11 (1995). Some commentators have argued that in light of the 1994 amendment and the recent improvements in the security of both media (including the introduction of digital cellular phones), the expectation of privacy in communications by cordless and cellular telephones should not be considered unreasonable. Jarvis& Tellam supra n.10, at 60-61. See also Hricik supra n.10, at 483, 485 (arguing that despite the fact that their privileged status would not be lost if cellular and cordless phone conversations were intercepted, lawyers should consider whether the cost of potential disclosure is outweighed by the benefit derived from the use of cordless or cell phones). Further, 18 U.S.C.A. (2512 prohibits the manufacture and possession of scanners capable of receiving cellular frequencies, and cordless and cellular phone communications have been afforded greater legal protection under several recent state court decisions. See, e.g., State v. Faford, 128 Wash.2d 476, 485-86, 910 P.2d 447, 451-52 (1996) (reversing trial court's admission of defendants' cordless phone conversations violated state privacy act because defendants had reasonable expectation of privacy in such communication); State v. McVeigh, 224 Conn. 593, 622, 620 A.2d 133, 147 (1995) (reversing trial court's admission of defendants' cordless telephone conversations because such communications were within scope of state law forbidding the intentional interception of wire communications).

17 Hricik supra n.10, at 497.

18 See United States v. Maxwell 42 M.J. 568, 576, 43 Fed. R. Evid. Serv. (Callaghan) 24 (A. F. Ct. Crim. App. 1995) (holding that user of e-mail maintained by OSP was protected against warrantless search of e-mails because user had reasonable expectation of privacy in such communications, unlike cordless phone communication) aff'd in part and rev'd in part, 45 M.J. 406 (U.S. Armed Forces 1996) (expectation of privacy exists in e-mail transmissions made through OSP).

19 The risks of interception and disclosure may be lessened by the recent introduction of digital cellular phones, whose transmissions are considered more difficult to intercept than their analog counterparts. New communications technology, however, does not always advance privacy concerns. The use of airplane telephones, for example, exposes users to the interception risks of cellular telephones as well as a heightened risk of disclosure due to eavesdropping on the airplane itself. Most recently, a world-wide, satellite-based cellular telephone system called Iridium has been introduced by Motorola. The principles articulated in this opinion should be considered by a lawyer when using such systems.

20 See, e.g., Practice Guide, Electronic Communications, in ABA/BNA LAWYERS' MANUAL ON PROFESSIONAL CONDUCT 55:403 (1996) ("[C]ourts seem to have taken it for granted that fax machines may be used [to transmit confidential information]," citing State ex rel. U.S. Fidelity and Guar. Co. v. Canady, 144 W.Va. 431, 443-44, 460 S.E.2d 677, 689-90 (1995) (holding that faxed communication was protected by the attorney-client privilege)). See also Jarvis & Tellam supra n.10, at 61 ("[T]here seems to be no question that faxes are subject to the attorney-client privilege . . . no one asserts that the use of a fax machine or the possibility of misdirection destroys any hope of a claim of privilege," citing ABA Comm. on Ethics and Professional Responsibility, Formal Ops. 94-382 and 92-368).

21 The names for the varieties of e-mail described in this section of the opinion are based on those used by Hricik, supra n.10, at 485-92.

22 See, e.g., Alaska Bar Ass'n Op. 98-2 (1998); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997); Vermont Advisory Ethics Op. No. 97-5 (1997). See also, Jarvis & Tellam, supra n.10, at 61; Hricik supra n.10, at 502-06.

23 In re Grand Jury Proceedings, 43 F.3d 966, 968 (5th Cir. 1994) (court considered e-mail messages along with other documents in work-product privilege analysis); United States v. Keystone Sanitation Co. Inc., 903 F. Supp. 803, 808 (M.D. Pa. 1995) (defendants waived privileged nature of e-mail messages due to inadvertent production).

24 Hricik supra n. 10, at 487.

25 See e.g., Alaska Bar Ass'n Op. 98-2 (1998); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997); Vermont Advisory Ethics Op. 97-5 (1997). See also, Hricik supra n.10, at 486-87.

26 Examples include America Online ("AOL"), CompuServe, and MCI Mail.

27 Hricik supra n.10, at 487-88.

28 If the inadvertent recipient is a lawyer, then the lawyer must refrain from examining the information any more than necessary to ascertain that it was not intended for her and must notify the sender, ABA Comm. on Ethics and Professional Responsibility, Formal Op. 92-368 (1992), an obligation that extends to information received by e-mail or fax, ABA Comm. on Ethics and Professional Responsibility, Formal Op. 94-382 (1994).

29 For a basic explanation of encryption technology, including the use of digital signatures, see Kenneth E. Russell, Dealing with Security, Encryption, and Ethics Concerns, in THE LAWYER'S QUICK GUIDE TO E-MAIL 93-105 (ABA Law Practice Management Section 1998) ("Russell").

30 For a discussion of some additional matters such formal policies might address (deletion and retention of e-mail messages, remote checking of messages while out of office, etc.), see Russell, supra n. 29, at 104-05.

31 For example, the terms of AOL's policy forbid access to e-mail except (1) to comply with the law, (2) to protect its own rights, or (3) to act in the belief that someone's safety is at risk. Hricik supra n. 10, at 489.

32 18 U.S.C.A. (2511(2) (a) (i) (It is "not unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks"). The qualified right of interception of OSPs cannot be argued to create unique risks to the confidentiality of e-mail communications because phone companies (and other providers of wire or electronic communication services) are given identical rights under 18 U.S.C.A. (2511(2) (a) (i)). Moreover, many commercial mail services reserve the right to inspect all packages and letters handled, yet no one suggests this diminishes the user's expectation of privacy. See Hricik supra n.10, at 492. It also is noteworthy that in 1998, the New York Legislature amended the state's rules of evidence to provide that no otherwise privileged communication "shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication." N.Y. Civ. Prac. L. & R. § 4547 (1998).

33 18 U.S.C.A. (2511(3) (a).

34 See e.g., supra n.18. See also Alaska Bar Ass'n Op. 98-2 (1998); D.C. Bar Op. 281 (1998); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997) (users of e-mail maintained by OSP have reasonable expectation of privacy despite greater risks than private network e-mail); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997); Vermont Advisory Ethics Op. 97-5 (1997); Jarvis & Tellam supra n.10, at 61; Hricik supra n.10, at 492.

35 Confidentiality also may be compromised by computer viruses, some of which have the capability of causing the user's document to be propagated to unintended recipients. However, a virus scanning program containing up-to-date definition files will detect and clean such viruses. See generally Carnegie Mellon Software Engineering Institute's CERT(r) Coordination Center Website, http://www.cert.org/index.html, for descriptions of these and other computer viruses.

36 See supra notes 30 & 31 and accompanying text.

37 18 U.S.C.A. (2511(2) (a) (i).

38 See 18 U.S.C.A. ((2511, 2701, 2702.

39 See Katz v. U.S., 389 U.S. 347, 352 (1967) (Fourth Amendment protection extended to conversation overheard by listening device attached to outside of public telephone booth).

40 See, e.g., Alaska Bar Ass'n Op. 98-2 (1998) (lawyers may communicate with clients via unencrypted e-mail; client consent is unnecessary because the expectation of privacy in e-mail is no less reasonable than that in the telephone or fax); D.C. Bar Op. 281 (1998) (lawyers' use of unencrypted e-mail is not a violation of duty to protect client confidences under District of Columbia Rule of Professional Conduct 1.6); Ky. Bar Ass'n Ethics Comm. Advisory Op. E-403 (1998) (absent "unusual circumstances" lawyers may use e-mail, including unencrypted Internet e-mail, to communicate with clients); New York State Bar Ass'n Comm. on Professional Ethics Op. 709 (1998) (lawyers may use unencrypted Internet e-mail to transmit confidential information without breaching the duty of confidentiality under state analogue to ABA Model Rule 1.6); Ill. State Bar Ass'n Advisory Op. on Professional Conduct No. 96-10 (1997) (lawyers may use unencrypted e-mail, including e-mail sent over the Internet, to communicate with clients without violating Rule 1.6 of the Illinois Rules of Professional Conduct; client consent is not required absent "extraordinarily sensitive" matter; expectation of privacy in e-mail is no less reasonable than that in ordinary telephone calls); N.D. St. B. Ass'n Ethics Comm. Op. 97-09 (1997) (attorneys may communicate with clients using unencrypted e-mail unless unusual circumstances warrant heightened security measures); S.C. Bar Ethics Advisory Comm. Op. No. 97-08 (1997) (finding reasonable expectation of privacy when sending confidential information by e-mail, including that sent through a private network, commercial service, and the Internet; use of e-mail to communicate client confidences does not violate South Carolina Rule of Professional Conduct 1.6); Vermont Advisory Ethics Op. 97-5 (1997) (lawyers may use unencrypted Internet e-mail to transmit confidential information without breaching the duty of confidentiality under state analogue to ABA Model Rule 1.6). Two opinions similarly endorsed e-mail as a means of communicating client confidences, but advised lawyers to seek client consent or consider the use of encryption prior to its use, unlike the present opinion: Pa. Bar Ass'n Comm. on Legal Ethics Op. 97-130 (1997) (lawyers should not use unencrypted e-mail to communicate with or about a client absent client consent); State Bar of Arizona Advisory Op. 97-04 (1996) (lawyers should caution client or consider the use of encryption before transmitting sensitive information by e-mail). Two other opinions advised lawyers to avoid the use of e-mail to communicate with or about clients: Iowa Bar Ass'n Op. 1997-1 (1997) (sensitive material should not be transmitted by e-mail - whether through the Internet, a non-secure intranet, or other types of proprietary networks - without client consent, encryption, or equivalent security system); N.C. State Bar Opinion 215 (1995) (advising lawyers to use the mode of communication that will best maintain confidential information, and cautioning attorneys against the use of e-mail). Commentary supportive of the conclusions reached in this opinion, in addition to Hricik supra n.10 and Jarvis & Tellam supra n.10, include William Freivogel, Communicating With or About Clients on the Internet: Legal, Ethical, and Liability Concerns, ALAS LOSS PREVENTION JOURNAL 17 (1996) (concluding that it is not ethically or legally necessary to encrypt Internet e-mail but cautioning them in light of the absence of controlling legal authority). For a list of Web pages containing articles on e-mail and confidentiality, see Russell, supra n. 29, at 103.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

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[1]

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.[2] 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.[3] 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.[4]

In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] 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).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information").

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,[6] 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 Lawyers); 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."[8] 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.)[9]

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]

[8] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2018).
[9] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).
[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

[11] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

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[12] 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,[13] whether further action is warranted,[14] 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,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] 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.[17]

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

[12] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).
[13] Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), *available at* https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx (noting that "[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment.").
[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.
[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

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.").
[19] *NIST Computer Security Incident Handling Guide*, at 6 (2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

> 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.[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."[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

[20] Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).
[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).[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.[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."[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

[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.").
[23] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).
[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).[25]

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.[26] 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.[27] 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.[28]

[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.[29] 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.[30] 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.[31]

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

[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.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.") (*citations omitted*).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

[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."[35] 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.[36]

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.[37] 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.[38] 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

[35] MODEL RULES OF PROF'L CONDUCT R. 1.9(c)(2) (2018).
[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.").
[37] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9, cmt. [9] (2018).
[38] *See* ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

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.[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.[40] 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 beach, 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.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] 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.[45]

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

[40] State Bar of Mich. Op. RI-09 (1991).
[41] National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[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."

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477R* **May 11, 2017**

Revised May 22, 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 email 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

*The opinion below is a revision of, and replaces Formal Opinion 477 as issued by the Committee May 11, 2017. This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2016. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).

2. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

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."[4] 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.[5]

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."[6] The scope of this requirement was

3. *See* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

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.

6. A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

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.)[7]

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] [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.[8]

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.[9] 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."[10]

7. *Id.* at 43.

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).

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.

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.[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:

> . . . 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.[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,

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 or 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."

12. ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

- 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).[13]

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.[14] 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.

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2016). "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 8, at 5.

14. See item 3 below.

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.[15] "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

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

15. *See, e.g.*, Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/.

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,[16] 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.

16. *See* Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

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.[17] If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.[18]

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.

17. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459, Duty to Protect the Confidentiality of E-mail Communications with One's Client (2011). Formal Op. 11-459 was issued prior to the 2012 amendments to Rule 1.6. These amendments added new Rule 1.6(c), which provides that lawyers "shall" make reasonable efforts to prevent the unauthorized or inadvertent access to client information. *See, e.g.*, Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer's email server).

18. Some state bar ethics opinions have explored the circumstances under which email 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;
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

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).

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 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.[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.

---

20. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

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] (2016). 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.authcheckdam.pdf.

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 [19] 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."

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.

23. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) & (4) (2016).

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 479 **December 15, 2017**

The "Generally Known" Exception to Former-Client Confidentiality

A lawyer's duty of confidentiality extends to former clients. Under Model Rule of Professional Conduct 1.9(c), a lawyer may not use information relating to the representation of a former client to the former client's disadvantage without informed consent, or except as otherwise permitted or required by the Rules of Professional Conduct, unless the information has become "generally known."

The "generally known" exception to the duty of former-client confidentiality is limited. It applies (1) only to the use, and not the disclosure or revelation, of former-client information; and (2) only if the information has become (a) widely recognized by members of the public in the relevant geographic area; or (b) widely recognized in the former client's industry, profession, or trade. Information is not "generally known" simply because it has been discussed in open court, or is available in court records, in libraries, or in other public repositories of information.

Introduction

Confidentiality is essential to the attorney-client relationship. The duty to protect the confidentiality of client information has been enforced in rules governing lawyers since the Canons of Ethics were adopted in 1908.

The focus of this opinion is a lawyer's duty of confidentiality to former clients under Model Rule of Professional Conduct 1.9(c). More particularly, this opinion explains when information relating to the representation of a former client has become generally known, such that the lawyer may use it to the disadvantage of the former client without violating Model Rule 1.9(c)(1).

The Relevant Model Rules of Professional Conduct

Model Rule 1.6(a) prohibits a lawyer from revealing information related to a client's representation unless the client gives informed consent, the disclosure is impliedly authorized to carry out the representation, or the disclosure is permitted by Model Rule 1.6(b).[1] Model Rule 1.9 extends lawyers' duty of confidentiality to former clients. Model Rules 1.9(a) and (b) govern situations in which a lawyer's knowledge of a former client's confidential information would create a conflict of interest in a subsequent representation. Model Rule 1.9(c) "separately regulates the use and disclosure of confidential information" regardless of "whether or not a subsequent

[1] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2017) [hereinafter MODEL RULES].

representation is involved."[2]

Model Rule 1.9(c)(2) governs the *revelation* of former client confidential information. Under Model Rule 1.9(c)(2), a lawyer who formerly represented a client in a matter, or whose present or former firm formerly represented a client in a matter, may not reveal information relating to the representation except as the Model Rules "would permit or require with respect to a [current] client." Lawyers thus have the same duties not to *reveal* former client confidences under Model Rule 1.9(c)(2) as they have with regard to current clients under Model Rule 1.6.

In contrast, Model Rule 1.9(c)(1) addresses the *use* of former client confidential information. Model Rule 1.9(c)(1) provides that a lawyer shall not use information relating to a former client's representation "to the disadvantage of the former client except as [the Model] Rules would permit or require with respect to a [current] client, or when the information has become *generally known*."[3] The terms "reveal" or "disclose" on the one hand and "use" on the other describe different activities or types of conduct even though they may—but need not—occur at the same time. The generally known exception applies only to the "use" of former client confidential information. This opinion provides guidance on when information is generally known within the meaning of Model Rule 1.9(c)(1).[4]

The Generally Known Exception

The generally known exception to the use of former-client information was introduced in the 1983 Model Rules.[5] The term is not defined in Model Rule 1.0 or in official Comments to Model Rule 1.9. A number of courts and other authorities conclude that information is *not* generally known merely because it is publicly available or might qualify as a public record or as a matter of public record.[6] Agreement on when information *is* generally known has been harder to achieve.

[2] ELLEN J. BENNETT ET AL., ANNOTATED MODEL RULES OF PROFESSIONAL CONDUCT 190 (8th ed. 2015).

[3] MODEL RULES R. 1.9(c)(1) (2017) (emphasis added).

[4] *See id.* at cmt. 9 (explaining that "[t]he provisions of this Rule are for the protection of former clients and can be waived if the client gives informed consent").

[5] *See* RONALD D. ROTUNDA & JOHN S. DZIENKOWSKI, LEGAL ETHICS: THE LAWYER'S DESKBOOK ON PROFESSIONAL RESPONSIBILITY § 1.9, at 534 (2017–2018) (explaining that the language was originally part of Model Rule 1.9(b), and was moved to Model Rule 1.9(c) in 1989).

[6] *See, e.g.*, Pallon v. Roggio, Civ. A. Nos. 04-3625(JAP), 06-1068(FLW), 2006 WL 2466854, at *7 (D. N.J. Aug. 24, 2006) ("'Generally known' does not only mean that the information is of public record. . . . The information must be within the basic understanding and knowledge of the public. The content of form pleadings, interrogatories and other discovery materials, as well as general litigation techniques that were widely available to the public through the internet or another source, such as continuing legal education classes, does not make that information 'generally known' within the meaning of Rule 1.9(c)." (citations omitted)); Steel v. Gen. Motors Corp., 912 F. Supp. 724, 739 (D. N.J. 1995) (in a discussion of Rule 1.9(c)(2), stating that the fact that information is publicly available does not make it 'generally known'); *In re* Gordon Props., LLC, 505 B.R. 703, 707 n.6 (Bankr. E.D. Va. 2013) ("'Generally known' does not mean information that someone can find."); *In re* Anonymous, 932 N.E.2d 671, 674 (Ind. 2010) (stating in connection with a discussion of Rule 1.9(c)(2) that "the Rules contain no exception allowing revelation of information relating to a representation even if a diligent researcher could unearth it through public sources" (footnote omitted); *In re* Tennant, 392 P.3d 143, 148 (Mont. 2017) (explaining that with respect to the Rule 1.9(c) analysis of

A leading dictionary suggests that information is generally known when it is "popularly" or "widely" known.[7] Commentators have essentially endorsed this understanding of generally known by analogizing to an original comment in New York's version of Rule 1.6(a) governing the protection of a client's confidential information. The original comment distinguished "generally known" from "publicly available."[8] Commentators find this construct "a good and valid guide"[9] to when information is generally known for Rule 1.9(c)(1) purposes:

> [T]he phrase "generally known" means much more than publicly available or accessible. It means that the information has already received widespread publicity. For example, a lawyer working on a merger with a Fortune 500 company could not whisper a word about it during the pre-offer stages, but once the offer is made—for example, once AOL and Time Warner have announced their merger, and the Wall Street Journal has reported it on the front page, and the client has become a former client—then the lawyer may tell the world. After all, most of the world already knows. . . .
>
> [O]nly if an event gained considerable public notoriety should information about it ordinarily be considered "generally known."[10]

Similarly, in discussing confidentiality issues under Rules 1.6 and 1.9, the New York State Bar Association's Committee on Professional Ethics ("NYSBA Committee") opined that "information is generally known only if it is known to a sizeable percentage of people in 'the local community or in the trade, field or profession to which the information relates.'"[11] By contrast, "[I]nformation is not 'generally known' simply because it is in the public domain or available in a public file."[12] The Illinois State Bar Association likewise reasoned that information is generally known within the meaning of Rule 1.9 if it constitutes "'common knowledge in the community.'"[13]

As the NYSBA Committee concluded, information should be treated differently if it is widely recognized in a client's industry, trade, or profession even if it is not known to the public at large. For example, under Massachusetts Rule of Professional Conduct 1.6(a), a lawyer generally is obligated to protect "confidential information relating to the representation of a client."[14] Confidential information, however, does not ordinarily include "information that is generally known in the local community or in the trade, field or profession to which the information relates."[15] Similarly, under New York Rule of Professional Conduct 1.6(a), a lawyer generally cannot "knowingly reveal confidential information . . . or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person,"[16] but "confidential information" does not include "information that is generally known in the local community or in the trade, field or profession to which the information relates."[17] Returning to Model Rule 1.9(c)(1), allowing information that is generally known in the former client's industry, profession, or trade to be used pursuant to Model Rule 1.9(c)(1) makes sense if, as some scholars have urged, the drafters of the rule contemplated that situation.[18]

when information is considered to be generally known, the fact that "the information at issue is generally available does not suffice; the information must be within the basic knowledge and understanding of the public;" protection of the client's information "'is not nullified by the fact that the circumstances to be disclosed are part of a public record, or that there are other available sources for such information, or by the fact that the lawyer received the same information from other sources'") (citations omitted)); Turner v. Commonwealth, 726 S.E.2d 325, 333 (Va. 2012) (Lemons, J., concurring) ("While testimony in a court proceeding may become a matter of public record even in a court denominated as a 'court not of record,' and may have been within the knowledge of anyone at the preliminary hearing, it does not mean that such testimony is 'generally known.' There is a significant difference between something being a public record and it also being 'generally known.'"); N.Y. State Bar Ass'n Comm. on Prof'l Ethics Op. 1125, 2017 WL 2639716, at *1 (2017) (discussing lawyers' duty of confidentiality and stating that "information is not 'generally known' simply because it is in the public domain or available in a public file" (reference omitted)); Tex. Comm. on Prof'l Ethics Op. 595, 2010 WL 2480777, at *1 (2010) ("Information that is a matter of public record may not be information that is 'generally known.' A matter may be of public record simply by being included in a government record . . . whether or not there is any general public awareness of the matter. Information that 'has become generally known' is information that is actually known to some members of the general public and is not merely available to be known if members of the general public choose to look where the information is to be found."); ROTUNDA & DZIENKOWSKI, *supra* note 5, § 1.9-3, at 554 (stating that Model Rule 1.9 "deals with what has become generally known, not what is publicly available if you know exactly where to look"); *see also* Dougherty v. Pepper Hamilton LLP, 133 A.3d 792, 800 (Pa. Super. Ct. 2016) (questioning whether an FBI affidavit that was accidentally attached to a document in an unrelated proceeding and was thus publicly available through PACER was "actually 'generally known,'" since "a person interested in the FBI affidavit 'could obtain it only by means of special knowledge'" (citing Restatement (Third) of the Law Governing Lawyers § 59, cmt. d). *But see* State v. Mark, 231 P.3d 478, 511 (Haw. 2010) (treating a former client's criminal conviction as "generally known" when discussing a former client conflict and whether matters were related); Jamaica Pub. Serv. Co. v. AIU Ins. Co., 707 N.E.2d 414, 417 (N.Y. 1998) (applying former DR 5-108(a)(2) and stating that because information regarding the defendant's relationship with its sister companies "was readily available in such public materials as trade periodicals and filings with State and Federal regulators," it was "generally known"); State ex rel. Youngblood v. Sanders, 575 S.E.2d 864, 872 (W. Va. 2002) (stating that because information was contained in police reports it was "generally known" for Rule 1.9 purposes); RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 59 cmt. d (2000) ("Information contained in books or records in public libraries, public-record depositories such as government offices, or publicly accessible electronic-data storage is generally known if the particular information is obtainable through publicly available indexes and similar methods of access.").

[7] THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 732 (4th ed. 2009).

[8] *See* ROY D. SIMON & NICOLE HYLAND, SIMON'S NEW YORK RULES OF PROFESSIONAL CONDUCT ANNOTATED 685 (2017) (discussing former comment 4A to New York Rule 1.6).

[9] *Id.*

[10] *Id.*

[11] N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 991, at ¶ 20 (2013).

[12] *Id.* at ¶ 17.

[13] Ill. State Bar Ass'n. Advisory Op. 05-01, 2006 WL 4584283, at *3 (2006) (quoting RESTATEMENT (SECOND) OF AGENCY § 395 cmt. b (1958)). The Illinois State Bar borrowed this definition from section 395 of the Restatement (Second) of Agency, which excludes such information from confidential information belonging to a principal that an agent may not use "in violation of his duties as agent, in competition with or to the injury of the principal," whether "on his own account or on behalf of another." RESTATEMENT (SECOND) OF AGENCY § 395 & cmt. b (1958).

[14] MASS. RULES OF PROF'L CONDUCT R. 1.6(a) (2017).

[15] *Id.* at cmt. 3A.

[16] N.Y. RULES OF PROF'L CONDUCT R. 1.6(a) (2017).

[17] *Id.* at cmt. [4A] ("Information is generally known in the local community or in the trade, field or profession to which the information relates is also not protected, unless the client and the lawyer have otherwise agreed. Information is not 'generally known' simply because it is in the public domain or available in a public file").

[18] *See* GEOFFREY C. HAZARD, JR. ET AL., THE LAW OF LAWYERING § 14.16, at 14-48 (2016) (discussing generally known and saying, "It seems likely that both the Kutak Commission and the Ethics 2000 Commission . . .

A Workable Definition of Generally Known under Model Rule 1.9(c)(1)

Consistent with the foregoing, the Committee's view is that information is generally known within the meaning of Model Rule 1.9(c)(1) if (a) it is widely recognized by members of the public in the relevant geographic area; or (b) it is widely recognized in the former client's industry, profession, or trade. Information may become widely recognized and thus generally known as a result of publicity through traditional media sources, such as newspapers, magazines, radio, or television; through publication on internet web sites; or through social media. With respect to category (b), information should be treated as generally known if it is announced, discussed, or identified in what reasonable members of the industry, profession, or trade would consider a leading print or online publication or other resource in the particular field. Information may be widely recognized within a former client's industry, profession, or trade without being widely recognized by the public. For example, if a former client is in the insurance industry, information about the former client that is widely recognized by others in the insurance industry should be considered generally known within the meaning of Model Rule 1.9(c)(1) even if the public at large is unaware of the information.

Unless information has become widely recognized by the public (for example by having achieved public notoriety), or within the former client's industry, profession, or trade, the fact that the information may have been discussed in open court, or may be available in court records, in public libraries, or in other public repositories does not, standing alone, mean that the information is generally known for Model Rule 1.9(c)(1) purposes.[19] Information that is publicly available is not necessarily generally known. Certainly, if information is publicly available but requires specialized knowledge or expertise to locate, it is not generally known within the meaning of Model Rule 1.9(c)(1).[20]

had in mind situations in which a lawyer has worked with a company in various legal contexts, learned considerable information about its products and practices, and later seeks to use this information in connection with [the] representation of an adverse party in an unrelated lawsuit or transaction of some kind").

[19] *See In re* Gordon Props., LLC, 505 B.R. 703, 707 n.6 (Bankr. E.D. Va. 2013) ("'Generally known' does not mean information that someone can find. It means information that is already generally known. For example, a lawyer may have drafted a property settlement agreement in a divorce case and it may [be] in a case file in the courthouse where anyone could go, find it and read it. It is not 'generally known.' In some divorce cases, the property settlement agreement may become generally known, for example, in a case involving a celebrity, because the terms appear on the front page of the tabloids. 'Generally known' does not require publication on the front page of a tabloid, but it is more than merely sitting in a file in the courthouse."); *In re* Tennant, 392 P.3d 143, 148 (Mont. 2017) (holding that a lawyer who learned the information in question during his former clients' representation could not take advantage of his former clients "by retroactively relying on public records of their information for self-dealing"); ROTUNDA & DZIENKOWSKI, *supra* note 5, § 1.9-3, at 554 (explaining that Model Rule 1.9(c)(1) "deals with what has become generally known, not what is publicly available if you know exactly where to look"); *see also supra* note 6 (citing additional cases and materials).

[20] *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 59 cmt. d (2000) (stating, *inter alia*, that information is not generally known "when a person interested in knowing the information could obtain it only by means of special knowledge").

Conclusion

A lawyer may use information that is generally known to a former client's disadvantage without the former client's informed consent. Information is generally known within the meaning of Model Rule 1.9(c)(1) if it is widely recognized by members of the public in the relevant geographic area or it is widely recognized in the former client's industry, profession, or trade. For information to be generally known it must previously have been revealed by some source other than the lawyer or the lawyer's agents. Information that is publicly available is not necessarily generally known.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 480 **March 6, 2018**

Confidentiality Obligations for Lawyer Blogging and Other Public Commentary

Lawyers who blog or engage in other public commentary may not reveal information relating to a representation, including information contained in a public record, unless authorized by a provision of the Model Rules.[1]

Introduction

Lawyers comment on legal topics in various formats. The newest format is online publications such as blogs,[2] listserves, online articles, website postings, and brief online statements or microblogs (such as Twitter®) that "followers" (people who subscribe to a writer's online musings) read. Lawyers continue to present education programs and discuss legal topics in articles and chapters in traditional print media such as magazines, treatises, law firm white papers, and law reviews. They also make public remarks in online informational videos such as webinars and podcasts (collectively "public commentary").[3]

Lawyers who communicate about legal topics in public commentary must comply with the Model Rules of Professional Conduct, including the Rules regarding confidentiality of information relating to the representation of a client. A lawyer must maintain the confidentiality of information relating to the representation of a client, unless that client has given informed consent to the disclosure, the disclosure is impliedly authorized to carry out the representation, or the disclosure is permitted by Rule 1.6(b). A lawyer's public commentary may also implicate the lawyer's duties under other Rules, including Model Rules 3.5 (Impartiality and Decorum of the Tribunal) and 3.6 (Trial Publicity).

Online public commentary provides a way to share knowledge, opinions, experiences, and news. Many online forms of public commentary offer an interactive comment section, and, as such, are also a form of social media.[4] While technological advances have altered how lawyers communicate, and therefore may raise unexpected practical questions, they do not alter lawyers' fundamental ethical obligations when engaging in public commentary.[5]

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2016 [hereinafter the "Model Rules"]. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

[2] A "blog" is commonly understood to be a website consisting of written entries (posts) regularly updated and typically written in an informal or conversational style by an individual or small group. As recently described in a California State Bar advisory opinion, "[b]logs written by lawyers run the gamut from those having nothing to do with the legal profession, to informational articles, to commentary on legal issues and the state of our system of justice, to self-promotional descriptions of the attorney's legal practice and courtroom successes to overt advertisements for the attorney or her law firm." State Bar of Cal. Comm'n on Prof'l Responsibility & Conduct Op. 2016-196 (2016).

[3] These are just examples of public written communications but this opinion is not limited to these formats. This opinion does not address the various obligations that may arise under Model Rules 7.1-7.5 governing advertising and solicitation, but lawyers may wish to consider their potential application to specific communications.

[4] Lawyers should take care to avoid inadvertently forming attorney-client relationships with readers of their public commentary. Although traditional print format commentary would not give rise to such concerns, lawyers interacting with readers through social media should be aware at least of its possibility. A lawyer commenting publicly about a legal matter standing alone would not create a client-lawyer relationship with readers of the commentary. *See* Model Rule 1.18 for duties to prospective clients. However, the ability of readers/viewers to make comments or to ask questions suggests that, where practicable, a lawyer include appropriate disclaimers on websites, blogs and the like, such as "reading/viewing this information does not create an attorney-client relationship."

Lawyer blogging may also create a positional conflict. *See* D.C. Bar Op. 370 (2016) (discussing lawyers' use of social media advising that "[c]aution should be exercised when stating positions on issues, as those stated positions could be adverse to an interest of a client, thus inadvertently creating a conflict.") *See also* ELLEN J. BENNETT, ELIZABETH J. COHEN & HELEN W. GUNNARSSON, ANNOTATED MODEL RULES OF PROFESSIONAL CONDUCT 148 (8th ed. 2015) (addressing positional conflicts). *See also* STEPHEN GILLERS, REGULATION OF LAWYERS: PROBLEMS OF LAW AND ETHICS 50-51 (11th ed. 2018) ("[S]ocial media presence can pose a risk for attorneys, who must be careful not to contradict their firm's official position on an issue in a pending case"). This opinion does not address positional conflicts.

[5] *Accord* D.C. Bar Op. 370 (2016) (stating that a lawyer who chooses to use social media must comply with ethics rules to the same extent as one communicating through more traditional forms of communication).

[6] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [3] (2017). There is also a general principle noted in the Restatement (Third) of the Law Governing Lawyers that "[c]onfidential client information does not include what a lawyer learns about the law, legal institutions such as courts and administrative agencies, and similar public matters in the course of representing clients." AMERICAN LAW INSTITUTE, RESTATEMENT OF THE LAW (THIRD) THE LAW GOVERNING LAWYERS §59, cmt. e (1998). It is beyond the scope of this opinion to define what specific elements will be considered to distinguish between protected client information and information about the law when they entwine.

[7] *See* Wis. Op. EF-17-02 (2017) ("a client's identity, as well as a former client's identity, is information protected by [Rule 1.6]"); State Bar of Nev. Comm'n on Ethics and Prof'l Responsibility Formal Op. 41, at 2 (2009) ("Even the mere identity of a client is protected by Rule 1.6."); State Bar of Ariz. Comm. on the Rules of Prof'l Conduct Op. 92-04 (1992) (explaining that a firm may not disclose list of client names with receivable amounts to a bank to obtain financing without client consent). *See also* MODEL RULES OF PROF'L CONDUCT R. 7.2 cmt. [2] (2017) & N.Y. Rules of Prof'l Conduct R. 7.1(b)(2) (requiring prior written consent to use a client name in advertising). *But see* Cal. Formal Op. 2011-182 (2011) ("…[I]n most situations, the identity of a client is not considered confidential and in such circumstances Attorney may disclose the fact of the representation to Prospective Client without Witness Client's consent.") (*citing to* LA County Bar Ass'n Prof'l Responsibility & Ethics Comm'n Op. 456 (1989)).

[8] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(1)-(7) (2017).

Duty of Confidentiality Under Rule 1.6

Model Rule 1.6(a) provides:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

As Comment [2] emphasizes, "[a] fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation."

This confidentiality rule "applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source."[6] In other words, the scope of protection afforded by Rule 1.6 is far broader than attorney-client privileged information.

Unless one of the exceptions to Rule 1.6(a) is applicable, a lawyer is prohibited from commenting publicly about any information related to a representation. Even client identity is protected under Model Rule 1.6.[7] Rule 1.6(b) provides other exceptions to Rule 1.6(a).[8] However, because it is highly unlikely that a disclosure exception under Rule 1.6(b) would apply to a

lawyer's public commentary, we assume for this opinion that exceptions arising under Rule 1.6(b) are not applicable.[9]

Significantly, information about a client's representation contained in a court's order, for example, although contained in a public document or record, is *not* exempt from the lawyer's duty of confidentiality under Model Rule 1.6.[10] The duty of confidentiality extends generally to information related to a representation whatever its source and without regard to the fact that others may be aware of or have access to such knowledge.[11]

A violation of Rule 1.6(a) is not avoided by describing public commentary as a "hypothetical" if there is a reasonable likelihood that a third party may ascertain the identity or situation of the client from the facts set forth in the hypothetical.[12] Hence, if a lawyer uses a hypothetical when offering public commentary, the hypothetical should be constructed so that there is no such likelihood.

The salient point is that when a lawyer participates in public commentary that includes client information, if the lawyer has not secured the client's informed consent or the disclosure is

[9] For ethical issues raised when a lawyer is participating in an investigation or litigation and the lawyer makes extrajudicial statements, see *infra* at page 6.

[10] *See* ABA Formal Op. 479 (2017). *See also In re* Anonymous, 932 N.E.2d 671 (Ind. 2010) (neither client's prior disclosure of information relating to her divorce representation to friends nor availability of information in police reports and other public records absolved lawyer of violation of Rule 1.6); Iowa S. Ct. Attorney Disciplinary Bd. v. Marzen, 779 N.W.2d 757 (Iowa 2010) (all lawyer-client communications, even those including publicly available information, are confidential); Lawyer Disciplinary Bd. v. McGraw, 461 S.E.2d 850 (W. Va. 1995) ("[t]he ethical duty of confidentiality is not nullified by the fact that the information is part of a public record or by the fact that someone else is privy to it"); State Bar of Ariz. Op. 2000-11 (2000) (lawyer must "maintain the confidentiality of information relating to representation even if the information is a matter of public record"); State Bar of Nev. Op. 41 (2009) (contrasting broad language of Rule 1.6 with narrower language of Restatement (Third) of the Law Governing Lawyers); Pa. Bar Ass'n Informal Op. 2009-10 (2009) (absent client consent, lawyer may not report opponent's misconduct to disciplinary board even though it is recited in court's opinion); Colo. Formal Op. 130 (2017) ("Nor is there an exception for information otherwise publicly available. For example, without informed consent, a lawyer may not disclose information relating to the representation of a client even if the information has been in the news."); *But see In re* Sellers, 669 So. 2d 1204 (La. 1996) (lawyer violated Rule 4.1 by failing to disclose existence of collateral mortgage to third party; because "mortgage was filed in the public record, disclosure of its existence could not be a confidential communication, and was not prohibited by Rule 1.6"); Hunter v. Va. State Bar, 744 S.E.2d 611 (Va. 2013) (rejecting state bar's interpretation of Rule 1.6 as prohibiting lawyer from posting on his blog information previously revealed in completed public criminal trials of former clients). See discussion of *Hunter*, *infra*, at note 20.

[11] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 04-433 (2004) ("Indeed, the protection afforded by Rule 1.6 is not forfeited even when the information is available from other sources or publicly filed, such as in a malpractice action against the offending lawyer.")

[12] MODEL RULES OF PROF'L RESPONSIBILITY R. 1.6 cmt. [4] (2017). The possibility of violating Rule 1.6 using hypothetical facts was discussed in ABA Formal Opinion 98-411, which addressed a lawyer's ability to consult with another lawyer about a client's matter. That opinion was issued prior to the adoption of what is now Rule 1.6(b)(4) which permits lawyers to reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to secure legal advice about the lawyer's compliance with these Rules. However, the directive provided in Formal Opinion 98-411 remains sound, namely, that a lawyer use caution when constructing a hypothetical. For an illustrative case, see *In re* Peshek, M.R. 23794, 2009 PR 00089 (Ill. 2010). Peshek was suspended for sixty days for violating Rule 1.6. Peshek served as a Winnebago County Public defender for about 19 years. After being assaulted by a client, Peshek began publishing an Internet blog, about a third of which was devoted to discussing her work at the public defender's office and her clients. Peshek's blog contained numerous entries about conversations with clients and various details of their cases, and Peshek referred to her clients by either first name, a derivative of their first name, or their jail ID number, which were held to be disclosures of confidential information in violation of Rule 1.6. She was suspended from practice for 60 days.

not otherwise impliedly authorized to carry out the representation, then the lawyer violates Rule 1.6(a).[13] Rule 1.6 does not provide an exception for information that is "generally known" or contained in a "public record."[14] Accordingly, if a lawyer wants to publicly reveal client information, the lawyer[15] must comply with Rule 1.6(a).[16]

First Amendment Considerations

While it is beyond the scope of the Committee's jurisdiction to opine on legal issues in formal opinions, often the application of the ethics rules interacts with a legal issue. Here lawyer speech relates to First Amendment speech. Although the First Amendment to the United States Constitution guarantees individuals' right to free speech, this right is not without bounds.[17] Lawyers' professional conduct may be constitutionally constrained by various professional regulatory standards as embodied in the Model Rules, or similar state analogs. For example, when a lawyer acts in a representative capacity, courts often conclude that the lawyer's free speech rights are limited.[18]

[13] We again note that Rule 1.6(b) provides other exceptions to Rule 1.6(a).

[14] Model Rule 1.9 addresses the duties lawyers owe to former clients. Rule 1.9(c)(1) permits a lawyer, who has formerly represented a client, to use information related to the representation that has become generally known to the disadvantage of a former client, and Rule 1.9(c)(2) prohibits a lawyer from revealing information relating to the representation except as the Rules permit or require with respect to a current client. This opinion does not address these issues under Model Rule 1.9. The generally known exception in Rule 1.9(c)(1) is addressed in ABA Formal Opinion 479.

[15] Lawyers also have ethical obligations pursuant to Rules 5.1 and 5.3 to assure that lawyers and staff they supervise comply with these confidentiality obligations.

[16] In addition to the requirements of Rules 1.6(a), a lawyer may consider other practical client relations and ethics issues before discussing client information in public commentary to avoid disseminating information that the client may not want disseminated. For instance, Model Rule 1.8(b) reads: "A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these Rules." Rule 1.8(b) could be read to suggest that a lawyer may use client information if it *does not* disadvantage a client. The lawyer, nevertheless, has a common-law fiduciary duty not to profit from using client information even if the use complies with the lawyer's ethical obligations. *See* RESTATEMENT OF THE LAW (THIRD) THE LAW GOVERNING LAWYERS § 60(2) (1998) ("a lawyer who uses confidential information of a client for the lawyer's pecuniary gain other than in the practice of law must account to the client for any profits made"). *Accord* D.C. Bar Op. 370 (2016) ("It is advisable that the attorney share a draft of the proposed post or blog entry with the client, so there can be no miscommunication regarding the nature of the content that the attorney wishes to make public. It is also advisable, should the client agree that the content may be made public, that the attorney obtain that client's consent in a written form.")

[17] *See* Gregory A. Garbacz, *Gentile v. State Bar of Nevada: Implications for the Media*, 49 WASH. & LEE L. REV. 671 (1992); D. Christopher Albright, *Gentile v. State Bar: Core Speech and a Lawyer's Pretrial Statements to the Press*, 1992 BYU L. REV. 809 (1992); Kathleen M. Sullivan, *The Intersection of Free Speech and the Legal Profession: Constraints on Lawyers' First Amendment Rights*, 67 FORDHAM L. REV. 569 (1998). *See also* Brandon v. Maricopa City, 849 F.3d 837 (9th Cir. 2017) (when a lawyer speaks to the media in her official capacity as an attorney for county officials, such speech involves her conduct as a lawyer and therefore is not "constitutionally protected citizen speech").

[18] *See In re* Snyder, 472 U.S. 634 (1985) (a law license requires conduct "compatible with the role of courts in the administration of justice"); U.S. Dist. Ct. E. Dist. of Wash. v. Sandlin, 12 F.3d 861 (9th Cir. 1993) ("once a lawyer is admitted to the bar, although he does not surrender his freedom of expression, he must temper his criticisms in accordance with professional standards of conduct"); *In re* Shearin, 765 A.2d 930 (Del. 2000) (lawyers' constitutional free speech rights are qualified by their ethical duties); Ky. Bar Ass'n v. Blum, 404 S.W.3d 841 (Ky. 2013) ("It has routinely been upheld that regulating the speech of attorneys is appropriate in order to maintain the public confidence and credibility of the judiciary and as a condition of '[t]he license granted by the court.'" [citing *Snyder*]); State ex rel. Neb. State Bar Ass'n v. Michaelis, 316 N.W.2d 46 (Neb. 1982) ("A layman may, perhaps, pursue his theories of free speech or political activities until he runs afoul of the penalties of libel or slander, or into

The plain language of Model Rule 1.6 dictates that information relating to the representation, even information that is provided in a public judicial proceeding, remains protected by Model Rule 1.6(a).[19] A lawyer may not voluntarily disclose such information, unless the lawyer obtains the client's informed consent, the disclosure is impliedly authorized to carry out the representation, or another exception to the Model Rule applies.[20]

At least since the adoption of the ABA Canons of Ethics, the privilege of practicing law has required lawyers to hold inviolate information about a client or a client's representation beyond that which is protected by the attorney-client privilege. Indeed, lawyer ethics rules in many jurisdictions recognize that the duty of confidentiality is so fundamental that it arises before a lawyer–client relationship forms, even if it never forms,[21] and lasts well beyond the end of the professional relationship.[22] It is principally, if not singularly, the duty of confidentiality that enables and encourages a client to communicate fully and frankly with his or her lawyer.[23]

Ethical Constraints on Trial Publicity and Other Statements

Model Rule 3.5 prohibits a lawyer from seeking to influence a judge, juror, prospective juror, or other official by means prohibited by law. Although using public commentary with the client's informed consent may be appropriate in certain circumstances, lawyers should take care not to run afoul of other limitations imposed by the Model Rules. [24]

some infraction of our statutory law. A member of the bar can, and will, be stopped at the point where he infringes our Canons of Ethics.").

[19] *See* ABA Formal Op. 479 (2017). See also cases and authorities cited *supra* at note 10.

[20] One jurisdiction has held that a lawyer is not prohibited from writing a blog that includes information relating to a representation that was disclosed in an open public judicial proceeding after the public proceeding had concluded. In Hunter v. Virginia State Bar, 744 S.E.2d 611 (Va. 2013) the Supreme Court of Virginia held that the application of Virginia Rule of Professional Conduct 1.6(a) to Hunter's blog posts was an unconstitutional infringement of Hunter's free speech rights. The Committee regards *Hunter* as limited to its facts. Virginia's Rule 1.6 is different than the ABA Model Rule. The Virginia Supreme Court rejected the Virginia State Bar's position on the interpretation and importance of Rule 1.6 because there was "no evidence advanced to support it." But see *People vs. Isaac* which acknowledges *Hunter* but finds a violation of Colorado Rule 1.6. We note, further, that the holding in *Hunter* has been criticized. *See* Jan L. Jacobowitz & Kelly Rains Jesson, *Fidelity Diluted: Client Confidentiality Give Way to the First Amendment & Social Media in Virginia State Bar ex rel. Third District Committee v. Horace Frazier Hunter*, 36 CAMPBELL L. REV. 75, 98-106 (2013).

[21] *See* MODEL RULES OF PROF'L CONDUCT R. 1.18(b) (2017) (Even when no client–lawyer relationship ensues, a lawyer who has had discussions with a prospective client shall not use or reveal information learned in the consultation except as permitted by the Rules). *Implementation Chart on Model Rule 1.18*, American Bar Ass'n (Sept. 29, 2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/mrpc_1_18.authcheckdam.pdf.

[22] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9 (2017); *see also* D.C. Bar Op. 324 (Disclosure of Deceased Client's Files) (2004); Swidler & Berlin v. United States, 524 U.S. 399 (1998). *See also* GILLERS, *supra* note 4, at 34 ("[w]hether the [attorney-client] privilege survives death depends on the jurisdiction but in most places it does").

[23] See generally Preamble to ABA Model Rules for a general discussion of the purposes underlying the duty of confidentiality. *See also* GEOFFREY C. HAZARD JR. & W. WILLIAM HODES, THE LAW OF LAWYERING, §§ 9.2 & 9.3 at 9-6, 9-14 (3d ed. Supp. 2012).

[24] *See, e.g., In re* Joyce Nanine McCool 2015-B-0284 (Sup. Ct. La. 2015) (lawyer disciplined for violation of Rule 3.5 by attempting to communicate with potential jurors through public commentary); *see also* The Florida Bar v. Sean William Conway, No. SC08-326 (2008) (Sup. Ct. Fla.) (lawyer found to have violated Rules 8.4(a) and (d) for posting on the internet statements about a judge's qualifications that lawyer knew were false or with reckless disregard as to their truth or falsity).

Lawyers engaged in an investigation or litigation of a matter are subject to Model Rule 3.6, Trial Publicity. Paragraph (a) of Rule 3.6 (subject to the exceptions provided in paragraphs (b) or (c)) provides that:

> A lawyer who is participating or has participated in the investigation or litigation of a matter shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

Thus any public commentary about an investigation or ongoing litigation of a matter made by a lawyer would also violate Rule 3.6(a) if it has a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter, and does not otherwise fall within the exceptions in paragraphs (b) or (c) of Model Rule 3.6.[25]

Conclusion

Lawyers who blog or engage in other public commentary may not reveal information relating to a representation that is protected by Rule 1.6(a), including information contained in a public record, unless disclosure is authorized under the Model Rules.

[25] Pa. Bar Ass'n Formal Op. 2014-300 (2014) (lawyer involved in pending matter may not post about matter on social media). This opinion does not address whether a particular statement "will have a substantial likelihood of materially prejudicing an adjudicative proceeding" within the meaning of Model Rule 3.6.

FORMAL ETHICS OPINION
KENTUCKY BAR ASSOCIATION

ETHICS OPINION KBA E-448
ISSUED: MARCH 14, 2019

The Rules of Professional Conduct are amended periodically. Lawyers should consult the current version of the rule and comments, SCR 3.130 (available at www.kybar.org/237), before relying on this opinion.

SUBJECT: Proposed self-defense opinion

QUESTION: May a lawyer reveal client confidential information reasonably necessary to respond to a former client's public criticism?

ANSWER: No

AUTHORITIES: Rule 1.6 (b)(3),Crystal, Defending Against Internet Criticism: "Silence is Golden," 26 South Carolina Lawyer 12 (2014); Fucile, Discretion in the Better Part of Valor: Rebutting Negative Online Client interviews, 83 Defense Counsel J. 84 (2016); *People v. Issac*, 2016 WL 6124510 (Col. 2016); State ex rel Counsel for the *Nebraska Supreme Court v. Tonderum*, 840 N.W. 487 (Nebraska 2013).

QUESTION: How may a lawyer ethically respond to a former client's public criticism?

ANSWER: See Opinion

NOTE TO READER

This ethics opinion has been formally adopted by the Board of Governors of the Kentucky Bar Association under the provisions of Kentucky Supreme Court Rule 3.530. This Rule provides that formal opinions are advisory only.

The self-defense exception to the duty of confidentiality (1.6(b)(3)is triggered by claims or disciplinary complaints against a lawyer. The exception does not encompass internet criticism. In Defending Against Internet Criticism: Silence is Golden, 26 South Carolina Law Review 12(2014), Nathan Crystal uses the Betty Tsamis case to illustrate: After being fired a flight attendant hired Tsamis to seek unemployment benefits from the state. Apparently Tsamis learned after she was hired that the attendant had been fired because he beat up a female co-worker. After a hearing the claim was denied and the attendant complained about Tsamis on the internet. This eventually resulted in Tsamis being publicly reprimanded for posting the following:

> This is simply false. The person did not reveal all the facts of the situation up front in our first and second meetings. . . . Despite knowing he would likely lose he chose to go forward with a hearing to try to obtain benefits. I dislike it very much when my clients lose but I cannot invent positive facts for clients when they are not there. I fell badly for him but his own actions in beating up a female coworker are what caused the consequences he is now so upset about.

In most instances the best advice is to ignore the criticism. For the lawyer who wants to respond, the Committee recommends the following:

My professional and ethical responsibilities do not allow me to reveal confidential client information in response to public criticism.