21ST CENTURY ETHICS ISSUES – THE INTERNET AND BEYOND

Sponsor: Criminal Law Section
CLE Credit: 1.0 ethics
Wednesday, June 17, 2015
3:35 p.m. - 4:35 p.m.
Thoroughbred 1-3
Lexington Convention Center
Lexington, Kentucky
A NOTE CONCERNING THE PROGRAM MATERIALS

The materials included in this Kentucky Bar Association Continuing Legal Education handbook are intended to provide current and accurate information about the subject matter covered. No representation or warranty is made concerning the application of the legal or other principles discussed by the instructors to any specific fact situation, nor is any prediction made concerning how any particular judge or jury will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgment of the individual legal practitioner. The faculty and staff of this Kentucky Bar Association CLE program disclaim liability therefore. Attorneys using these materials, or information otherwise conveyed during the program, in dealing with a specific legal matter have a duty to research original and current sources of authority.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Presenter</td>
<td>i</td>
</tr>
<tr>
<td>21st Century Ethics Issues – The Internet and Beyond</td>
<td>1</td>
</tr>
<tr>
<td>Kentucky Bar Association Ethics Opinion KBA E-403</td>
<td>5</td>
</tr>
<tr>
<td>Kentucky Bar Association Ethics Opinion KBA E-434</td>
<td>13</td>
</tr>
<tr>
<td>Kentucky Bar Association Ethics Opinion KBA E-437</td>
<td>17</td>
</tr>
<tr>
<td>Ethical Concerns of Internet Communication</td>
<td>25</td>
</tr>
<tr>
<td>Ethical Risks of Technology</td>
<td>31</td>
</tr>
<tr>
<td>ABA Approves Researching Jurors' Public Presence</td>
<td>37</td>
</tr>
</tbody>
</table>
PROFESSOR PETER A. JOY is the Henry Hitchcock Professor of Law at Washington University School of Law in St. Louis where he teaches a legal profession and comparative legal ethics seminar, trial practice & procedure, and co-directs the Criminal Justice Clinic. In the Criminal Justice Clinic, he and his students work closely with the St. Louis County Office of the Missouri State Public Defender Office. Professor Joy co-authors an ethics column for the ABA quarterly publication Criminal Justice, and is the co-author of the book Do No Wrong: Ethics for Prosecutors and Defenders. He writes in the areas of legal ethics, criminal justice, access to justice, and clinical legal education. Professor Joy is past chair of the Professional Responsibility Section of the Association of American Law Schools (AALS), former co-chair of the Ethics and Gideon Committee of the ABA Criminal Justice Section, and a former Program Director for the National Institute of Trial Advocacy (NITA). He received his A.B. from Youngstown State University and his J.D. from Case Western Reserve University.
I. AMERICAN BAR ASSOCIATION (ABA) FORMAL OPINION 11-459, AUGUST 4, 2011

Duty to Protect the Confidentiality of E-mail Communications with One’s Client

A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.

Practice Pointer: In your engagement letter or fee agreement, address the use of email. Also, discuss this explicitly with your client. Ask your client these questions: Where are the computers you use for email? Who has access to each computer? Are any of the computers connected to a network?

II. ABA FORMAL OPINION 11-460, AUGUST 4, 2011

Duty when Lawyer Receives Copies of a Third Party’s E-mail Communications with Counsel

When an employer’s lawyer receives copies of an employee’s private communications with counsel, which the employer located in the employee’s business e-mail file or on the employee’s workplace computer or other device, neither Rule 4.4(b) nor any other Rule requires the employer’s lawyer to notify opposing counsel of the receipt of the communications. However, court decisions, civil procedure rules, or other law may impose such a

---

1 Available at http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf.

2 Available at http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_460_nm_formal_opinion.authcheckdam.pdf.
notification duty, which a lawyer may then be subject to discipline for violating. If the law governing potential disclosure is unclear, Rule 1.6(b)(6) allows the employer's lawyer to disclose that the employer has retrieved the employee's attorney-client e-mail communications to the extent the lawyer reasonably believes it is necessary to do so to comply with the relevant law. If no law can reasonably be read as establishing a notification obligation, however, then the decision whether to give notice must be made by the employer-client, and the employer's lawyer must explain the implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision.

Practice Pointer: Remember, confidentiality (Rule 1.6) requires you to keep confidential and not disclose any "information relating to the representation of [the] client," unless there is an applicable exception to the confidentiality obligation, the client gives "informed consent" to the disclosure, or, under Rule 1.6(b)(6), you may "reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary . . . to comply with other law or court order." This requires you to understand and comply with relevant law. If no law can reasonably be read to establish a reporting obligation, the decision whether to give notice must be made by the employer-client.

**III. ABA FORMAL OPINION 466, APRIL 24, 2014**

Lawyer Reviewing Jurors' Internet Presence

Unless limited by law or court order, a lawyer may review a juror's or potential juror's Internet presence, which may include postings by the juror or potential juror in advance of and during a trial, but a lawyer may not communicate directly or through another with a juror or potential juror.

A lawyer may not, either personally or through another, send an access request to a juror's electronic social media. An access request is a communication to a juror asking the juror for information that the juror has not made public and that would be the type of *ex parte* communication prohibited by Model Rule 3.5(b). The fact that a juror or a potential juror may become aware that a lawyer is reviewing his Internet presence when a network setting notifies the juror of such does not constitute a communication from the lawyer in violation of Rule 3.5(b).

In the course of reviewing a juror's or potential juror's Internet presence, if a lawyer discovers evidence of juror or potential juror misconduct that is criminal or fraudulent, the lawyer must take reasonable remedial measures including, if necessary, disclosure to the tribunal.

---

3 Available at [http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_466_final_04_23_14.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_466_final_04_23_14.authcheckdam.pdf).
Practice Pointer: Searching potential juror’s Internet presence is permitted, but subject to any court orders, court rules, or laws in the jurisdiction. Sending an access request to a potential juror’s or juror’s electronic social media is prohibited, and some jurisdictions prohibit using services, such as LinkedIn, that send automatic notifications to juror-subscribers.

IV. KENTUCKY BAR ASSOCIATION ETHICS OPINIONS

A. Email

Ethics Opinion KBA E-403 (March 1998) (attached)

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 SCR 3.130(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 [SCR 3.130(7.10)-(7.20), and the so called advertising rules set forth at SCR 3.130(7.01)-(7.08)] should apply to a lawyer's "web-site" on the Internet.

B. Social Network Sites

Ethics Opinion KBA E-434 (November 17, 2012) (attached)

Subject: Ethical Considerations Relating to a Lawyer's Use of Social Network Sites⁴ to Benefit a Client⁵

---

⁴ 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 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.

⁵ 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.
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.


C. Cloud Computing

Ethics Opinion KBA E-437 (March 21, 2014) (attached)

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.

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/237) 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.


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[sic] 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 the 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 ethics 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[sic] 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[sic] 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[sic] 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[sic] 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.
Subject: Ethical Considerations Relating to a Lawyer’s Use of Social Network Sites¹ to Benefit a Client²

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.


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 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

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[sic] 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.
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. 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. Also relevant is SCR 3.130(8.4), which prohibits the lawyer from engaging in dishonest conduct.

---


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 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."
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 unconsented 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.

---

\(^6\) 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."
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 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.
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

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

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 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. 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.

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

---

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.
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 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.

---

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.
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

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 arrangement7 regarding online storage or treatment of confidential client

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.

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/.
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?

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?

\(^8\) 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."


\(^9\) 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.
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?

**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)).

**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.

---

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.

The use of the Internet by attorneys – through websites, social networking, and blogging – has increased dramatically in recent years.

The American Bar Association’s Legal Technology Survey Report found that among the lawyers surveyed, 78 percent maintain an online presence on sites such as Facebook or LinkedIn as compared to 43 percent in 2009 and 15 percent in 2008; 17 percent have landed a client through the use of online communities or social networks; and 6.7 percent have a virtual law practice. This increased use raises a host of ethical issues. Some lawyers, for example, appear to believe that communications between attorneys that take place on the Internet are insulated from ethics rules, as when a Miami criminal defense lawyer recently posted a photo of a client’s underwear on Facebook – and quickly lost her job. (See David Ovalle, “Lawyer’s Facebook Photo Causes Mistrial in Miami-Dade Murder Case,” Miami Herald (Sept. 13, 2012), http://tinyurl.com/9h5ntf3.) As the fate of this lawyer – and the rest of this column – demonstrate, communications that take place on the Internet are not beyond the reach of ethics rules.

Among the significant issues are ones regarding advertising and solicitation. For example, can blogs constitute advertisements for purposes of Model Rule 7.2? The application of advertisement and solicitation rules to Internet communications is a detailed subject we will address in a separate column.

**Inadvertent Clients**

The Model Rules of Professional Conduct do not address when and how someone becomes a lawyer’s client. Instead, state tort and contract law govern this subject. In many situations, it is obvious when a person is or is not a lawyer’s client. But in some situations, including initial interaction between a lawyer offering and a stranger seeking legal services, when someone gains client status is not clear. As we discussed in our last column, “Client or Prospective Client: What’s the Difference?,” 27 Crim. Just. 51 (Fall 2012), courts tend to use a three-part formula to determine the existence of a lawyer-client relationship: (1) a request for legal advice or other legal service; (2) the giving of legal advice or other legal service; and (3) reasonable reliance.

Requests for advice are often made through Internet communications, and lawyers routinely offer advice in response. On websites such as AVVO, for example, requests and advice are routinely exchanged. One key issue here is the reasonableness of reliance on such advice. In such Internet settings, lawyers regularly use disclaimers and warnings to avoid a finding of reasonableness. But there may well be limits. For

---

* Peter A. Joy is the Henry Hitchcock Professor of Law and director of the Criminal Justice Clinic at Washington University School of Law in St. Louis, Missouri. He can be reached at joy@wulaw.wustl.edu.

** Kevin C. McMunigal is the Judge Ben C. Green Professor of Law at Case Western Reserve University School of Law in Cleveland, Ohio. He can be reached at kcm4@case.edu.
example, the District of Columbia Ethics Committee has held that "even the use of a disclaimer may not prevent the formation of attorney-client relationships if the parties' subsequent conduct is inconsistent with the disclaimer." (D.C. Ethics Op. 316 (2002)) The opinion warns that "lawyers seeking to avoid formation of attorney-client relationships through chat room conversations would be well advised to avoid providing legal advice in such communications." (Id.)

Another issue is what constitutes legal "advice." General advice, such as "consult a lawyer as soon as possible" or a discussion of general legal principles, is usually not treated as legal advice. Information or advice doesn't become "legal advice" for purposes of client creation unless it involves application of the law to the particular facts of a person's situation. But such a line between "general information" and "legal advice" is not always easy to spot, and a lawyer could easily cross it in the context of an Internet exchange with someone looking for legal advice. A key is to avoid recommendations tailored to the facts of the individual's situation. The lawyer "should not seek to elicit or respond to the specifics of particular individuals' situations." (Id.) Other ethics committees have taken the same position concerning lawyers speaking at public seminars or on radio talk shows. (See, e.g., Ass'n of the Bar of the City of N.Y. Comm. on Prof'l & Judicial Ethics, Formal Op. 1998-2 (1998); Ohio Sup. Ct. Bd. of Comm'r's on Grievances & Discipline, Op. 94-13 (1994).)

Inadvertent Prospective Clients

Unlike becoming a client, the Model Rules do address when and how someone becomes a lawyer's "prospective client," a status we addressed in detail in our last column. Model Rule 1.18 creates this status, between "client" and "nonclient." It gives rise to both confidentiality and conflict-of-interest duties. These duties may restrict the lawyer's future conduct, such as accepting representation of a future client with interests that conflict with those of the prospective client.

A person who "consults with a lawyer" about the possibility of representation but never receives representation – because the client decides not to hire the lawyer or the lawyer decides against taking the person on as a client – is a "prospective client." Can communications between a person and a lawyer that take place through a website or social network create prospective client status? The answer is clearly "yes" under certain circumstances.

The text of the rule indicates that a person becomes a prospective client only if he or she "consults with a lawyer" about the possibility of representation. This phrase suggests that there must be some reciprocity to the communication, that the lawyer must provide some indication of willingness to listen and consider representation before the person becomes a "prospective client." A key here is whether the lawyer makes a communication that is seen as inviting the submission of information.

Comment [2] to Model Rule 1.18, newly adopted in August 2012, explains that a person who "communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship" does not gain prospective client status (emphasis added). Whether the communication is bilateral and whether the person has a reasonable expectation that the lawyer is willing to discuss representation "depends on the circumstances." Reciprocity and reasonableness will be present, for example, if the lawyer "either in person or
through the lawyer's advertising in any medium, specifically requests or invites the
submission of information about a potential representation without clear and reasonably
understandable warnings and cautionary statements that limit the lawyer's obligations,
and a person provides information in response." In contrast, reciprocity and
reasonableness will not be present "if a person provides information to a lawyer in
response to advertising that merely describes the lawyer's education, experience, areas
of practice, and contact information, or provides legal information of general interest."
Comment [2] states that it is important for the lawyer to include an effective disclaimer to
avoid the formation of an unintended prospective client relationship with someone who
communicates unilaterally with the lawyer. Several ethics committees have also taken
this position. (See, e.g., Mass. Bar Ass'n, Op. 07-01 (2007); Ass'n of the Bar of the City

**Competence**

Model Rule 1.1, perhaps the most fundamental of all ethics rules, requires that a lawyer
act competently in representing a client. Competence requires adequate factual
investigation. If a lawyer-client relationship is found to have been established through a
lawyer responding to a request for advice, a key question is whether the lawyer acted
competently by having adequate information before giving advice. Advice offered
through a website, social network, or blog is likely to be based on limited and possibly
inaccurate information.

Competence also requires a lawyer to determine whether a matter requires specialized
knowledge or experience. Communications on social networks and blogs are often free-
flowing and informal, and may tempt a lawyer to give advice in a field in which the lawyer
is not competent. Lack of experience in a matter is no defense to a charge of
incompetent representation. (See, e.g., Matter of Deardorff, 426 N.E.2d 689 (Ind. 1981);
Attorney Grievance Comm'n of Maryland v. Brown, 517 A.2d 1111 (Md. 1986); Matter of
Yetman, 552 A.2d 121 (N.J. 1989).)

**Confidentiality**

Discussion of pending or even past cases on a website, social network, or blog creates
an obvious risk of a confidentiality violation. Model Rule 1.6 protects a current client's
confidential information, and Model Rule 1.9 protects a past client's confidential
information. A lawyer might be enticed to engage in a discussion of current or past cases
in order to appear more interesting or important in the eyes of friends and acquaintances
or to generate interest in a website or blog to increase name recognition in hopes of
gaining future business. A lawyer might seek to avoid violating confidentiality by not
mentioning the client's name or by using a pseudonym for the client. But if a reader of
the blog, such as another lawyer or a party other than the client involved in a case, can
"connect the dots" to figure out to whom the lawyer is referring, confidentiality will be
violated.

Former public defender Kristine Ann Peshek's use of her blog, "The Bardd (sic) Before
the Bar – Irreverant (sic) Adventures in Life, Law and Indigent Defense," provides a
cautory tale for any lawyer blogging or using other social media. (In re Peshek, No.
09CH89 (Ill. Attorney Registration & Disciplinary Comm'n Aug. 25, 2009), available at
http://iardc.org/09CH0089CM.html.) In addition to discussing her hobbies and health,
Peshek devoted a portion of her blog to client stories. She referred to her clients by
either their first name or jail identification number. Her blog was open to the public and not password-protected. In one story, in which she used her client's jail identification number, Peshek wrote, "This stupid kid is taking the rap for his drug-dealing dirtbag of an older brother because 'he's no snitch.'" (Id.) In other postings, she mentioned client "Dennis," gave his court date and facts from the case, and said her client was "standing there in court stoned." Peshek also gave details of a probation revocation hearing for "Laura" that detailed a hearing in which Peshek described her client lying to the judge. (Id.)

In addition to losing her job, Peshek received a sixty-day suspension from the practice of law for breaching client confidentiality, failing to call upon a client to rectify a fraud upon the court, failing to disclose to a tribunal a material fact to avoid assisting a client in a criminal or fraudulent act, conduct that is prejudicial to the administration of justice, and conduct involving dishonesty, fraud, deceit, or misrepresentation.

Truthfulness

The Model Rules contain several broad prohibitions of lawyer false statements. Model Rule 4.1(a) states that "[i]n the course of representing a client a lawyer shall not knowingly . . . make a false statement of material fact or law to a third person." A lawyer's communications in blogging or social networking might not fall within this provision if not made in the course of representing a client. But Model Rule 8.4(c) sets forth a broader provision that "[i]t is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Unlike Model Rule 4.1(a), this prohibition contains no limitation to conduct in the course of representing a client. Thus, it might reach false statements made by a lawyer on a blog about a case in which the lawyer is not participating.

A number of jurisdictions have addressed the use of a social network to investigate and gather facts about a case. The Philadelphia Bar in Opinion 2009-02 took a restrictive position, finding that the lawyer can't use information even if it is accessible to all social network members. Someone working for a lawyer also cannot "friend" someone to gain information without revealing the purpose in doing so and the individual's association with the lawyer. Unlike Philadelphia, New York State Bar Opinion 843 does allow a lawyer who is a network member to use information accessible to all network members. But, like Philadelphia, it prohibits a lawyer from " friending" someone without disclosing the lawyer's purpose. New York City Bar Formal Opinion 2010-2 takes an even more lenient position, allowing a lawyer to "friend" without revealing the purpose as long as no false statements, such as ones about identity or purpose, are used.

Other jurisdictions have recently allowed lawyers to use deception in investigations, which would presumably include deception involving social networks. (For detailed coverage of this topic, see our previous column: "Deceit in Defense Investigations," 25 Crim. Just. 36 (Fall 2010).)

Anticontact Rule

Model Rule 4.2 prohibits one lawyer in a litigated case from communicating with the client of another lawyer in the matter. E-mailing another lawyer's client or responding or even reading an e-mail sent to the lawyer from another lawyer's client may violate this rule. What about contacting an opposing lawyer's client through Facebook? Or
responding to a communication from that lawyer's client on Facebook? There is no reason to believe this wouldn't be barred by the rule.

Blogging raises interesting questions about the reach of the anticontact rule. What if defense counsel in a high-profile litigated case makes what they consider a generous settlement offer on behalf of the client only to be quickly rebuffed by plaintiff's counsel? What if defense counsel suspects plaintiff's counsel may not have fully advised the plaintiff of the settlement offer, or perhaps even communicated it to the plaintiff? May defense counsel (with the defendant's consent) discuss the settlement offer, and counsel's reasons that the plaintiff should accept it, on a blog in the hope that the plaintiff will read it?

**Trial Publicity**

Model Rule 3.6 limits what lawyers participating in a litigated case may say publicly about that case. It prohibits statements that "will have a substantial likelihood of materially prejudicing" a trial. This prohibition, though, is limited to statements "the lawyer knows or reasonably should know will be disseminated by means of public communication." Interpretation and application of this language raises some interesting questions. Does making a statement on a blog itself constitute dissemination "by means of public communication"? What about statements made on a social network? What if a lawyer is aware that reporters who are following a case also read the lawyer's blog or follow the lawyer on Twitter? Would the lawyer know or reasonably be expected to know (Model Rule 3.6) that statements posted on these social media will be read and repeated by reporters in other public media? The more popular communication outlets such as blogs and Twitter become, the greater the likelihood that lawyer statements on them will fall under Model Rule 3.6.

**Criticism of Judges**

Model Rule 8.2(a) prohibits a lawyer from making a false statement about the "qualifications or integrity" of a judge that is known to be false or "with reckless disregard as to its truth." Note that there is no express provision limiting the rule to statements made or disseminated publicly. Are statements made on a blog or social network exempt from this rule?

In the Peshek disciplinary case above, some of the postings that resulted in job loss and discipline referred to one judge as "a total asshole" and another as "Judge Clueless." In 2009, the Florida Bar disciplined attorney Sean Conway for his comments about a judge before whom he had appeared after he described her as "an evil, unfair witch" with an "ugly, condescending attitude" who was "seemingly mentally ill."

**Conclusion**

Cases and ethics opinions dealing with the legal ethics of social networking teach us that statements and acts likely to land lawyers in ethical trouble outside the Internet context are also likely to land lawyers in ethical trouble when made or done on a social network, blog, or website. The increasingly public nature of such Internet venues makes discovery by ethics authorities increasingly likely, and the permanence of electronic records eases enforcement. The primary lesson: if you wouldn't do or say something off the Internet, don't do or say it on the Internet.
Law practice today increasingly depends on technology. The ABA 2010 Legal Technology Survey Report, for example, found that 76 percent of responding lawyers used smart phones, up from 64 percent in 2009. Both prosecutors and defense counsel use e-mail, circulate electronic drafts of legal pleadings, briefs, and other case materials, and rely on smart phones and other mobile devices. Many law offices use remote data backup and cloud computing. Such use of technology raises a number of ethical issues.

What if a lawyer sends an e-mail intending it to be delivered to one recipient only to find that it was accidentally sent to one or more unintended recipients? What if a lawyer loses a smart phone containing client e-mails and documents? Such errors can seriously compromise client confidentiality and attorney-client privilege as well as do serious practical and strategic damage to a client's case.

In this column we explore the ethical issues some of today's technology creates for lawyers and what ethics rules and opinions say about precautions lawyers should take to protect client information.

**Relevant Model Rules**

Confidentiality and competence are twin touchstones for assessing ethical obligations regarding technology. In sum, lawyers must act competently to protect confidentiality. Comment [16] to Model Rule 1.6 requires a lawyer to "act competently to safeguard" confidential information "against inadvertent or unauthorized disclosure" by either the lawyer or others working with the lawyer. Ethics authorities across the country emphasize the importance of the interaction between competence and confidentiality as lawyers and law firms make greater use of technology.

What does competence require regarding technology? We discuss in detail below what ethics authorities say about some specific technology issues. Certain aspects of competence, though, apply to all technology issues and are worth stating at the outset. Comment [6] to Model Rule 1.1 on competence makes clear that the duty of competence is dynamic rather than static. It states that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice" (emphasis added). Competence requires that a lawyer stay aware of the technology currently used in law practice, the risks it poses, and the security measures available to reduce those risks. Competence mandates that a lawyer keep pace with professional peers in addressing the risks of technology. Comment [5] to Model Rule 1.1 states that

---

* Peter A. Joy is the Henry Hitchcock Professor of Law and director of the Criminal Justice Clinic at Washington University School of Law in St. Louis, Missouri; he can be reached at joy@wulaw.wustl.edu.

** Kevin C. McMunigal is the Judge Ben C. Green Professor of Law at Case Western Reserve University School of Law in Cleveland, Ohio; he can be reached at kcm4@case.edu.
competence includes "use of methods and procedures meeting the standards of competent practitioners." As engineers develop and lawyers adopt new security measures, such as encryption software for e-mail and scrubbing software for metadata in electronic files, a lawyer who lags behind other lawyers in such security measures runs the risk of being found incompetent in safeguarding client information.

E-mail

Consider the following scenario. Lawyer 1 is outside defense counsel for a corporation criminally charged in a fraud case. In an e-mail, the prosecutor communicates to Lawyer 1 a guilty plea offer with a tight deadline. Lawyer 1 is traveling on another case when she receives the prosecutor's offer. Before boarding a plane, she sends an e-mail with her smart phone to the corporation, alerting in-house counsel to the offer. Once at her destination, Lawyer 1 finds a reply e-mail from in-house counsel asking her to assess the strengths and weaknesses of the corporation's position and the advantages and disadvantages of the guilty plea offer. In her hotel room that night, Lawyer 1 writes a lengthy e-mail responding to in-house counsel's request in which she reviews the anticipated testimony of several defense witnesses she recently interviewed. Lawyer 1 sends the e-mail to in-house counsel and accidentally sends a copy to the prosecutor. May the prosecutor read the e-mail? Must the prosecutor notify Lawyer 1 of her mistake? Has Lawyer 1 violated her ethical obligations to her client?

Recipient obligations. As we discussed in a prior column, "Brother's Keeper: Must You Protect Opponent's Confidentiality?," 18 Crim. Just. 43 (Fall 2003), jurisdictions vary greatly in the obligations they impose on the recipient of a misdirected e-mail. Some take an approach that seeks to protect the sender from such a mistake, mandating that the recipient not read such an e-mail and notify the sender of her mistake. (See, e.g., N.J. Rules of Prof. Conduct R. 4.4(b).) Other jurisdictions adopt an unprotective approach, allowing the recipient to read and use the content of such a misdirected e-mail. (See, e.g., Mt. Hawley Ins. Co. v. Felman Production, Inc., 271 F.R.D. 125, 130-31 (S.D. W. Va. 2010).)

Sender obligations. What about Lawyer 1, the sender? Did she violate her ethical obligations by accidentally sending the e-mail to the prosecutor? A single act of misdirecting an e-mail is unlikely to be treated as an ethical violation. But Lawyer 1's having used e-mail to communicate highly sensitive confidential information without using encryption may be an ethical violation. Ethics authorities allow lawyers to use e-mail to communicate with and about clients and do not require lawyers routinely to encrypt all e-mails, even those containing confidential information. (See, e.g., ABA Formal Op. 99-143 (1999); Mass. Bar Ethics Op. 195 (2008); N.Y. Bar Ethics Op. 709 (1998); Utah State Bar Ethics Op. 00-01 (2000).) But when a lawyer is transmitting highly sensitive information of the sort transmitted by Lawyer 1, some ethics authorities recognize a duty either to encrypt e-mail or use a more secure means of communication. (See, e.g., Cal. State Bar Formal Op. 2010-179 ("Encrypting email may be a reasonable step for an attorney to take... when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous."); D.C. Bar Ethics Op. 281 (1998) (stating that unencrypted e-mail is permissible in most situations but "individual circumstances may require greater means of security").)
Lawyer 2 represents a public official under investigation for accepting bribes to influence government contracts. The prosecutor offers a sentence reduction if the client pleads guilty and cooperates in the bribery investigation of another public official. The amount of the sentence reduction will depend on the cooperation the client provides. The client tells Lawyer 2 that he has information not only about the public official accepting bribes, but also about crimes the prosecutor is currently unaware of involving members of organized crime rigging bids on government construction contracts. Lawyer 2 and the client exchange drafts of a proposed plea agreement and proffer of testimony that include information about both the bribery and the bid rigging. The client, though, has second thoughts about revealing the bid rigging because he fears for his family's safety. Lawyer 2 deletes all references to the bid rigging in the plea agreement and proffer before sending them in electronic form via e-mail to the prosecutor for review. The "deleted" information about the bid rigging, though, remains accessible to the prosecutor in the file's metadata.

May the prosecutor search the electronic file for confidential metadata? In technology jargon, such searching is sometimes referred to as "mining" for metadata. Did Lawyer 2 violate his ethical obligations by failing to remove metadata from the electronic file? Again, in technology jargon, such removal is sometimes referred to as "scrubbing" metadata from an electronic file.

Recipient obligations. As with misdirected e-mail, jurisdictions vary greatly in the obligations they impose on lawyer recipients of electronic files containing metadata. Some, such as Alabama, take a protective approach mandating that lawyers not search for confidential metadata. (See, e.g., Ala. Ethics Op. 2007-02.) Other jurisdictions, such as Maryland, adopt a nonprotective approach allowing recipients to mine for metadata. (See, e.g., Md. State Bar Op. 2007-09.)

Sender obligations. A lawyer can eliminate the risk of disclosing confidential metadata in several ways. The lawyer can use "scrubbing" software to remove metadata prior to transmitting an electronic file. Such software is readily available, relatively inexpensive, and now widely used by lawyers. One can also eliminate the risk posed by metadata by converting the final version of a document into a PDF or other "picture" file that contains none of the original file's metadata. The ready availability of various means to eliminate the risks of metadata and the fact that most practitioners now use some means of eliminating metadata strongly suggest that a lawyer who fails to use such measures fails to use "methods and procedures meeting the standards of competent practitioners" as required by Comment [5] to Model Rule 1.1. (See, e.g., Colo. Bar Op. 119 (2008); Iowa State Bar Op. 11-01 (2011).)

Smart Phones, Tablets, Laptops

Lawyer 3 attends a pretrial hearing. During breaks, she sends e-mails about the case to the client and other lawyers in her firm using her iPhone. At the end of the hearing, Lawyer 3 packs her briefcase and heads back to her office. Inadvertently, though, she leaves her iPhone on one of the courtroom counsel tables. The prosecutor and case agent stay in the courtroom for several minutes after the hearing discussing the witnesses they plan to call at trial. As they leave the courtroom, the case agent sees the iPhone, picks it up, and hands it to the prosecutor. When Lawyer 3 gets to her office,
fear sets in as she searches her coat pockets and briefcase in vain for the phone. At first, she thinks about the hassle and expense of replacing the phone. When she realizes where she left it and remembers what is on it – attorney-client e-mails and texts, as well as some documents – her fear turns to panic. Has Lawyer 3 committed an ethics violation if confidential client information is revealed to the prosecution through loss of the cell phone?

**Recipient obligations.** Unlike a misdirected e-mail or possible metadata in an electronic document, the prosecutor knows immediately that both the phone and everything on the phone belongs to Lawyer 3. In that sense, it is much like a wallet found on the street or a misdirected document a lawyer might receive with notice that it belongs to someone else.

We are not aware of any ethics opinions that address lost smart phones, but some ethics authorities have addressed the analogous situation of a lawyer receiving a document or other material with notice that the material belongs to someone else. In those situations, failure to return the material has been found to be a dishonest act, in violation of Model Rule 8.4(c). Additionally, the recipient lawyer has an obligation not to review the contents. (See, e.g., D.C. Ethics Op. 256 (1995); D.C. Ethics Op. 318 (2002).) The same reasoning would apply to the prosecutor finding the smart phone.

**Lawyer 3’s obligations: password protection, locating, and remote wiping?** Three technological measures are available to protect client confidentiality if a lawyer loses a mobile device such as an iPhone. First, password protection is typically available on such devices if the lawyer simply enables it. Second, there are applications that permit an owner to locate a lost or stolen mobile device using a computer or another mobile device. Third, applications permit one remotely to erase or “wipe” data on a lost or stolen mobile device.

Password protection is a standard feature on virtually all smart phones as well as tablet and laptop computers. No added expense is involved. It takes less than a minute to enable password protection and create a four-digit password to protect data on a smart phone. Tablet and laptop computers also have password protection features. The ready availability and ease of use of password protection, along with the fact that many lawyers and others already routinely use password protection, strongly suggest that any competent practitioner would use password protection on a device containing confidential client information.

Locator applications, such as “Find My iPhone,” allow one to use another device to locate a missing smart phone, tablet, or laptop on a map. The owner can display a message or play a sound on the mobile device. Purchasing such an application could assist a lawyer in recovering a lost or stolen mobile device used for client matters.

Many operating systems and locator applications come with a wiping feature that permits one to erase the data on the device remotely. Remotely wiping a smart phone or other mobile device means resetting the device to its factory default settings and clearing any data stored on it.

To use mobile devices competently for client matters, we believe that password protection has become accepted practice and thus required for a lawyer to be considered competent in securing client information. The extra steps of using locator
apps and remote wiping capabilities are also advisable, if not required by prevailing practice, to provide extra layers of protection for client information.

Some firms, as an additional security measure, require lawyers to segregate client information in the form of e-mail and documents from the lawyers' personal information, just as client property must be kept separate from a lawyer's property. For example, some firms require each lawyer to use separate smart phones and separate computers for work and personal use. In addition to segregating client information, devices provided by a firm often have greater security features than are likely to be found on personal devices. Using separate devices also reduces the risk that a lawyer may accidentally compromise client confidential information when making personal use of an electronic device.

Lawyers often use smart phones, tablets, and laptops outside their offices and connect them to the Internet on Wi-Fi in a coffee shop, airport, or courthouse. If the lawyer is using the device for client work, the client's confidential information may be accessed by hackers if the network is unsecured. As discussed previously, this raises issues of competence under comments [16] and [17] to Model Rule 1.1. California Standing Committee on Professional Responsibility and Conduct Formal Opinion 2010-179 addresses the use of public wireless Internet connections to conduct legal research on client matters and exchange e-mail with clients. The committee observed that ethical guidance to lawyers has not kept pace with ever-evolving technology. While e-mail on a secured network may not need encryption, talking or sending e-mail or a text message on an unsecured network, such as public access Wi-Fi, does raise ethical concerns. With regard to use of public wireless connections, the committee concluded that the lawyer may not use a wireless connection for client work and communications unless the lawyer takes appropriate precautions, such as a combination of file encryption, encryption of wireless transmissions, and a personal firewall. Depending on the sensitivity of the matter, the lawyer may have to avoid using public wireless connections or notify the client of the possible risks of disclosure of confidential information and seek client consent.

**Remote Data Backup and Cloud Computing**

Many lawyers now use remote data backup and cloud computing. Both raise questions of competence and confidentiality. Remote data backup involves a lawyer keeping original electronic files on computers or servers in the lawyer's office while contracting with a third party to keep electronic copies of the files at another location outside the lawyer's office. With cloud computing, the lawyer keeps original electronic files outside the lawyer's office on a server controlled by another person. Examples include Gmail, Google Docs, Dropbox, or iCloud. In both remote data backup and cloud computing, the primary concern is potential third-party access to confidential client information.

Several state ethics opinions have addressed remote data backup and cloud computing. The consensus is that both are permissible if the lawyer takes reasonable steps to guard against disclosure and unauthorized access.

"Reasonable steps" for remote backup may include entering into an enforceable agreement with the remote backup provider to preserve confidentiality and security of the client information, evaluating the security measures of the provider to determine if they are adequate, and periodically monitoring the security measures. (See, e.g., N.Y. State Bar Ethics Op. 842 (2010).)
"Reasonable care" for cloud computing may include backing up data to restore data that has been lost or destroyed, installing a firewall to limit access to the law office network, and implementing electronic audit trail procedures to monitor who is accessing the data.

Pennsylvania Formal Opinion 2011-200 provides a thorough analysis of the issues and summarizes ethics opinions on the subject of cloud computing from more than a dozen states. The committee notes that some of the benefits of cloud computing are that it can simplify document management and control costs by efficiently handling voluminous data with minimal infrastructure expenses for the lawyer. But the lawyer must investigate the provider to assure that it has sufficient security measures in place, determine that the provider has an ongoing third-party audit of security, and create plans to address security breaches. In addition, the lawyer who uses remote data backup or cloud computing must take steps to "assure that the jurisdictions in which the data are physically stored do not have laws or rules that would permit a breach of confidentiality in violation" of the ethics rules. (Id.)

The lawyer must also enter into an enforceable written service agreement with the provider that guarantees confidentiality and prohibits unauthorized access. For example, the provider should be required to notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider turns it over. The lawyer should also be permitted to audit the provider's security procedures and obtain copies of security audits. Finally, the provider should ensure that the lawyer has the ability to retrieve data if the lawyer terminates the agreement or the provider goes out of business. Provisions such as these will help the lawyer protect client confidentiality as well as guarantee the lawyer access to the data.

Finally, the Pennsylvania ethics opinion, like many in other states, advises that, depending on the scope of representation and sensitivity of the data involved, the lawyer may have to inform the client in advance of the attorney's use of cloud computing, outline the risks as well as the advantages of online storage and transmission, and obtain client consent. If the client instructs the lawyer not to use certain technology, then such technology should not be used in the representation of that client.

Conclusion

Competence and confidentiality require a lawyer to be up to speed on current technology, its risks, and how to deal with those risks. Lawyers need to educate themselves to ensure that the communication tools and methods they use are secure. In many instances this will require lawyers to seek out technical education and assistance from others. Acting competently in regard to technology to protect confidentiality not only protects the lawyer from ethical violations, it also reduces the risks of damaging a client's case and alienating the client.
Electronic devices and their ubiquity, along with the Internet and social media, create a host of challenges for the jury system. One is the risk that jurors may communicate improperly during a trial. Another is the risk that jurors may attempt to do their own factual or legal "research" about a case, in effect doing an end run around the limitations established by the rules of evidence. Lawyers using the Internet to find information about potential jurors during jury selection pose an additional challenge. Competency may well require a lawyer to do such electronic research. But at the same time, a lawyer is prohibited from communicating with or influencing a juror outside the courtroom. Ethics authorities in a number of states have addressed these issues in recent years, and the ABA has recently weighed in on them as well.

The ABA Standing Committee on Ethics and Professional Responsibility recently issued an advisory ethics opinion explaining that, unless limited by law or a court order, a lawyer may review a juror's or potential juror's background and presence on websites and social media. In Formal Opinion 466 (Apr. 24, 2014), available at http://tinyurl.com/pqv9dbn, the standing committee explains that Model Rule 3.5(b) prohibits a lawyer from communicating _ex parte_ with a juror or prospective juror, but a lawyer may review a juror's public presence on the Internet. However, a lawyer may not request access to a juror's social media accounts, concluding that such a request would violate Model Rule 3.5's prohibition against _ex parte_ communication with a juror.

The rationale for prohibiting contact with jurors or prospective jurors is to prevent improper influence on jurors, who should decide matters solely upon the evidence produced during trial. The standing committee observes that there is also "a strong public interest in identifying jurors who might be tainted by improper bias or prejudice." (Id. at 2.) The new ethics opinion seeks to strike a balance between these two policies and states that "[l]awyers need to know where the line should be drawn between properly investigating jurors and improperly communicating with them." (Id.) Citing several state and local ethics opinions that have previously addressed this issue, this formal opinion highlights and is generally consistent with a trend among bar ethics committees coming to grips with the emerging use of social media in the practice of law.

While jury _voir dire_ typically serves the function of identifying and weeding out potential jurors based on possible bias or prejudice, lawyers have long engaged in pretrial investigation of prospective jurors' backgrounds for evidence of possible bias or prejudice in preparation for jury _voir dire_. In high-profile cases, lawyers often use jury

---

* Peter A. Joy is the Henry Hitchcock Professor of Law and director of the Criminal Justice Clinic at Washington University School of Law in St. Louis, Missouri; he can be reached at joy@wulaw.wustl.edu.

** Kevin C. McMunigal is professor of law at Case Western Reserve University School of Law in Cleveland, Ohio; he can be reached at kcm4@case.edu.
consultants to poll persons likely to qualify as jurors in a locale to identify which demographic groups and personal qualities would be most sympathetic to their clients. Lawyers also conduct personal background research of potential jurors using credit checks and online court records, as well as examining property and tax records. In today's Internet world, it is both obvious and logical that lawyers would turn to the Internet to research prospective jurors.

For example, in 2011 the district attorney in Cameron County, Texas, announced that his office would use prospective jurors' Facebook profiles and postings to assist with jury selection. (Laura B. Martinez, "Cameron Co. DA Will Check Facebook Profiles for Jury Picks," Brownsville Herald, Jan. 17, 2011.) That same year, a district attorney in Oregon stated that he used Facebook searches to help pick a jury in a death penalty case. (Ana Campoy & Ashby Jones, "Searching for Details Online, Lawyers Facebook the Jury," Wall St. J., Feb. 22, 2011.) The prosecutor used details such as whether CSI: Crime Scene Investigation was a favorite television show to determine whether potential jurors might have unrealistic expectations about the use of forensic evidence. He also looked for clues on Facebook pages to determine how they might feel about the defendant. Another news article identified a criminal defense lawyer in Missouri who builds Excel spreadsheets on potential jurors using Facebook, MySpace, Google, and the state database of civil and criminal cases. (Brian Grow, "Internet v. Courts: Googling for the Perfect Juror," Reuters (Feb. 17, 2011), http://tinyurl.com/qbobmmy.) In a case involving an African-American client, the lawyer sought to keep a white female on the jury because the juror's Facebook page included pictures of the juror with an African-American man.

Recognizing the increasing use of websites and social media, the standing committee's opinion addresses three levels of lawyer review of juror Internet presence: (1) lawyer review of a juror's website or electronic social media (ESM); (2) lawyer review where a lawyer requests access to a juror's ESM; and (3) lawyer review of a juror's Internet presence where the juror becomes aware of the lawyer's review through a website or ESM feature that notifies the juror of the identity of the lawyer viewer. The opinion also discusses a lawyer's obligation upon discovery of juror misconduct via social media.

**Improper Communications**

Before reviewing potential jurors' online presence, a lawyer must first be familiar with local court rules, standing orders, case authority, and, in some cases, a case management order. If there is no rule, precedent, or court order, then the jurisdiction's version of Model Rule 3.5 will set the ethical limits of communications with jurors and potential jurors.

Model Rule 3.5(b) states that a lawyer may not communicate *ex parte* with a juror or prospective juror during a proceeding unless authorized to do so by law or court order. This prohibition includes any communications leading up to trial and during trial. Violating this rule may lead to professional discipline. (See, e.g., The Florida Bar v. Peterson, 418 So.2d 246 (Fla. 1982) (publicly reprimanding and imposing a one-year probation on attorney for sitting with jurors in restaurant during trial recess in spite of lack of intent to influence jurors); In re Nelson, 750 S.E.2d 85 (S.C. 2013) (imposing a six-month suspension on prosecutor for communicating with a juror during case tried by another prosecutor in his office); Matter of Holman, 286 S.E.2d 148 (S.C. 1982) (disbarring attorney for communicating with a juror selected for trial).)
In addition, unauthorized communication with a juror or prospective juror may trigger contempt of court proceedings. (See, e.g., U.S. v. Warlick, 742 F.2d 113 (4th Cir. 1984) (affirming contempt of court conviction of lawyer using private investigator to contact and question prospective jurors).) If the communication is made with the intent to influence a juror's vote or opinion, it also may constitute the crime of jury tampering. (See, e.g., 18 U.S.C. §§1503-04 (prohibiting communications with jurors with intent to influence them); N.Y. Penal Law §215.25 ("A person is guilty of tampering with a juror in the first degree when, with intent to influence the outcome of an action or proceeding, he communicates with a juror in such action or proceeding, except as authorized by law.").)

A lawyer is also prohibited from violating the ethics rules through the acts of another, Model Rule 8.4(a), and may not use others to communicate with jurors or prospective jurors. At least one state ethics opinion, South Carolina Ethics Op. 93-27 (1993), has considered this prohibition in the context of communicating with jurors and found that a lawyer cannot use a third party to communicate with prospective jurors. In In re Myers, 584 S.E.2d 357 (S.C. 2003), a prosecutor received a reprimand for permitting a member of his jury selection team to telephone a potential juror.

The fact that a communication with a juror or prospective juror may occur online, rather than in person or over the telephone, does not exempt the communication from the ethical or legal proscriptions. But does researching prospective jurors using the Internet constitute impermissible communications with them?

**Duty of Competency**

Model Rule 1.1, perhaps the most fundamental of all ethics rules, requires that a lawyer act competently in representing a client. Competence requires "thoroughness and preparation reasonably necessary for the representation," and this encompasses all aspects of client representation including jury selection. Comment [8] to the rule states that a lawyer "should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Given the availability of information about prospective jurors on the Internet, does a lawyer have an affirmative duty to investigate jurors using the Internet? If a lawyer does use the Internet to investigate jurors, is the duty of competency implicated in how the lawyer conducts the investigation?

The standing committee states that it "does not take a position on whether the standard of care for competent lawyer performance requires using Internet research." (ABA Formal Op. 466, at 2 n.3.) The New York City Bar Association Committee on Professional Ethics, Formal Op. 2012-02, states that "standards of competence and diligence may require doing everything reasonably possible to learn about the jurors who will sit in judgment on a case," including using the Internet. New Hampshire Bar Association Ethics Committee, Op. 2012-13/05, found that lawyers have "a general duty to be aware of social media as a source of potentially useful information in litigation, to be competent to obtain that information directly or through an agent, and to know how to make effective use of that information in litigation," and may view a witness's unrestricted Facebook page or Twitter feed. Although the New Hampshire opinion addressed using the Internet to research witnesses, it appears equally applicable to researching jurors.
There may also be court rules or case law requiring lawyers to research some aspects of prospective jurors' backgrounds available on the Internet. In Missouri, Supreme Court Rule 69.025 requires a lawyer to make a reasonable investigation into potential jurors' backgrounds before asking about their litigation history in \textit{voir dire}. Missouri Supreme Court Rule 69.025(b) defines "reasonable investigation" as reviewing online court records through the court's Case.net system, which contains Missouri civil and criminal court records. A year before the court adopted this rule, it stated in Johnson v. McCullough, 306 S.W.3d 551, 558-59 (Mo. 2010), that "in light of advances in technology allowing greater access to information that can inform a trial court about the past litigation history of venire members, it is appropriate to place a greater burden on the parties to bring such matters to the court's attention at an earlier stage." The court also stated that "[l]itigants should endeavor to prevent retrials by completing an early investigation." (\textit{Id.} at 559.) In Missouri, failure to research litigation records online before the jury is impaneled will likely foreclose seeking a new trial or appealing a verdict on the basis of juror nondisclosure of prior litigation history.

In terms of the level of competency required in using the Internet to research jurors, the ABA opinion states that lawyers should be aware of automatic, subscriber-notification features on some ESM networks, and that lawyers should periodically review terms and conditions, including privacy features, when using ESM networks. As we will discuss later in this column, failing to disable a subscriber-notification feature could result in a prospective juror being notified that a lawyer has viewed the juror's online information, which bar disciplinary authorities may view as unauthorized communication with a juror. Fully understanding how social media operates is necessary to use it competently in researching jurors.

\textbf{Review of Juror's Website or ESM}

Several state and local advisory ethics opinions state that review of a juror's website or ESM is permissible under the state's version of Model Rule 3.5(b). For example, Kentucky Bar Association, Op. E-434 (2012), states: "If the site is 'public,' and accessible to all, then there does not appear to be any ethical issue." New York City Bar Association Committee on Professional Ethics, Formal Op. 2012-2, similarly holds that a lawyer may use websites or ESM to research potential jurors, and New York County Lawyers' Association Committee on Professional Ethics, Formal Op. 743 (2011), states that a lawyer may search juror's "publicly available" webpages and ESM. (\textit{See also} Or. State Bar Ass'n, Formal Op. 2013-189 ("Lawyer may access publicly available information [about a juror, witness, or opposing party] on social networking website.").

The ABA opinion follows the lead of state and local bar associations and states that review of a juror's website or ESM is permissible under Model Rule 3.5(b). The standing committee explains that a review is one that does not involve the lawyer making an access request to the juror, analogizing it to a lawyer, or someone acting on behalf of a lawyer, driving down a prospective juror's street and observing publicly available information about where the prospective juror lives. The opinion reasons that "[t]he mere act of observing that which is open to the public would not constitute a communicative act that violates Rule 3.5(b)." (ABA Formal Op. 466, at 4.)

In reaching its conclusion that a review of a juror's website or ESM is permissible, the standing committee cites to several of the state and local ethics opinions reaching this
same conclusion. The standing committee does not cite any authority prohibiting review of a juror’s website or ESM, and we were unable to locate any such authority.

**Access Requests to Jurors**

While review of a juror’s online presence is permissible, the state and local ethics opinions that address the issue of sending an access-to-information request to prospective jurors uniformly disapprove of access requests as impermissible communications with jurors. For example, New York County Lawyers’ Association Committee on Professional Ethics, Formal Op. 743 (2011) states, "[s]ignificant ethical concerns would be raised by sending a 'friend request,' attempting to connect via LinkedIn.com, signing up for an RSS feed for a juror's blog or 'following' a juror's Twitter account." (See also N.Y.C. Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2012-2 (stating that a lawyer may not chat, message, or send a "friend request" to a juror); Or. State Bar Ass'n, Formal Op. 2013-189 (stating that "a lawyer may not send a request to a juror to access non-public personal information on a social networking website, nor may a lawyer ask an agent to do so").

The ABA opinion reaches the same conclusion and states that "a lawyer may not personally, or through another, send an access request to a juror." (ABA Formal Op. 466, at 4.) Sending an access request would be a communication with a juror or prospective juror prohibited by Model Rule 3.5(b). The standing committee analogizes this to a lawyer, or someone working for a lawyer, "driving down the juror's street, stopping the car, getting out, and asking the juror for permission to look inside the juror's house because the lawyer cannot see enough when just driving past." (Id.)

Not all information posted on a juror website or ESM may be available to the public for passive review. Because of this, the temptation exists for a lawyer, or someone working for the lawyer, to send an access request to the juror to obtain a more thorough understanding of the person's likes, dislikes, interests, activities, and other aspects of the juror’s personal history on webpages not open to the general public.

**Review Triggering Notification to Juror**

Some social media networks, such as LinkedIn, automatically notify subscribers of the identity of someone who has reviewed their profiles. State and local advisory opinions differ on whether such notifications triggered by a lawyer's review of a juror would constitute a prohibited communication with a juror.

New York City Bar Association Committee on Professional Ethics, Formal Op. 2012-02, found that such network-generated notices to jurors would be a communication from the lawyer to a juror because the lawyer's view of the juror's online information would trigger the notice and involve "the process of bringing an idea, information or knowledge to another's perception – including the fact that they have been researched." The committee found that the network-generated notice would be a prohibited communication if the lawyer was aware that simply viewing the juror's online information would trigger the notice, but the committee took "no position on whether an inadvertent communication would be a violation of the Rules."

New York County Lawyers’ Association Committee on Professional Ethics, Formal Op. 743 (2011), also found that such network-generated notices were a communication. The
committee further found, "If a juror becomes aware of an attorney's efforts to see the juror's profiles on websites, the contact may well consist of an impermissible communication, as it might tend to influence the juror's conduct with respect to the trial."

The New York State Bar Association Social Media Ethics Guidelines, available at http://tinyurl.com/jwruf8v, cautions lawyers that even an automatic notice sent by social media networks "may be considered a technical ethical violation." It explains that to avoid such a notice generated by LinkedIn when viewing a juror's public profile, the lawyer must change the lawyer's LinkedIn settings to be anonymous or be completely logged out of the lawyer's LinkedIn account.

Departing from these opinions, the ABA Standing Committee finds that automatic notices are not prohibited communication with a juror under Model Rule 3.5. In reaching this conclusion, the standing committee reasons that it is the ESM service communicating with the juror and not the lawyer. Referring to the drive-by car analogy, the standing committee says it would be "akin to a neighbor's recognizing a lawyer's car driving down the juror's street and telling the juror that the lawyer had been seen driving down the street." (ABA Formal Op. 466, at 5.)

**Discovery of Juror Misconduct**

The standing committee also discusses the ethical obligations of a lawyer who discovers juror misconduct via social media, though that is not the focus of the opinion. It states that Model Rule 3.3 requires a lawyer who represents a client in an adjudicative proceeding to take remedial measures, including informing the tribunal, if the lawyer learns that a juror has engaged in criminal or fraudulent conduct related to the proceeding. The standing committee observes that not all improper conduct will be either criminal or fraudulent, and therefore some improper conduct may not trigger the reporting obligation under Model Rule 3.3.

While the reporting duty under Model Rule 3.3 may not cover all juror misconduct, the standing committee cites a case, U.S. v. Juror Number One, 866 F.Supp.2d 442 (E.D. Pa. 2011), in which a juror was found guilty of criminal contempt for failing to follow jury instructions and e-mailing other jurors. Thus, a lawyer learning of a juror failing to follow a jury instruction not to communicate about a case, including communicating electronically via the Internet, may be required to report this conduct if not following the jury instructions could be grounds for criminal contempt in the jurisdiction. In addition, the standing committee notes that the ethics rules in some jurisdictions may require the reporting of *all improper conduct* by a venire person or juror. (See, e.g., N.Y. Rules of Prof'l Conduct R. 3.5(d) (2013) (stating that "[a] lawyer shall reveal promptly to the court improper conduct by a member of the venire or a juror").)

**Conclusion**

The ABA Standing Committee in Formal Opinion 466 provides much-needed guidance concerning the ethical use of the Internet and social media to investigate jurors and prospective jurors. The opinion follows a growing trend among state ethics committees and some courts addressing the issue of lawyers researching jurors online. While the ABA's ethics opinion seeks to clarify the intersection of ethics and technology, its position concerning automatic notifications to juror-subscribers of services such as LinkedIn is not the position taken in every jurisdiction. This conflict serves as a reminder
of the importance for lawyers to be aware of the rules, court orders, case authority, and advisory ethics opinions in the jurisdictions in which they practice.