The Use of Cloud Computing, Mobile Devices and Social Media in the Practice of Law (December 9, 2016)

Pamela A. Bresnahan
*Vorys, Sater, Seymour and Pease LLP*

Lucian T. Pera
*Adams and Reese LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.
New technologies have the potential to help lawyers practice smarter and more efficiently. However, such technology also contains risks for lawyers. Lawyers should be aware of those risks in order to avoid violating their ethical obligations. Lawyers should understand the implications that use of a particular technology will have on their obligations and utilize appropriate measures to comply with such obligations. This article addresses the implications of a lawyer’s use of cloud computing, mobile devices and social media, as well as a lawyer’s counseling of clients regarding their use of social media. The rules governing attorney conduct in the relevant jurisdiction should always be consulted when analyzing the use of these and other technologies.

I. OPERATING IN THE CLOUD AND MANAGING ETHICAL RISKS

Technological advancements have led to the increased accessibility of information. In certain respects, information can be accessed from almost anywhere at any time, because of the prevalence of smartphones, other mobile devices and increased connectivity to the internet. Such advances provide increased opportunities for lawyers and law firms to access information related to their practices, while away from the office, through the use of “cloud computing.” Cloud computing has been described as a “sophisticated form of remote electronic data storage on the internet. Unlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored ‘in the cloud’ is kept on large servers located elsewhere and maintained by a vendor.”

Advantages that may be utilized from cloud computing include increased access to client data by a lawyer or law firm and increased access by clients to their own files over the internet. Cloud computing can also help protect against loss of data by duplicating information on several servers and performing regular backups.

However, lawyers and law firms that utilize cloud computing should be aware of certain ethical concerns that may arise from its use. The main concern is the confidentiality of the data being stored in the cloud. When operating in the cloud, client confidences and secrets are not under the

2. Id.
direct control of the lawyer or law firm and, thus, there is the potential for a third party to gain access to confidential client information. Rule 1.6 of the ABA Model Rules of Professional Conduct provides that “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [certain exceptions].” If proper protocols are not put in place, a lawyer or law firm risks violating Rule 1.6 or its state analogs, when using the cloud to store confidential information.

Following reforms to the ABA Model Rules, a new subpart to Rule 1.6 reads “[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” Revised comments [18] and [19] provide guidance regarding how to measure the reasonableness of efforts taken to prevent inadvertent disclosure or unauthorized access. Comment [18] states that:

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 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].

---

5. ABA Model Rules of Prof'l Conduct R. 1.6(a) (2013).
6. ABA Model Rules of Prof'l Conduct R. 1.6(c) (2013).
Comment [19] reads:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.8

The language of these comments forms “the core set of principles used throughout virtually all ethics opinions in American jurisdictions that address confidentiality concerns in the cybersecurity context.”9

While there is the potential for unauthorized access to information a lawyer is required to keep confidential pursuant to Rule 1.6 or a state analog, ethics opinions addressing the use of cloud computing have nevertheless generally approved of the practice, subject to there being appropriate precautions put in place.10 For example, the Nevada and Alabama State Bars have each issued ethics opinions calling for a standard of reasonable care. The Nevada State Bar has stated that an “attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney’s direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services” and “if the third party can be reasonably relied upon to maintain the confidentiality and agrees to do

so, then the transmission is permitted by the rules even without client consent.”\textsuperscript{11} The Alabama Disciplinary Commission agreed, concluding that “a lawyer may use ‘cloud computing’ or third-party providers to store client data provided that the attorney exercises reasonable care in doing so.”\textsuperscript{12} Such a duty requires that a lawyer be knowledgeable about how the data will be stored by the provider, about the security measures that will be put in place and to ensure that the provider will abide by a confidentiality agreement in its handling of data.\textsuperscript{13} The Arizona State Bar has also weighed in, saying that lawyers “should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.”\textsuperscript{14} It is also important that a lawyer “know how data can be retrieved if the cloud computing provider goes out of business or if the cloud computing services are interrupted.”\textsuperscript{15} The Iowa State Bar has also concluded that a lawyer “must ensure that there is unfettered access to the data when it is needed” and “must be able to determine the nature and degree of protection that will be afforded the data while residing elsewhere.”\textsuperscript{16} With respect to selecting a provider, the Board of Professional Responsibility of the Supreme Court of Tennessee recently noted that the “primary obligation is to select a reliable provider under the circumstances. In making this selection, the lawyer should consider the provider’s ability to protect the information, to limit authorized access only to necessary personnel and to ensure that the information is backed up, is reasonably available to the lawyer and is reasonably safe from unauthorized intrusion.”\textsuperscript{17}

Generally, exercising the proper level of care will require that the lawyer examine a cloud computing vendor’s terms of service to evaluate whether client information will be adequately protected.\textsuperscript{18} If a lawyer is not competent to determine whether there are reasonable measures in place to protect client confidentiality through the use of a particular technology,

\begin{itemize}
\item \textsuperscript{12} Alabama State Bar, Ethics Op. 2010-02 (2010).
\item \textsuperscript{13} Id.
\item \textsuperscript{14} State Bar of Arizona, Ethics Op. 09-04 (2009).
\item \textsuperscript{15} Geraghty, Pera & Saikali, \textit{supra} note 9, at 78 (citing Washington State Bar Ass’n, Op. No. 2215 (2012)).
\item \textsuperscript{16} Iowa State Bar Ass’n, Committee on Ethics and Practice Guidelines, Ethics Op. 11-01 (2011).
\item \textsuperscript{17} Bd. of Prof’l Responsibility of the Supreme Court of Tenn., Formal Ethics Op. 2015-F-159 (2015).
\item \textsuperscript{18} See Virginia State Bar, Legal Ethics Op. 1872 (2013).
\end{itemize}
“the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer.”\textsuperscript{19} However, as commentators discussing Alaska Ethics Opinion 2014-3 have noted, “a lawyer’s decision to delegate to an IT professional the tasks relating to cloud computing is another form of outsourcing governed by [Alaska Rule of Professional Conduct 5.3].”\textsuperscript{20} “Accordingly, the lawyer must make reasonable efforts to ensure that the IT professional’s conduct in overseeing these cloud computing issues is compatible with the lawyer’s professional obligations.”\textsuperscript{21} Thus, delegation to an IT professional does not relieve a lawyer from his or her obligation to ensure that client confidentiality is adequately protected.

In 2013, the Maine Board of Overseers of the Bar provided a list of actions a lawyer should take with respect to the use of a cloud computing vendor, to be in accordance with the Maine Rules of Professional Conduct. The Board stated that a lawyer should ensure that a vendor: (1) explicitly agrees that it has no ownership or security interest in the data; (2) has an enforceable obligation to preserve security; (3) will 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 produces the requested information; (4) has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing; (5) provides the firm with the right to audit the provider’s security procedures and to obtain copies of any security audits performed; (6) will host the firm’s data only within a specified geographic area; and, (7) provides the ability for the law firm, on demand, to get data from the vendor’s or third-party data hosting company’s servers for the firm’s own use or for in-house backup.\textsuperscript{22}

The State Bar of California Standing Committee on Professional Responsibility and Conduct has also provided a list of factors an attorney should consider, prior to utilizing a new technology. Those factors include: (1) the attorney’s ability to assess the level of security afforded by the technology; (2) the legal ramifications of third-parties intercepting, accessing or exceeding authorized use; (3) the sensitivity of the particular information; (4) the impact to the client of an inadvertent disclosure; (5) the urgency of the situation; and, (6) client instructions and circumstances.\textsuperscript{23}

\textsuperscript{19} Geraghty, Pera & Saikali, supra note 9, at 66.
\textsuperscript{21} Id.
Even where a lawyer otherwise uses cloud computing in accordance with appropriate security measures, the Massachusetts Bar Association has opined that a lawyer “remains bound . . . to follow an express instruction from his or her client that the client’s confidential information not be stored or transmitted by means of the Internet, and all lawyers should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first obtaining the client’s express consent to do so.”24 Therefore, a different storage method should be utilized for any client who objects to having his or her confidential information stored via the cloud. Additionally, a prudent lawyer should likely not rely exclusively on the cloud for storage of client information and should continue to maintain other storage systems as well, particularly when dealing with information that is extremely sensitive.

It is important that a lawyer be mindful of the standards set by their local jurisdiction, in connection with their use of cloud computing and protection of confidential information. Indeed, the increasing risk to client confidentiality posed by cloud computing has caused some to suggest that “it be mandatory for every lawyer to take a biennial CLE on recent metadata and cloud-computing advancements.”25 Perhaps a harbinger of things to come, Florida recently became the first state to require continuing legal education in technology. On September 29, 2016, the Supreme Court of Florida adopted an amendment to the Rules Regulating the Florida Bar to require that three (3) out of thirty-three (33) hours of CLE over a three (3) year period be in an approved technology program.26 While there is currently no such general technology CLE requirement outside of Florida, lawyers should nonetheless be vigilant that they understand and are in compliance with their relevant rules of professional conduct when utilizing cloud computing.

II. USING MOBILE DEVICES

As with the use of cloud computing, a lawyer must guard against disclosure of confidential information and violations of other ethical duties through the

use of mobile devices in his or her practice. Ethics opinions have provided guidance in this area as well.

The Florida Bar has concluded that “[i]f a lawyer chooses to use [sic] Devices that contain Storage Media, the lawyer has a duty to keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality.”27 In 2010, the Ethics 20/20 Commission’s Working Group on the Implications for New Technologies suggested certain precautions that a lawyer should take when utilizing portable devices. These precautions include:

1. Providing adequate physical protection or having methods for deleting data remotely in the event of a lost or stolen device;
2. Encouraging the use of strong passwords;
3. Purging data from a device before it is replaced with a new device;
4. Installing safeguards to combat viruses, malware and spyware;
5. Erecting firewalls;
6. Ensuring data is backed up frequently;
7. Updating operating systems to ensure the latest security protections are installed;
8. Configuring software and network settings to minimize risk;
9. Encrypting sensitive information;
10. Identifying and, when appropriate, eliminating metadata from electronic documents before sending them; and,
11. Avoiding public Wi-Fi hotspots when transmitting confidential information.28

In 2010, the State Bar of California Standing Committee on Professional Responsibility and Conduct examined a hypothetical fact pattern to determine if an attorney would violate the duties of confidentiality and competence by conducting legal research and e-mailing a client using a laptop connected to a public wireless internet connection at a coffee shop and from the attorney’s home, while connected to the attorney’s personal wireless system. The committee concluded that use of the public wireless system at the coffee shop risked violating both the duties of confidentiality

28. Geraghty, Pera & Saikali, supra note 9, at 72.
and competence because of the lack of security features provided in most public wireless systems, unless the attorney took appropriate precautions.\textsuperscript{29} Such precautions might include “using a combination of file encryption, encryption of wireless transmissions and a personal firewall.”\textsuperscript{30} However, if the situation involved a matter of particular sensitivity, an attorney “may need to avoid using the public wireless connection entirely or notify [the client] of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.”\textsuperscript{31} On the other hand, the committee believed that an attorney’s use of a personal wireless connection at home would not constitute a violation of the duties of confidentiality and competence, so long as appropriate security features have been configured on the system.\textsuperscript{32} This hypothetical fact pattern and analysis provides a good rule of thumb regarding the precautions that should be taken when utilizing mobile devices to conduct client business.

Lawyers must not only take appropriate precautions to protect confidential information, in light of their professional obligations, while using a mobile device, but also must take appropriate precautions when disposing of a device that has previously been used and that may contain confidential or other client information. When disposing of an electronic device, a lawyer “should ensure that confidential information has been removed.”\textsuperscript{33} The failure to protect against disclosure of confidential information to a subsequent user of a device could result in a violation of Rule 1.6.\textsuperscript{34} The Florida Bar has stated that, if a vendor is involved in the sanitization of a device upon disposal, it is not sufficient to merely obtain an agreement from the vendor that the device will be sanitized.\textsuperscript{35} Rather, the lawyer has “an affirmative obligation to ascertain that the sanitization has been accomplished, whether by some type of meaningful confirmation, by having the sanitization occur at the lawyer’s office, or by other similar means.”\textsuperscript{36}

\textsuperscript{30} Id.
\textsuperscript{31} Id.
\textsuperscript{32} Id.
\textsuperscript{33} Geraghty, Pera & Saikali, supra note 9, at 72 (citing Alabama State Bar, Ethics Op. 2010-02 (2010)).
\textsuperscript{34} Alabama State Bar, Ethics Op. 2010-02 (2010).
\textsuperscript{35} The Florida Bar, Ethics Op. 10-2 (2010).
\textsuperscript{36} Id.
III. SOCIAL MEDIA

A. Lawyers Using Social Media

A lawyer utilizing social media should exercise due care to comply with his or her ethical and professional obligations. The nature of social media, and the ubiquity of its use in modern society, increases the potential for a lawyer to inadvertently violate a rule of professional conduct, should proper diligence not be exercised. A non-exhaustive list of potential pitfalls of a lawyer utilizing social media includes: (1) disclosure of confidential or privileged information; (2) communicating with represented parties; (3) inadvertent creation of attorney-client relationships; and, (4) violations of rules regarding legal advertising and/or solicitation of clients.37 A resource that can help a lawyer deal with ethical concerns involving the use of social media is the Social Media Ethics Guidelines issued by the New York State Bar Association, which seeks to provide guidance on what is ethically permitted when using social media.38 West Virginia also recently published a legal ethics opinion that discusses a variety of ethical issues surrounding the use of social media.39

Care must be exercised not to reveal any confidential or privileged information when posting to social media. For example, an attorney who published a public blog containing “confidential information about her clients and derogatory comments about judges”40 received 60-day suspensions in both Illinois and Wisconsin as a result of such conduct.41 A lawyer must also be extremely careful when deciding whether and how to respond to a negative review on social media, keeping in mind that the duty of confidentiality survives termination of an attorney-client relationship. For example, the Supreme Court of Georgia rejected an attorney’s petition for a mild form of voluntary discipline where the attorney had posted personal and confidential information about a

40. In re Peshek, 798 N.W.2d 879, 879 (Wis. 2011) (per curiam).
41. See id.
former client in response to negative reviews that the client had posted on consumer websites.42

Bar Associations have also generally rejected the notion that the self-defense exception to Rule 1.6 is applicable in the context of a lawyer responding a negative review on social media.43 In that regard, the Commercial and Federal Litigation Section of the New York State Bar Association issued a guideline that states that the prohibition against disclosure of confidential information “applies, even if the lawyer is attempting to respond to unflattering comments posted by the client.”44 To aid lawyers who wish to respond to an unflattering post, the Pennsylvania Bar Association has proposed the following suggested response: “A lawyer’s duty to keep client confidences has few exceptions and in an abundance of caution I do not feel at liberty to respond in a point-by-point fashion in this forum. Suffice it to say that I do not believe that the post presents a fair and accurate picture of the events.”45

While lawyers must avoid revealing confidential or privileged information when posting information on social media, it may be permissible in certain jurisdictions for a lawyer to reveal information that has become a matter of public record. For example, the Supreme Court of Virginia held in 2013 that “[t]o the extent that the information is aired in a public forum, privacy considerations must yield to First Amendment protections. In that respect, a lawyer is no more prohibited than any other citizen from reporting what transpired in the courtroom.”46 In Hunter, the Virginia State Bar instituted disciplinary proceedings against an attorney who authored a blog and argued that the attorney violated Rule 1.6 by revealing information “that could embarrass or likely be detrimental to his former clients by discussing their cases on his blog without their consent.”47 However, the Supreme Court of Virginia agreed with the attorney’s contention that the Virginia State Bar’s interpretation of Rule 1.6 was unconstitutional because the matters discussed in the blog had already been revealed in public judicial proceedings and were protected by the First Amendment.48 Therefore, the

42. See In re Skinner, 740 S.E.2d 171, 172 (Ga. 2013) (per curiam).
47. Id. at 492.
48. Id. at 502.
Court concluded that the state could not prohibit [through Rule 1.6] an attorney from discussing information about a client or former client that was not protected by the attorney-client privilege. However, other jurisdictions may not allow the revelation of information relating to the representation of a client simply because the information at issue has already been made public. The Supreme Court of Colorado recently imposed a six month suspension on an attorney, with the requirement that the attorney petition for reinstatement, where the attorney had posted online responses to two negative reviews posted on Google+. The attorney “revealed substantial information relating to the representations of . . . two clients, without authorization and without permission, in violation of Colo. RPC 1.6(a).” The Presiding Disciplinary Judge determined it was “irrelevant . . . whether this information was already public: comment three to Colo. RPC 1.6(a) states that the rule ‘applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source.’” Therefore, attorneys should be mindful of their local jurisdiction’s treatment of information that is a matter of public record before posting any such information on social media or elsewhere.

However, where Rule 1.6 or an appropriate analog is applicable, simply avoiding the explicit typing and posting of confidential information may not be enough in certain circumstances. Vigilance must be maintained to avoid inadvertent disclosures that may occur via social media, as a result of the use of certain technology or devices. For instance, geo-tagging a social media post or photograph may reveal the lawyer’s geographic location when travelling on confidential business, which could lead to a rule violation.

Use of social media also creates the potential for a lawyer to communicate with a represented party, which is forbidden by ABA Model Rule 4.2 in circumstances where the represented person’s lawyer has not given consent to the communication. The prior consent provision of state analogs of Rule 4.2, often referred to as the “no contact rule,” has been strictly interpreted. For example, the North Carolina State Bar and New York City Bar have each interpreted the rule to prohibit a

49. Id.
51. Id. at *8.
52. Id.
53. Harvey, McCoy & Sneath, supra note 37.
lawyer from using the “reply all” feature when responding to an e-mail from an opposing attorney who has copied his or her client on the original e-mail, unless there is express or implied consent to do so based on the circumstances.55 In the social media context, the sending of a Facebook friend request, LinkedIn invitation or other similar communication could be an improper communication when used in an attempt to gain access to a represented party’s private social media content.56 However, a lawyer may generally view social media content that is not shielded by privacy settings and open to public viewing.57 In addition to the caution lawyers should exercise in their communications on social media, the D.C. Bar recently urged lawyers to exercise caution when a social media site requests permission to access the lawyer’s e-mail contacts or to send e-mails to individuals in the lawyer’s address book.58 Providing social media sites with such permissions “could potentially identify clients or divulge other information that a lawyer is obligated to protect from disclosure.”59

Attorney-client relationships may also inadvertently be created through use of social media if an attorney is not careful. Such relationships may be formed, in certain circumstances, when a lawyer responds to comments on a blog post or legal questions posted on a message board or similar communication.60 Therefore, appropriate disclaimers should be utilized in connection with one’s social media activity, especially when responding to a prospective client’s request for information or advice.61 Otherwise an attorney risks committing an ethical breach, or even legal malpractice, in a situation where the attorney is not consciously aware that he or she is even in an attorney-client relationship. However, one may generally write about legal topics in general, without creating an attorney-client relationship, so long as individual legal advice is not being communicated.62

56. Harvey, McCoy & Sneath, supra note 37.
57. Id.
59. Id.
60. Harvey, McCoy & Sneath, supra note 37.
61. Id.
With respect to legal advertising via social media, a lawyer should be diligent to assure that any ads posted comply with the rules regarding attorney advertising in the appropriate jurisdiction.\(^{63}\) The State Bar of California Standing Committee on Professional Responsibility and Conduct made clear in 2012 that material posted by an attorney on social media must comply with the rules governing attorney advertising in the state, so long as the material posted satisfies the criteria used to constitute a “communication” within the meaning of the rules.\(^{64}\) Therefore, attorneys must be mindful of the local rules governing advertising before posting messages. For example, use of “puffery” and false statements of material fact or law should be avoided.\(^{65}\) Additionally, some states prohibit the use of words such as “specialist,” “certified” or “expert” without possessing appropriate qualifications.\(^{66}\) Particular attention must be paid to social networking sites that invite lawyers to identify “specialties” or areas of expertise in their profiles, such as Avvo and LinkedIn.\(^{67}\) Otherwise, an attorney risks committing an inadvertent violation of the rules governing attorney advertising.

Attorneys should be mindful of these and other rules of professional conduct that may be implicated through their use of social media. Therefore, it is recommended that attorneys consult their local rules of professional conduct and ethics opinions and judicial opinions interpreting those rules, prior to engaging in the use of social media.

**B. Lawyers Advising Clients About Their Use of Social Media**

In certain scenarios, information and photographs posted on social media can have a great effect upon a client’s case. Therefore, lawyers should be aware of the ethical implications of providing advice regarding their clients’ social media use. Important to consider is whether a lawyer may advise a client about what to post or not post on social media and whether the lawyer may advise a client to remove an existing post from a social media account.

---

65. Id. at 159; see also ABA Model Rules of Prof’l Conduct R. 4.1 (2013).
66. See, e.g., Ill. Rules of Prof’l Conduct R. 7.4(c); N.Y. Rules of Prof’l Conduct R. 7.4(a).
In certain cases, competent representation includes providing advice to a client regarding the legal ramifications of social media postings, including existing and future postings, if the postings could be relevant to the legal matter.68 Put another way, “an attorney may properly review a client’s social media pages, and advise the client that certain materials posted on a social media page may be used against the client for impeachment or similar purposes.”69 Both the Florida Bar and New York County Lawyers Associations have also concluded that a lawyer may ethically advise a client to use the highest level of privacy settings on the client’s social media accounts.70 Use of such settings will typically prevent adverse counsel from obtaining direct access to the social media page without requesting access through formal discovery.71

Ethics opinions addressing whether a lawyer may counsel a client to remove an existing social media post that may be at issue in a legal matter point to the law of spoliation of evidence as the relevant inquiry. A lawyer may not counsel a client to engage in conduct that the lawyer knows is criminal or fraudulent or to unlawfully obstruct another party’s access to evidence.72 Therefore, a lawyer should not advise a client to remove an existing social media post, if doing so would constitute spoliation of evidence in the relevant jurisdiction.73 Additionally, a lawyer may not advise a client to post information on social media that is false or misleading.74 However, according to the Florida Bar, if there would be no violation of the rules governing spoliation or preservation of evidence, a lawyer may advise a client to “remove information relevant to the foreseeable proceeding from social media as long as the social media information or data is preserved.”75 Thus, a lawyer should be aware that, even when permissibly counseling a client to remove certain information from social media, he or she must also “take appropriate action to preserve the information in the event it should prove to be relevant and discoverable.”76

72. See ABA Model Rules of Prof’l Conduct R. 1.2(d), 3.4(a) (2013).
IV. CONCLUSION

Modern technology, in many respects, has changed the manner in which attorneys practice law. New technologies allow for increased access to information and increased efficiency. However, use of technologies such as cloud computing, mobile devices and social media contain inherent risks, especially with regard to the duties one has to protect their clients’ confidential information. Therefore, it is important for attorneys to understand the ethical concerns that must be addressed through their use of such technologies (and future technologies) in connection with the practice of law. Proper care and precautions should always be utilized to ensure compliance with one’s appropriate ethical and legal concerns and the relevant rules governing attorney conduct should be reviewed prior to one’s use of a new technology. Below are fifteen hypothetical scenarios that demonstrate some of the ethical concerns addressed above.
Hypothetical 1 – Calming Nelly

You have a partner who can a bit of a “nervous Nelly.” He worries about nearly everything and, because you have a late-model iPhone and an iPad, he frequently asks you what sometimes seem to be frivolous questions. He must have just read some marketing piece from an electronic security firm, because he comes into your office in a panic with several questions.

May a lawyer ethically communicate with a client using...
  A cordless home phone?
  A cell phone?
  Texting on a cell phone?
  Exchanging Facebook messages?
  Unencrypted email?
  Gmail or other online email services?

Hypothetical 2 – Clouds on the Horizon

When your partner tells you it’s time to replace the network server where your office keeps email and documents, she also tells you that the law firm down the hall just replaced their server and stores all their information “in the cloud.” And, she says, they say they have saved a lot of money doing so.

May you store confidential client communications in the “cloud”?

Hypothetical 3 – The Good Son

You represent an elderly couple in a lawsuit. You regularly communicate with them by email, sending them copies of correspondence with opposing counsel, pleadings, and the like. A few months into your representation you learn that they routinely ask their son to help them by printing off your emails to them.

Is there any advice you should give the couple about this?

Hypothetical 4 – Advising the Restless Employee

You represent a licensed securities broker employed by a big brokerage. She is considering her options for staying with the firm or moving to another firm and wants your advice on her legal rights and obligations.

Shortly after your first meeting, in your law office, she emails you from her company email address.
Is there any advice you should give the broker about this?

Hypothetical 5 – Reply to All

You have been representing a company for about 18 months in an effort to negotiate the purchase of a patent from a wealthy individual inventor.

The negotiations have been very cordial at times, but occasionally turn fairly contentious. You and your company’s vice president have met several times with the inventor and his lawyer, both at the inventor’s home and in a conference room in your client company’s headquarters. After some of the fruitful meetings, you and the other lawyer have exchanged draft purchase agreements, with both of you copying your clients – the vice president and the inventor.

Last week things turned less friendly, and you heard that the inventor’s lawyer might be standing in the way of finalizing a purchase agreement. This morning you received a fairly chilly email from that lawyer, rejecting your latest draft purchase agreement and essentially threatening to “start all over again” in the negotiations given what he says are your client’s unreasonable demands. As in earlier emails, the other lawyer copied the email to his client, the inventor.

May you respond to the other lawyer’s email using the “Reply to All” function, and defending your client’s positions in the negotiations?

Hypothetical 6 – Stolen Laptop

Late one evening, you get a frantic phone call from your associate. She says she stopped off for dinner with her husband on the way home from work and that, on leaving the restaurant, she found her car window smashed and her briefcase stolen. And her firm-issued laptop that had been inside was gone, too.

What do you do?

Hypothetical 7 – The Departed

A little more than two weeks ago, the bright young associate you raised from a pup gave her two-week notice. Her last day was last Tuesday. Her departure was reasonably cordial.

This morning, your office manager tells you there’s a problem.

The departed associate had a personal laptop and smartphone she used for work. They were configured, with your office’s help, to access her office email and other office systems remotely. And she never got
around to honoring the office manager’s request to bring the laptop and phone in so that your tech guy could remove firm email and other files from them. Your office manager says her access to email firm systems is cut off, but he’s convinced that the departed associate still has firm data on her devices.

Do you have an ethics problem?

Hypothetical 8 – Road Warrior

One of the lawyers in your office lives on the road.
For that reason, she also lives on her laptop.
When you have traveled with her, you have noticed that she always tries to find a place in a courthouse, coffee shop, hotel lobby, hotel room, or airport that has free wi-fi, to do her work. Occasionally, she even pays a few bucks for a wi-fi connection.

Is the firm’s and its clients’ information safe in her hands?

Hypothetical 9 – Cheapo Neighbors

About six months ago, your paralegal convinced you to buy and install a wi-fi hotspot in your office, saying it was cheap, and would let you and others in your office connect to firm systems with your tablets and laptops without using internet cables. And, your paralegal said, clients could use it in the lobby while they waited for appointments.

Suddenly, within the last few weeks, you can never log on to the wi-fi. After investigating, your office manager tells you he thinks may be folks outside the office are using it and hogging capacity. After all, he says, there’s no password on the wi-fi and the signal can be reached by the lawyers to whom you lease the second floor and customers in the Subway sandwich shop across the driveway.

Do you have a problem?

Hypothetical 10 - Handshake

You are the firm’s managing partner.
After interviewing three separate technology companies, you settle on one to replace your former consultant, whose prices just got too high.
As you are concluding your call to the company you decided to hire, you casually mention to the owner, “Well, send me over your standard contract, with the terms and prices we discussed, and we’ll look it over.” The company owner is quiet for a moment and says, “Well,
we have usually just done business on a handshake. Is that OK? We certainly trust you.”

*Do you need a written agreement? If so, what should it say?*

**Hypothetical 11 – What, Me Worry?**

One day, as you are having lunch with two other lawyers from your office, one brings up a report he read about a big law firm whose computers were hacked. Then one of the lawyers says, “Well, thank goodness we don’t have any of those big international clients. Who’d want to hack us?”

*What should you do to protect your office?*

**Hypothetical 12 – Going Paper-Less**

Last month, you hired a new paralegal, replacing your former longtime paralegal.

One morning, your new paralegal suggests that you really could be using your office’s case management software much more fully – for example, storing all documents and email about a matter there, and going paperless. “In fact,” she said, “at my old firm, we got rid of almost everything in our paper client files, kept it all nicely organized in the same program you have, and turned the file room into an office for another lawyer. Just give me the go-ahead and I’ll make it happen.”

*May you ethically do away with paper client files and go “paperless”?*

**Hypothetical 13 – File Storage Company**

Six months ago, you successfully closed a client’s acquisition of a piece of real property. All your post-deal clean-up work is done, all funds disbursed, and all fees and expenses paid.

You write the client a letter thanking her for calling on you, telling her the matter is over, and telling her that you’d be happy to provide her a copy of her client file if she would like, but that your normal document retention policy is to keep files for two years and then destroy them, and that this is your plan as to her file. The client never responds.

*Are you required to keep the file? If so, for how long?*
Hypothetical 14 – File Converter

Same facts as Hypothetical 13, but…

The client responds to your letter by asking for a copy of the file in electronic format, with everything in PDF files.

As you review your file materials, you see that there are some paper documents in the file, some handwritten notes, some drafts with handwritten markups by you and people in your office, email in Microsoft Outlook, a bunch of Word documents, and a few Excel spreadsheets.

_Are you required to honor the client’s request?_

Hypothetical 15 – Old Laptops

For several years, you have served on the board of a non-profit organization that helps disadvantaged high school students learn about the business world.

At a quarterly board meeting, you hear some discussion about the difficulty the group is having raising funds to buy more laptops for the students to use in their internships with local businesses.

Suddenly, you remember that, over the next few months, your office is upgrading its laptops and will have about five old ones it no longer needs. You mention this, and the organization’s staff director gets very excited, saying they might well be able to clean them up, do some inexpensive upgrades, and let the students use them.

_May you donate your old laptops to the organization?_