**SOCIAL MEDIA, ELECTRONIC COMMUNICATIONS &**

**INFORMATION STORAGE – DONE ETHICALLY**

**Leslie A.T. Haley, Haley Law PLC**

**I. ELECTRONIC COMMUNICATIONS GENERALLY**

Advances in technology have brought new methods of communication and information storage to the practice of law, including e-mail, mobile telephones, facsimile machines, digital document creation and storage, electronic bulletin boards, chatrooms, and listservs.

A lawyer's duties with respect to protecting the confidentiality of client information—whether under the ethics rules or the evidentiary attorney-client privilege—remain the same regardless of the method by which the information is communicated or stored. However, the unique features of electronic communication and storage require that special attention be paid to (1) the specific precautions necessary to protect client information; and (2) the possibility of triggering a duty of confidentiality by unintentionally forming a lawyer-client relationship—or, more likely, a lawyer-“prospective client” relationship.

When a lawyer sends, receives, or stores client information in electronic form, the lawyer's duty to protect that information from disclosure to unauthorized individuals is the same as it is for information communicated or kept in any other form. However, electronic information has features that affect both the means required to protect client information and the manner in which the duty is triggered in the first place.

Those features include:

1. ***Decreased control over the nature and amount of information received from others***, as well as a decreased ability to identify the sender prior to opening an e-mail. This creates the possibility that by merely opening an e-mail, the lawyer may create a lawyer-“prospective client” relationship with the sender (whose identity might have been previously unknown), triggering a number of professional obligations, including the duty of confidentiality.
2. ***Greater susceptibility to unauthorized access.*** Electronic communications may be more susceptible to interception by unauthorized or unknown persons than are other forms of communication. Creation and storage of client information in electronic form via outside service providers also heighten the risk of unauthorized disclosure.
3. ***The existence of metadata*** (embedded information about a document, such as when it was created, who has worked on it, and how it has been changed), which creates a greater risk of unknown or inadvertent disclosure. Many electronic documents contain metadata that is usually hidden from users' view and that may include protected information. Its invisibility creates a heightened risk that the information won't be removed before the electronic documents are turned over to others.
4. ***Increased opportunity for inadvertent disclosure of client information*** due to the greater ease of transmitting large amounts of information electronically.

An additional concern becomes the issue of the client’s use of their own e-mail, cellphone, social media sites and other electronic devices and resources. It quickly becomes the lawyer’s responsibility to advise and assist the client in managing those resources as well, since a compromise of client information by opposing party or counsel can be extremely detrimental to the client’s matter.

**II. E-MAILS**

Some older ethics opinions forbade use of cellular and cordless phones and unencrypted e-mail without client consent. However, more recent authorities condone the use of electronic communication, even without encryption, reasoning that the expectation of privacy is the same as for ordinary telephone use. In this regard, some opinions rely partly on the fact that the unauthorized interception of electronic communications is a federal crime under the Electronic Communication Privacy Act, 18 U.S.C. §§2511, 2701. As the ABA's Standing Committee on Ethics and Professional Responsibility reasoned in [ABA Formal Ethics Op. 99-413](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_ethics_opinion_99_413&vname=mopcref55) (1999):

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

So while security related to email usage with co-counsel or opposing counsel seems protected, what about email communications with your client. As Rule 1.6 states, the duty of protecting the client’s confidences belongs to the lawyer, therefore, it is prudent that when considering email communications with a client the lawyer considers several factors, such as:

1. Is the client’s email address personal or a business address?
2. Is the client’s email access on a personal computer or shared computer (meaning employer computer or household computer)?
3. Is the client’s access to that email secure (or have they shared their password with others)?

**A. E-Mail Cautions:**

1. Make sure you know who the intended recipients are and to whom copies should be sent.
2. The client’s file should be documented to show appropriate contact information on client at time of Intake.
3. Determination should be made at time of Intake of client’s matter as to whether e-mail communication is an appropriate form of communication based on the nature of the matter and information.
4. A system should be developed to insure that copies of e-mails are put into the file as documentation of matters communicated (an electronic file should be established to track all electronic communications).
5. “Reply” or “reply all”? Make sure you use e-mail responses appropriately. Just because opposing counsel copies his client on an e-mail communication to lawyer that does not give lawyer permission to cc: his response to opposing party as well. Think about this as you would a letter with a cc: at the bottom; lawyer would never cc: opposing party in his response even though opposing counsel copies his client on the letter. Same rules apply as per Rule 4.2. Lawyer cannot cc: his e-mail response to opposing party without opposing counsel’s permission or he will have violated Rule 4.2 regarding communications with person’s represented by counsel.
6. When appropriate, use an e-mail form that indicates the materials contained are attorney-client privileged and intended only for the party to whom they were directed. The note should further indicate that should someone other than the intended recipient receive the communication, the attorney’s office should be contacted immediately and the communication returned without having been read. (*See* Virginia LEO 1702 addressing this issue which adopted the conclusion reached in ABA Formal Opinion 92-368 (subsequently withdrawn by ABA Formal Opinion 05-437). Virginia LEO 1702 states that a lawyer who “receives materials that on their face appear to be subject to the attorney-client privilege or otherwise confidential, under circumstances where it is clear they were not intended for the receiving lawyer, should refrain from examining the materials, notify the sending lawyer and abide by the instructions of the lawyer who sent them.” (Note that Virginia has not adopted ABA Model Rule 4.4(b) which states: RESPECT FOR RIGHTS OF THIRD PERSONS:(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.)

**B. Client's Use of Employer's Computer**

Several cases have examined what happens when employees communicate with their personal attorneys via employer-provided networks or computers. The courts analyzed whether the employer clearly reserved the right to monitor employees' electronic communications, thus eliminating any reasonable expectation of confidentiality and vitiating any claim of privilege.

**III. CELL PHONES AND OTHER HANDHELD ELECTRONICS**

Cell phones are routinely used by all of us as a major form of communication. While our carriers tell us the security of using cell phones has dramatically increased and the likelihood on interception of calls or other information is unlikely there are still precautions that need to be in place regarding the practice of law and the use of cell phones. Cell phones have become so much more than just a routine device to place telephone calls and have 24 hour access to communications.

Additionally, so many other electronic devices have been incorporated by lawyers to make our lives easier and more mobile, such as I Pads, Laptops, etc. The biggest risk of carrying your client information with you is a breach of security. If you leave the device, lose it, or have it stolen you risk a serious breach of client confidentiality, especially if all your client files and matters are stored electronically and accessible on this device.

Make sure that all cellphones, laptops, I Pads, etc., that are used in your firm or by you personally have the highest level of security. All cellphones should at a minimum be password protected in the event of loss or theft.

Additionally, the client needs to be advised regarding use of their cellphone as it may relate to their legal matter. Does the client use text messaging? What about Facebook posts? Or Instant Messaging?

Text messaging is only somewhat secure and is subject to spoofing. Apple says their software makes text messaging more secure, but admits that even with theirs a person can spoof another. As to how long your carrier stores your text messages: well it depends upon the carrier. The log of messages and calls usually is kept for at least a year but only some carriers retain the content of the message, and usually for a maximum of 3-5 days only. So if you’re looking to subpoena a text message you have a very limited window of opportunity.

**IV. DOCUMENTS**

**A. Inadvertent Receipt/Disclosure of Document**

Because electronic communication makes it possible to transmit large amounts of data with relative ease, it therefore presents greater opportunities for inadvertent disclosure of client information, including privileged information. Since Virginia has not adopted Model Rule 4.4(b) this issue is most recently addressed in LEO 1702 (referenced previously).

The question of whether the attorney-client privilege is waived when a lawyer inadvertently transmits privileged information to another is a question of substantive law that varies from one jurisdiction to another. Generally speaking, courts have taken one of three positions on it:

• the “strict” position that inadvertent disclosure always destroys the privilege; e.g., *Wichita Land & Cattle Co. v. Am. Fed. Bank FSB*, 148 F.R.D. 456 (D.D.C. 1992) (“[d]isclosure of otherwise-privileged materials, even where the disclosure was inadvertent, serves as a waiver of the privilege”);

• the “lenient” position that only a knowing waiver by the client can destroy the privilege; e.g., *Mendenhall v. Barber-Greene Co.*, 531 F. Supp. 936 (S.D. Fla. 1991) (“mere inadvertent production by the attorney does not waive the client's privilege’); or

• the “intermediate” position that the effect on the privilege depends on the circumstances of the disclosure; e.g., *Elkton Care Ctr. Assocs. v. Quality Care Mgmt.*, 805 A.2d 1177, [18 Law. Man. Prof. Conduct 572](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=a0a5y9f4z0&vname=mopcref55) (Md. Ct. Spec. App. 2002) (discussing three approaches and adopting intermediate position; court identifies five factors to consider in deciding whether circumstances amount to waiver of privilege); *Amersham Biosciences Corp. v. PerkinElmer Inc.*, No. 03-4901 (JLL), 2007 WL 329290 (D.N.J. Jan. 31, 2007) (applying five-factor test to party's inadvertent disclosure of privileged metadata).

The Restatement embraces the intermediate position. *Restatement (Third) of the Law Governing Lawyers* (2000) §79 cmt. h (Reporter's Note indicates that majority of courts “take the intermediate position” and “preserve the privilege unless, in effect, the client's own negligence produced the compromising disclosure”).

A great case example: A client sent a law firm a compact disk containing several hundred e-mails. The client asked the firm to review the information, remove privileged material, and produce the remainder to an adversary's discovery manager for conversion to paper format. A firm lawyer reviewed most of the files, deleted some that he considered privileged, and failed to review others that the firm's software could not open. Copies of the deleted files, however, remained on the disk in the form of metadata and the discovery manager's software was able to retrieve, convert, and produce to the adversary both the deleted files and the files that the lawyer could not open.

The court held that the law firm's efforts to protect privileges did not display the “reasonable diligence” necessary to preserve privileges, with the result that all privileges were lost as to the entire contents of the disk. *Amersham Biosciences Corp. v. PerkinElmer Inc.*, No. 03-4901 (JLL), 2007 WL 329920 (D.N.J. Jan. 31, 2007).

**B. Metadata**

Many types of computer software create information that is not visible on the screen or in the printed document, but that can be accessed by those with knowledge of the software's properties. This hidden information, sometimes referred to as “metadata,” may reveal such details about the document's authorship, preparation, prior drafts, and revisions, and therefore about the attorney's legal strategy—even information that the drafter thought had been erased from the visible document. See, e.g., *Advante Int'l Corp. v. Mintel Learning Tech.*, No. C 05-01022 JF(RS), 2008 WL 108900 (N.D. Cal. Jan. 8, 2008) (analyzing discoverability of “redline” version—that is, with deletions still visible—of draft interrogatory response inadvertently produced on client's hard disk.)

**Duty to Prevent Disclosure of Metadata**

Several ethics opinions have concluded that lawyers who transmit electronic documents to third parties have a duty to ensure that no client information is revealed in embedded metadata. Both Rule 1.1 regarding competent representation and Rule 1.6 regarding confidentiality require lawyer’s attention to understanding metadata.

Similarly, a lawyer's failure to take reasonable precautions to remove metadata containing client information before producing it to an adversary in litigation may waive the attorney-client privilege. See*Amersham Biosciences Corp. v. PerkinElmer Inc.*, No. 03-4901 (JLL), 2007 WL 329290 (D.N.J. Jan. 31, 2007) (law firm waived attorney-client privilege and work product protection concerning client e-mails by producing compact disk containing information in hidden metadata files and files inaccessible to producing firm but later recovered by adversary's outside discovery manager); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005) (defendant waived attorney-client privilege as to metadata removed in original production by failing to timely raise objection; ordered to produce).

**Searching for Others' Metadata**

Jurisdictions are split on the question whether it is ethically permissible for a receiving lawyer to search for metadata in electronic documents. Virginia has taken no position on the issue of metadata. The ABA's Standing Committee on Ethics and Professional Responsibility concluded that a receiving lawyer is free to look for hidden, embedded information and use it. [ABA Formal Ethics Op. 06-442](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_ethics_opinion_06_442&vname=mopcref55), 22 Law. Man. Prof. Conduct 555 (2006); accord Maryland Ethics [Op. 2007-09](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_md_ethics_opinion_2007_09&vname=mopcref55), 22 Law. Man. Prof. Conduct 626 (2006) (lawyer receiving metadata may look for and use it, and need not notify sender when it is found).

Other ethics committees, however, have advised that a receiving lawyer should refrain from looking for embedded data in electronic documents. Alabama Ethics [Op. 2007-02](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_al_ethics_opinion_2007_02&vname=mopcref55), 23 Law. Man. Prof. Conduct 219 (2007) (“mining of metadata by an attorney to uncover confidential information would be a violation of [Rule 8.4]”); Arizona Ethics [Op. 07-03](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_az_ethics_opinion_07_03&vname=mopcref55), 23 Law. Man. Prof. Conduct 641 (2007) (when receiving electronic document, lawyer has duty “not to ‘mine’ the document for metadata”); District of Columbia Ethics [Op. 341](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_dc_ethics_opinion_341&vname=mopcref55), 23 Law. Man. Prof. Conduct 501 (2007) (receiving lawyer prohibited from viewing metadata if lawyer has “actual knowledge” that sender “inadvertently” included it); Florida Ethics [Op. 06-2](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_fl_ethics_opinion_06_2&vname=mopcref55) (2006) (Rule 4.4(b) prohibits lawyers from trying to obtain any information from metadata unless it was purposely and knowingly supplied); New York State Ethics [Op. 749](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_ny_ethics_opinion_749&vname=mopcref55) (2001) (looking for information revealed in metadata constitutes “an impermissible intrusion on the attorney-client relationship in violation of the Code” of Professional Responsibility).

**Federal Rule Civil Procedure 26(b)(5)(B)**

This rule requires a party receiving privileged or work product documents claiming to have been inadvertently produced by the other side to hold those documents until a court analyzes the situation. The Rule does not address whether the production has waived any protection. Before discovery starts in federal litigation it may be important to obtain a court order with a “clawback” provision specifying realistic terms and conditions for recovering inadvertently-produced documents.

**By Failure to Object**

In *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005), the defendants in an age discrimination action were ordered to produce several thousand spreadsheets “in the manner in which [the information] was maintained.” Before producing electronic versions of the spreadsheets, however, the defendant “scrubbed” the metadata from them. The district court judge, on learning that the metadata had been removed, ordered the defendant to show cause why it should not be sanctioned for disobeying the discovery order. Among other reasons the defendant's lawyers offered for the scrubbing was that the “metadata may reveal information extracted from a document, such as the items redacted by Defendant's counsel, as well as other protected or privileged matters.”

The court held, however, that because the defendant's lawyers had failed to invoke any privilege objection to the production of the information, any applicable privilege had been waived.

As to the question whether a party has an obligation generally to supply metadata in the production of electronic documents, the court declared “that when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.”

**C. Cloud-based Document Retention and Sharing**

Several authorities have held that it is proper to allow third persons outside the lawyer-client relationship to create and/or store electronic versions of client files if the information is protected from further disclosure. 

In handling client files and records—whether in paper or electronic format—lawyers must take reasonable measures to ensure that client confidentiality is not breached. See, e.g., *Statewide Grievance Comm. v. Paige*, 2004 WL 1833462 (Conn. Super. Ct. 2004) (unpublished) (lawyer customarily reused paper containing confidential client information as scrap, allowing others to have access to client information in violation of Rule 1.6).

***Document Storage.***  May a lawyer require, as a condition of the representation, that the client’s file be kept in electronic format? Yes, as long as the client’s interests are not prejudiced by such a condition of representation. Virginia LEO 1818. Remember e-mails and other electronic documents are all part of the client’s file.

***Document Destruction.***  In determining what to destroy or retain in a client’s file, the attorney should be mindful of the Legal Ethics Committee’s recommendations in LEO 1305 that before destroying a client’s paper file the lawyer should review that file to make sure that any documents that may be of continued use or benefit to the client only if they are maintained in paper form not destroyed.

The lawyer has a duty to inform or notify the client regarding destruction of the file or client property, as per Rule 1.4. Additionally, the lawyer has a duty to maintain client confidences while storing or disposing of client files or property as per Rule 1.6. Best form is to have provisions in your engagement/fee agreement outlining the firm’s file retention policies as to length of time and parameters of file storage.

***Technical Support Providers.*** [ABA Formal Ethics Op. 95-398](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=3706812&fname=aba_ethics_opinion_95_398&vname=mopcref55) (1995) (lawyer considering giving computer service provider access to client files must ensure that provider has or will establish “reasonable procedures to protect the confidentiality” and that it “fully understands its obligations in this regard”).

As to Google docs in particular, Massachusetts has issued an opinion that states:

“Applying its conclusions to Google docs, Lawyer's proposed Internet based data storage solution, the Committee observes that Google has adopted written terms of service and a privacy policy for users of Google docs (see generally<http://www.google.com/google-d-s/terms.html>) that reference and incorporate various other Google policies. Among other things, Google represents that data stored on Google docs is "private" and "password protected," but can be voluntarily shared by the user with others or published to the World Wide Web. The Committee further observes that Google docs and other Internet based storage solutions, like many, if not most, remotely accessible software systems and computer networks, are not immune from attack by unauthorized persons or other forms of security breaches.” Massachusetts Opinion 12-03(5-17-12).

(See attached article on Cloud Computing)

**V. SOCIAL MEDIA AND RELATED ISSUES**

Regardless of your practice area, online connections are fraught with the same ethical pitfalls as in-person interaction with potential clients and others. With the volume of communication made possible by social networking sites, these ethical risks are only magnified:

* Commenting on pending trials or revealing specific case results without a disclaimer.
* Recklessly criticizing judges or other attorneys, or giving that impression.
* Revealing privileged or confidential information.
* Exposing the law firm to claims of defamation or harassment.
* Sending messages that appear to be legal advice, which can create unintended attorney-client relationships.
* Violating ethics rules against solicitation of legal work.
* Practicing law in a jurisdiction where you are not licensed.
* Receiving messages that contain malware or illegal materials.

A. Diligence and competence (Rule 1.1 and 1.4) require the lawyer to:

1. Understand if/how clients are using social networking,
2. Advise clients as to their further use of social networking to their best advantage, and
3. Use social networking sites as investigative tools (opposing party, witnesses, jurors)

B. Confidentiality (Rule 1.6):

1. Messages via Twitter or other social networks must be treated with the same degree of reasonable care as messages via e-mail or other traditional communications.
2. Discussion about pending legal matters raises problems, and generally should be left to traditional e-mail format.

C. Lawyer Advertising and Marketing (Rule 7.1-7.5):

* 1. Statements made on social networks about a lawyer’s services may be subject to the advertising rules.
  2. Name and address of responsible lawyer. Rule 7.2(e).
  3. Disclaimers required for specific case results [Rule 7.2(a)(3)] and specialization claims [Rule 7.4(d)]
  4. Linked In allows you to ask for and receive “recommendations” from clients, colleagues, etc.
  5. Client recommendations are analogous to client testimonials, so:
     1. You can’t have your client say things about you that you can’t say,
        1. Rule 8.4(a)
     2. You probably have a duty to monitor your social network sites and blogs for comments and recommendations that may require revision or deletion.
     3. For example, the lawyer cannot permit to remain on his LinkedIn page a client recommendation that says the lawyer is the “best personal injury lawyer in town” because it is a comparative statement that cannot be factually substantiated. Rule 7.1(a)(3).
  6. Invitations from a lawyer to a prospective client into the lawyer’s LinkedIn or Facebook page would likely not fall within Rule 7.3, because they can always decline the invitation – therefore not considered in-person communication with prospective clients.
  7. Disclaimer required for listing “specialty” on LinkedIn [Rule 7.4(d)] and “endorsements” made by peer or colleagues can and should be edited, if necessary, to ensure they comply with the lawyer advertising rules.

D. Unintended Relationships (Law Firm Web Sites, Chatrooms):

Despite the informality of social networking, the giving of legal advice to others including friends and acquaintances may create unintended client-lawyer relationships. At the very least, it can create confidentiality and conflicts issues. See LEO 1842 (communications with web site visitors). See also ABA Formal Opinion 10-457 (August 5, 2010) (Lawyer Websites).

1. **Triggering Duty of Confidentiality**

A lawyer's duty of confidentiality, whether under the ethics rules or the evidentiary attorney-client privilege, is owed only to those deemed to be clients: current, former, and prospective. *See* [Rule 1.6](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_rules_1_6&vname=mopcref55), [Rule 1.9](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_rules_1_9&vname=mopcref55),  [Rule 1.18](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_rules_1_18&vname=mopcref55); *Restatement (Third) of the Law Governing Lawyers* §§68-86 (2000) (on attorney-client privilege).

In most instances, whether an individual falls within one of these categories is a straightforward matter, having been determined by a clear understanding between the parties. But when those involved do not agree as to the nature of their relationship, courts will make the determination based upon all of the circumstances, including the course of dealings between the parties and especially the reasonable expectations of the purported “client.” Consequently, a court may find that an individual is a current, former, or prospective client, notwithstanding the lawyer's belief that the individual is none of these.

With respect to electronic communication, the greatest risk of unintentionally triggering a duty of confidentiality is by unintentionally creating a lawyer-“prospective client” relationship. A “prospective client” is defined by  [Rule 1.18(a)](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_rules_1_18_a_&vname=mopcref55) as any “person who discusses with a lawyer the possibility of forming a client-lawyer relationship with respect to a matter.” Rule 1.18(b) indicates that, even if no lawyer-client relationship is formed, a lawyer “shall not use or reveal information learned in the consultation [with a prospective client], except as Rule 1.9 would permit [as to former clients].” Comment [2] to the rule notes, however, that a person who communicates “unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship” is not a prospective client entitled to have the information he supplies protected from disclosure or use. See also *Restatement (Third) of the Law Governing Lawyers* §70 (2000) (for purposes of attorney-client privilege, “client” includes “prospective client”).

In this context, what makes electronic communications different from in-person or telephonic communications is the decreased control the lawyer-recipient has over the nature and amount of information conveyed to her. This information comes in segments, such as an e-mail or a posting in a chatroom, whose length and contents are entirely controlled by the sender. Here, the lawyer cannot limit the information received by interrupting the speaker, leaving the room, or hanging up the phone. Once the e-mail is opened, the lawyer has received its entire contents. To further complicate matters, the lawyer may not even be able to determine the sender's identity until after opening the e-mail and receiving all of the information.

This scenario presents the possibility that, simply by opening an e-mail in which the sender discusses a legal matter, a lawyer could find herself with ethical obligations to that person–even if the sender was previously unknown to the lawyer—provided the circumstances were such that the sender reasonably believed that the lawyer was willing to discuss the possibility of representing him in the matter. Several authorities have opined on the circumstances that may trigger a lawyer-“prospective client” relationship—and consequently, a duty of confidentiality—in the context of online communications, and what precautions a lawyer may take to avoid unintended obligations.

Legal information of general application about a particular subject or issue is not “legal advice” and should not create any lawyer-client issues for the blogging or posting lawyer. Appropriate disclaimers will assure this conclusion.

However, if a lawyer by online forms, e-mail, chatroom, social networking site, etc. elicits specific information about a person’s particular legal problem and provides advice to that person, there is a risk that a lawyer-client relationship will have formed. LEO 1842.

Despite the informal nature of most online social networking, lawyers must consider whether informational advice on a blog or website creates the impression of giving legal advice that will be relied upon by a visitor to the site. Another important consideration is the universal reach of online postings. Your website is not only visited by people in your home jurisdiction, so giving friendly online advice to potential clients in states where you are not licensed can easily amount to the unauthorized practice of law under Rule 5.5.

A simple question to ask yourself is whether the online resource you’ve created does anything that would create client expectations. But, clear disclaimers can be helpful in resolving this potential problem.

More tricky than creating unintended client relationships is stumbling into confidentiality and conflict issues. Virginia State Bar LEO 1842 explains that communications with web site users are governed by the same Rules as any other communication with potential clients. The opinion discusses a typical hypothetical: A law firm’s “passive website” lists contact information for each of the firm’s attorneys, and one of the firm’s domestic attorneys receives and reads an unsolicited email from a woman describing the demise of her marriage including her affair with another man. When the attorney realizes she already represents the husband in this matter, what can the attorney do with the information she has learned from this email? Does she owe any duty to keep the wife’s secret?

The Committee concluded that the attorney owes no duty to the wife, since her detailed email was unsolicited and because the wife used “mere contact information provided by the law firm on its website,” which does not create a “reasonable expectation that the information contained in the email will be kept confidential.”

Key to this analysis is (1) whether the firm’s website “creates a reasonable belief that the law firm is specifically inviting or soliciting the communication of confidential information” and (2) “whether it is reasonable for the person providing the information to expect that it will be maintained as confidential.”

The Opinion’s next hypothetical firm runs afoul of this test by including a form on its website that specifically asks potential clients to share the details of their claims in exchange for an evaluation of the case. When a firm receives information via these communications, even where the firm declines to represent the potential client, Rule 1.6 imposes a duty of confidentiality with respect to any information gleaned from the form.

Just as with a live interview of a prospective client, a lawyer has a duty to protect the confidences of prospective clients who submit information via the firm’s website. What’s more, Rule 1.7(a)(2) imposes a material limitation conflict on the lawyer, who will not be able to represent any adverse parties due to the duty of confidentiality owed to the potential client who contacted him online.

The Committee’s simple solution? A “click-through” disclaimer that requires website visitors to agree to disclaimer terms before being allowed to submit any information through an online form. A lawyer should clearly inform online visitors that no attorney-client relationship will result from this communication and that the lawyer cannot guarantee that information shared via the website will be kept confidential.

Whether the disclaimer is sufficiently clear and conspicuous to be effective is the question on which some authorities particularly focus. *Barton v. U.S. Dist. Court for Cent. Dist. of California*, 410 F.3d 1104, [21 Law. Man. Prof. Conduct 290](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=a0b0y6v7q2&vname=mopcref55) (9th Cir. 2005) (attorney-client privilege attached to information people supplied via Web site soliciting information, notwithstanding disclaimer on site stating that no formal lawyer-client relationship was being formed; disclaimer was “potentially confusing to clients” regarding lawyers' confidentiality obligations); California Formal Ethics [Op. 2005-168](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_ca_ethics_opinion_2005_168&vname=mopcref55), 21 Law. Man. Prof. Conduct 584 (information in e-mail submitted via link in firm's Web site could not be disclosed, notwithstanding disclaimer that it would not create “confidential relationship”; disclaimer was “potentially confusing to a lay person”).

A disclaimer “won't make a difference” if a lawyer in an online forum answers “fact-specific legal questions.” A 2010 ABA ethics opinion which offers helpful guidance on the issue. The opinion explains that attorneys “who answer fact-specific legal questions may be characterized as offering personal legal advice,” while a lawyer who simply “poses and answers a hypothetical question usually will not be characterized as offering legal advice.” See ABA Formal Ethics [Op. 10-457](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=28440837&fname=aba_ethics_opinion_10_457&vname=mopcnotallissues), [26 Law. Man. Prof. Conduct 577](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=28440837&fname=a0c4g9j2v3&vname=mopcnotallissues) (2010). “To avoid misunderstanding,” the ABA's ethics committee advised, “lawyers who provide general legal information [should] include statements that characterize the information as general in nature.”

E. Chatrooms, Listserves

Lawyers who participate in online discussions via chatrooms or listservs sometimes expressly identify themselves to other participants as lawyers. If a lawyer-client relationship is formed or another participant in the discussion is deemed to be a prospective client under [Rule 1.18](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_rules_1_18&vname=mopcref55), the lawyer must not disclose or adversely use the information conveyed. District of Columbia Ethics [Op. 316](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_dc_ethics_opinion_316&vname=mopcref55), 18 Law. Man. Prof. Conduct 667 (2002) (lawyer speaking in real time in chatroom or listserv must safeguard confidences revealed “even if an attorney-client relationship has not formed but the lawyer is in a situation in which he or she properly should regard an advice seeker as a prospective client”); New Mexico Ethics [Op. 2001-1](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_nm_ethics_opinion_2001_1&vname=mopcref55), 17 Law. Man. Prof. Conduct 573 (2001) (“If a lawyer begins a dialogue on the Listserve, it is possible that an attorney-client relationship may come into existence [and so create a duty to protect the information conveyed]…. Further, it is incumbent upon the lawyer to retain as confidential any matters the person intends to be confidential”); Philadelphia Ethics [Op. 98-6](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=sum_mpcr_philly_ethics_opinion_98_6&vname=mopcref55) (1998) (cautions lawyers about participation in chatrooms: “[a lawyer] should also be mindful that in the course of an interaction with any person on the internet an attorney/client relationship may begin with all that such a relationship implies including … expectations of confidentiality”).

The fact that others may also have viewed the information posted by a client or prospective client in a chatroom or on a listserv does not affect the lawyer's ethical obligation under [Rule 1.6](http://lawyersmanual.bna.com/mopw2/display/link_res.adp?fedfid=6826873&fname=aba_rules_1_6&vname=mopcref55) not to disclose the information.

1. **Lawyer-Only Listservs, Blogs, Etc.**

Increasingly, lawyers, like other professionals, are participating in law-related listservs to network and consult with colleagues. However, just as lawyers may not, without client authorization, disclose client information in chatrooms, blogs, newspapers, broadcast media, or other public forums, lawyers must take care not to disclose client information on listservs, even ones limited to lawyers. See Los Angeles County Ethics Op. 514, 21 Law. Man. Prof. Conduct 452 (2005) (lawyers communicating on professional association's listserv “should avoid including information in listserv postings identifiable to particular cases or controversies”).

F. Pretexting

Before beginning a jury trial, many attorneys are turning to social networking sites as an invaluable research tool into the suitability of citizens on the jury list. Judges are increasingly checking probationer’s web pages for evidence of drug and alcohol violations. But, diligent research becomes an ethical violation when this passive collection of available information leads to more active online investigations. A defense attorney or investigator, for example, cannot “friend” a prosecution witnesses in an attempt to glean impeachment evidence.

Virginia Rule 8.4(c) prohibits the “dishonesty, fraud, deceit or misrepresentation” required to pretextually “friend” someone online only to garner information useful to a client or harmful to the opposition. And, under Rule 8.4(a) a lawyer cannot use another person to circumvent the Rules, so paralegals and investigators must also be careful how much they dig online.

|  |
| --- |
| The Philadelphia Bar Association’s ethics committee declared unethical a lawyer’s plan to collect information about an adverse litigation witness by hiring an investigator to gain access to the witness’s personal online social networking profiles (Philadelphia Bar Ass’n Professional Guidance Comm., Op. 2009-02, March 2009).  Employing a third party to befriend an adversarial witness through an online social network in order to obtain access to the witness’s personal pages clearly constitutes unethical deception, the committee said, because the plan involves concealing “the highly material fact” that any information collected from those pages would later be used to impeach the witness. The committee concluded that the proposed course of conduct would violate Pennsylvania Rules of Professional Conduct 8.4(c) (conduct involving dishonesty, fraud, deceit, or misrepresentation), 4.1(a) (knowingly making false statements of material fact to third person) and 8.4(a) (violating Rules through acts of another). And, the attorney was held accountable for the investigator’s conduct under Rule 5.3(c)(1), which makes lawyers responsible for behavior the lawyer “orders” or “ratifies.” |

Furthermore, when communicating with any person online, whether under a friendly pretext or after appropriate disclosures, attorneys should also bear in mind the dictates of Rules 4.2 and 4.3 for dealing with those represented by counsel or with unrepresented persons.

G. Law Firm Policies Regarding Social Media:

Developments in the online world heighten the importance of implementing internal law firm policies governing members' use of social media. The growing popularity of Quora—an online Q&A website frequented by attorneys—offers one example of how developments in social media present ethics risks for lawyers and firms. [Quora](https://www.quora.com/) is an increasingly popular question-and-answer website that went public in June 2010 and has become a hub for dispensing online legal advice.

Law firms would be well advised to develop internal policies governing members' use of social media, according to panelists who spoke at a law firm general counsel's forum during the 2012 Aon Law Firm Symposium, held here Oct. 10-12. Stacy L. Brainin, general counsel of Haynes & Boone in Dallas, warned attendees that there are “clear liability issues” attached to attorneys' internet usage. She added, however, that the professional imperative of engaging with social media makes it less feasible to simply prohibit potentially risky online activities. “It is something we all have to deal with, so the best thing to do is identify the risks and establish policies that can protect your firm,” Brainin said.

Brainin cited statistics from a [2012 ABA](http://www.americanbar.org/groups/departments_offices/legal_technology_resources/publications.html)[previous hit](http://lawyersmanual.bna.com/mopw2/display/split_display.adp?fedfid=28571822&wsn=497282500&vname=mopcnotallissues&searchid=19946154&doctypeid=4&type=date&scm=3300&pg=0)[technology](http://www.americanbar.org/groups/departments_offices/legal_technology_resources/publications.html)[next hit](javascript:top.docjs.next_hit(1))[survey](http://www.americanbar.org/groups/departments_offices/legal_technology_resources/publications.html) which showed that:

• 88 percent of the firms in the survey are listed on LinkedIn;

• 55 percent have Facebook pages;

• up to 22 percent host their own blogs; and

• 13 percent maintain a Twitter presence.

These activities, Brainin said, all present risks relating to client confidentiality, prohibited forms of advertising and solicitation, unauthorized practice, and the unintended formation of professional relationships.

Let’s also remember that lawyers in law firms have an ethical duty to supervise subordinate lawyers and non-lawyer staff to ensure that their conduct complies with applicable rules of conduct, including the ethical duty of confidentiality. See Rules 5.1 and 5.3.

Social media policies should be sensitive to the generational differences that generally make younger attorneys less cognizant of the professional risks posed by their online activities, the speakers indicated. The importance of safeguarding client confidentiality is “not as intuitive” to younger attorneys and firms should develop training and orientation programs with an eye towards the age gap.

Similar care should be taken when creating website profiles that list an attorney's “representative cases” or “prior successes”. Simply disclosing a client's identity may constitute a breach of confidentiality in some instances and the risk might not be eliminated by omitting names. Client names could be listed on other portions of the firm's website and it's not that difficult to piece things together and connect a matter to a name.

H. Social Media Tips:

* 1. Keep personal and professional interests separate. Facebook is better suited for personal, family, and friend connections.
  2. **Remember**: “the whole world is watching!”
  3. Frequently monitor and update your posts
  4. Regard social media as a powerful marketing tool.
  5. Use the built-in privacy capabilities of the social networking sites, and consider limiting the access of users you are connected with.
  6. Remember that what you put out there is permanent!
  7. Remember the RPCs still apply to all social networking!

**VI. UNDISCLOSED RECORDING —LEO 1814**

This opinion was issued on March 9, 2011 and holds that a criminal defense lawyer or an agent for the lawyer may ethically employ lawful undisclosed recording during an interview with a material witness. Many of the states originally issued ethics opinions stating that undisclosed recording was either generally improper or *per se* unethical, subject to some limited exceptions. Not all states subscribed to this view and more recently a number of states have reversed or significantly revised their opinions to allow undisclosed recording.

In LEO 1814 the committee also applied Rule 4.3(a) which states that when a lawyer is dealing on behalf of a client with a person not represented by counsel, such as the potential witness in the case, the lawyer cannot state or imply that the lawyer is disinterested; and, when a 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 Committee opines that with undisclosed tape-recording there is a higher risk of the unrepresented party misunderstanding the lawyer or the lawyer’s agent’s role, which correspondingly places a higher burden on the lawyer or the lawyer’s agent to ensure that the unrepresented person does not misunderstand the lawyer or the agent’s role. The Committee relied on opinions in other jurisdictions holding that when a lawyer contacts an unrepresented party on behalf of a client, the lawyer must identify him/herself and his/her representational role. *See Louisiana State Bar Ass’n v. Harrington,* 585 So.2d 514, 517 (La. 1990) (lawyer’s failure to identify himself as a lawyer or carefully explain role in matter violated Rule 4.3 of the Rules of Professional Conduct of the Louisiana State Bar Association); *In re Air Crash Disaster Near Roselawn, Indiana on October 31, 1994*, 909 F.Supp. 1116, 1123 (N.D. Ill. 1995) (questionnaire sent to Defendant’s employees that did not disclose on its face the fact that it was prepared on behalf of plaintiffs’ attorney and implied that it was of a neutral and unbiased character violated Rule 4.3 of Rules of Professional Conduct for the Northern District of Illinois).

LEO 1814 concludes that when a criminal defense lawyer or an agent acting under their supervision uses lawful methods, such as undisclosed tape-recording, as part of his/her interviewing witnesses or preparing his/her case, those methods cannot be seen as reflecting adversely on his/her fitness to practice law; therefore, such conduct will not violate the prohibition in Rule 8.4(c).

The Committee further opined that when a criminal defense lawyer or an agent acting under his/her supervision uses lawful methods, such as undisclosed tape- recording, as part of his/her interviewing witnesses or preparing his/her case, the lawyer or his/her agent must assure that the unrepresented third party is aware of the lawyer or agent’s role.