The Impact of the Internet on a Lawyer's Standard of Care and Professional Responsibility

Part I

Del O'Roark, Loss Prevention Consultant, Lawyers Mutual Insurance Company of Kentucky

Introduction

The Internet profoundly changed the practice of law. It grew from a quick way of sending messages to the enormous capability it has today for transmission of documents. In addition, it has become an invaluable practice tool for lawyers. Today legal research on the Internet is routine, electronic dockets are used by most courts, case investigation often begins with a Google search, and lawyer websites and blogs saturate the Internet.

These developments turned lawyer use of the Internet from a minor risk management consideration to something that has significant professional responsibility and malpractice issues. The primary concern is client confidentiality closely followed by advertising and solicitation issues. Are you clear on the professional responsibility standards for using the Internet to send client confidential information, the significance of metadata in e-mailed documents, and the implications of using your computer on the Internet thereby exposing it to hacking and loss of client confidentiality?

Lawyer websites trigger the advertising and solicitation ethics rules. Do lawyer blogs require compliance with these rules as well? Are they really not so subtle client solicitation ostensibly offering friendly legal information? Does someone in your office have a personal blog on which they discuss the firm? If you fail to use the Internet to research and investigate a matter, are you negligent if you miss something available there? Is it malpractice if you miss a deadline because you did not use the Internet to check electronic court case management systems?

The idea for this article came from these and other Internet issues I noted in monitoring malpractice and disciplinary cases. The problem in writing about them, however, is that rapid change is the one constant in practicing law using the Internet. The expression "it's like trying to paint a moving train" came to mind as I considered how to write something useful. I concluded that the following subjects are of the most current interest and best treated in a two-part article:

Part I

- E-mail Confidentiality
- E-Mail Metadata
- E-mail Disclaimers
- Uninvited E-Mail
- Computer Assisted Legal Research (CALR)
- Google Research
- Internet Court Case Management Systems

Part II (*To be published in a forthcoming issue of the Bench & Bar*)

- Lawyer Websites
- Blogs, Chat Rooms, and Bulletin Boards
- Internet Lawyer Referral Services
- Duty to Protect Client Electronic Documents from Internet Attacks

My purpose is to alert you to the issues and provide, when I can, available guidance and resources. Given the fast moving nature of many of these issues, you should use anything you find of interest here only as a starting point for your independent evaluation of how it affects your practice.

E-Mail Confidentiality

When the Internet took off as a significant means for transmission of legal documents to clients there was considerable angst about the vulnerability of these transmissions to interception or hacking. The KBA Ethics Committee resolved the question for Kentucky lawyers in KBA E-403(1998) in adopting the following language from an Illinois Bar ethics opinion:

> [T]he Committee concludes that because (1) the expectation of privacy for electronic mail is no less reasonable than the expectation of privacy for ordinary telephone calls, and (2) the unauthorized interception of an electronic message subject to the ECPA is illegal, a lawyer does not violate Rule 1.6 by communicating with a client using electronic mail services, including the Internet, without encryption. Nor is it necessary … to seek specific client consent to the use of unencrypted e-mail. … [T]here may be unusual circumstances involving an extraordinarily sensitive matter that … require enhanced security measures like encryption. These situations [are] of the nature that ordinary telephones and other normal means of communication [are] also … inadequate.

The ABA Ethics Committee adopted the identical reasoning in ABA Formal Ethics Op. 99-413 in 1999. It is now routine to use e-mail when communicating with a client and just about everyone else. Nonetheless, in the interest of assuring preservation of the attorney-client privilege, work product immunity, and

client confidentiality the following risk management practices should be employed:

1. The sensitivity of the information and the cost of disclosure to the client are factors to consider when deciding whether to communicate privileged information over the Internet. Taking into consideration how often e-mail is misaddressed, how easily it is forwarded by addressees to others, and that e-mail differs from a telephone call in that it creates a record that is nearly ineradicable, using encrypted e-mail or another more secure means of communication of privileged information is often the best risk management.

2. Be sure that the firm's letter of engagement includes a paragraph on all means of communication the firm uses – fax, cell phone, e-mail, etc. It should disclose the risk of interception and provide that the client consents to these means.

3. Establish written procedures for managing e-mail that protect confidentiality by covering:
   - who has access to confidential e-mail;
   - how confidential multiple address messages and group distributions are to be controlled;
   - how confidential e-mail is to be backed up, stored, and destroyed; and
   - how people who work at home get access to the firm's computer system and send and receive confidential e-mail.

   These written procedures not only serve to protect confidentiality, but are Exhibit A in any allegation that the firm was negligent in protecting client information.

4. Encrypting e-mail remains the safest way to send confidential information. Many lawyers considered encryption in the mid-90's and decided against it because of its complexity. Fortunately, encryption software has gotten cheaper, better, and easier to use. Now may be a good time to reconsider. Encryption is especially useful in sending confidential e-mail to business clients with major computer systems where the risk of unintended distribution is greatest. More important, encryption best protects the interests of clients. What better reason could there be to use it?[1]

E-Mail Metadata

Metadata is data about data that can be transmitted in electronic documents — most frequently in e-mail and in response to discovery requests. In evaluating whether lawyers could review and use metadata in received e-documents the 2004 New York State Bar ethics opinion provides this helpful definition of metadata:

> Word-processing software commonly used by lawyers, such as Microsoft Word and Corel WordPerfect, include features that permit recipients of documents transmitted by e-mail to view "metadata," which may be loosely defined as data hidden in documents that is generated during the course of creating and editing such documents. It may include fragments of data from files that were previously deleted, overwritten or worked on simultaneously. Metadata may reveal the persons who worked on a document, the name of the organization in which it was created or worked on, information concerning prior versions of the document, recent revisions of the document, and comments inserted in the document in the drafting or editing process. The hidden text may reflect editorial comments, strategy considerations, legal issues raised by the client or the lawyer, legal advice provided by the lawyer, and other information. Not all of this information is a confidence or secret, but it may, in many circumstances, reveal information that is either privileged or the disclosure of which would be detrimental or embarrassing to the client.[2]

The New York Ethics Committee concluded that the use of computer technology to 'mine' for client confidences and secrets revealed in metadata constitutes "an impermissible intrusion on the attorney-client relationship …." The ABA Ethics Committee, however, took the position in 2006 that the Model Rules of Professional Conduct do not prohibit such conduct. The Florida, Alabama, and Arizona bar ethics committees rejected that ABA's position and joined New York in precluding metadata mining.[3]

All the opinions cover in some degree the need for diligence on the part of the sending lawyer to protect confidentiality by taking steps to preclude inadvertent inclusion of metadata in e-mail and other e-documents. Some of the ethics opinions distinguish between e-documents obtained through discovery and those voluntarily provided to other persons – making it clear that the ethics opinion does not govern discovery requests. This distinction is based on the supremacy of substantive law over ethics rules on questions of discovery, including waiver of privilege and work product immunity. These issues are beyond the jurisdiction of an ethics committee to adjudicate.

To my knowledge there is no Kentucky authority on the issue of review and use of metadata in e-mail and other e-documents. The states prohibiting lawyers from mining for metadata have followed in principle the ethics rules for the receipt of inadvertently sent materials (think fax) similar to Kentucky's standard as expressed in KBA E-374 (1995):

> When it is clear that the materials were not intended for the receiving lawyer, the lawyer should refrain from examining the materials, notify the sending lawyer and abide the instructions of the lawyer who sent them.

In deciding how to proceed on this issue note that the Kentucky Supreme Court currently has pending before it a proposed change to Kentucky Rule of Professional Conduct SCR 3.130 (4.4), Respect for the Rights of Third Persons. The change adopts KBA E-374 guidance for the treatment of inadvertently sent documents. The proposed Comment [2] to the Rule specifically provides that a document includes e-mail and other e-documents. Should the Court approve this proposal, it will place Kentucky with those states that have rejected the ABA's open season on metadata mining. For risk management purposes that is the approach to follow until more definitive guidance is provided. If you want to be more aggressive, I recommend you consult your judicial district's Ethics Hotline adviser before reviewing and using inadvertently sent metadata.[4]

Risk managing e-mail to avoid inadvertently disclosing confidential or privileged metadata involves carefully determining the format in which to create and send e-documents. Philip Lyon in his article *Confidentiality and Ethics In A Hi-Tech World: Some Nuts and Bolts Solutions* advises that to avoid sending metadata:

- Keep an eye on documents to ensure that the track changes features of word processors are not activated;
- Download and use a metadata removal tool; and
- Send all outgoing files in some format that strips metadata from a document, such as .rtf or pdf.[5]

One note of caution. The requirements for what e-document format to use when responding to a discovery request depends on how the discovery request is styled. For more on this consideration see my article *E-Discovery Risk Management Is the "New New" Thing* (KBA *Bench & Bar*, Vol. 69, No. 6, p. 64 at 68, Nov. 2005; also available on Lawyers Mutual's website at www.lmick.com — go to the Risk Management/*Bench & Bar* page).

E-Mail Disclaimers

Lawyers routinely use disclaimers in e-mail that warn about confidentiality requirements and forbid unauthorized use of the information in the mail. This is good practice and is recommended. The efficacy of e-mail disclaimers, however, is largely untested and may serve more to give comfort to the sending lawyer than anything else. In drafting disclaimers use plain English – think in terms of the least sophisticated person who may receive an e-mail. Do not assume that terms such as 'attorney-client relationship' or 'confidential,' that have specific meaning for lawyers, are understood by nonlawyers. Display disclaimers prominently. Rulings that have not accepted lawyer website disclaimers as effective often note their brevity or inconspicuous display.

Uninvited E-Mail

What is a lawyer's duty of confidentiality to a person who, uninvited, e-mails them directly seeking representation – not through a firm website or by responding to any type of invitation to contact the lawyer based on lawyer marketing? A California lawyer received an uninvited e-mail in which the sender asked to be represented in an auto accident matter and included the information that she had a few drinks just prior to the accident. The sender obtained the lawyer's e-mail address from a bar association alpha list of lawyers not intended to serve as a referral service. The lawyer read this e-mail just after an initial interview with a prospective client who turned out to be the injured party in that accident. The lawyer asked the Legal Ethics Committee of the San Diego County Bar Association whether the uninvited e-mail was confidential, whether she could represent the injured prospective client, and, if so, whether she could use the information received in the e-mail in that representation?

In well written Ethics Opinion 2006-1, the Ethics Committee opined "… that private information received from a non-client via an unsolicited e-mail is not required to be held as confidential by the lawyer where the lawyer has not had an opportunity to warn or stop the flow of non-client information at or before the communication is delivered." The Committee concluded "that if an unsolicited e-mail transmitting information about an adverse party is not confidential, an attorney should be permitted to utilize that information for the lawful purposes of representing an existing client."

If uninvited e-mail becomes an issue for you, read this opinion. It is available on the San Diego County Bar Association website.[6] Keep in mind that the KBA Ethics Hotline is available to help you with close calls. Also note that pending before the Kentucky Supreme Court is the adoption of ABA Model Rule of Professional Conduct 1.18, Duties to Prospective Clients, that covers when a prospective client is entitled to confidentiality. Comment [2] to the proposed rule provides:

> Not all persons who communicate information to a lawyer are entitled to protection under this Rule. A person who communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship, is not a "prospective client" within the meaning of paragraph (a).

Should the Supreme Court adopt Rule 1.18 with Comment [2], Kentucky lawyers will have the guidance they need on this issue.

Computer Assisted Legal Research (CALR) – *It's a Matter of Competence*

More recent members of our Bar will be amused that there ever was a question whether CALR is a requisite for lawyer competence. With the current numerous commercial providers of CALR, along with LawReader.com specializing in Kentucky law and the KBA's free Casemaker Legal Research engine, lawyers failing to avail themselves of these powerful resources expose themselves to allegations of negligence for failing to competently research a matter. No lawyer can afford to be com-

puter illiterate.

Google Investigations

The ALI-ABA is advertising the newsletter *Internet Fact Finding For Lawyers* with the attention grabbing question: Is There a "Duty to Google? The ad asserts that failure to do so is a matter of due diligence. The newsletter authors cite instances when lawyers were stung by failing to Google for missing parties. This proved particularly embarrassing when the court used Google and promptly found relevant information.

The purpose of the newsletter is to help identify websites that are useful for fact finding. For more information Google *Internet Fact Finding For Lawyers*.[7] Note that Google is also highly useful as law finder as well as a fact finder. I am now able to get virtually all state bar ethics opinions over the Internet.

Internet Court Case Management Systems

One of the surest ways to receive a claim for malpractice is to miss a case-dispositive deadline. With the advent of court electronic case management systems that allow lawyers to file documents, view filed documents, receive court orders, and track case docketing over the Internet, the question arises whether failure to diligently track cases on these systems is negligence. The 6th Circuit case of *Kuhn, et al. v. Sulzer Orthopedics, et al* is the leading case I found on this question.

Kuhn concerned whether a lawyer's failure to timely file an appeal to the court's injunction order was excusable because the lawyer did not receive written notice of it and only learned of it when an office paralegal found it when reviewing the court's electronic docket after the time for appeal. The following language from the decision says it all:

> We decline to follow *Nunley* and *Avolio*. Both cases were decided long before electronic dockets became widely available which, as the district court noted, do not even require an attorney "to leave the seat in front of his computer" to keep apprised of what is happening in his cases. .... An interpretation of Rule 4(a)(6) that allowed parties to ignore entirely the electronic information at their fingertips would severely undermine the benefits for both courts and litigants fostered by the CM/ECF system [*Case Management/ Electronic Case Filing*], including ease and speed of access to all the filings in a case. In addition, such an interpretation would defy common sense: It might be one thing not to penalize a party who did not learn about the issuance of an appealable order in the bygone days of hiring "'runners' to physically go to the courthouse to check the docket," but here all Harris had to do was register his email address with the district court's CM/ECF system to receive the court's orders. …. Failing that, Harris simply had to scan periodically the electronic docket for recent activity. Indeed, the unreasonableness of Harris's conduct here is evident in that ultimately, he learned about the district court's Injunction Order in precisely this way: His paralegal checked the online docket and discovered the order. (*citations omitted*)[8]

The damages at stake in the *Kuhn* case were as much as $800,000 – maybe more. Any malpractice claim against Kuhn's lawyer will be difficult to defend, to say the least. Good practice and good risk management require firm policies that call for routine and meticulous monitoring of all electronic court case management systems in which the firm has a pending case. *Kuhn* is highly recommended professional reading. ■

ENDNOTES

1. Extract from my article *The Latest on Ethics and Malpractice In the Dot Com World of Law*, KBA *Bench & Bar*, Vol. 65, No. 5, p. 33 at 34, Sep. 2001.
2. The New York State Bar Ass'n Comm. on Professional Ethics, Op.782, 12/8/2004.
3. ABA Formal Op. 06-442; Ala. Op. RO-2007-02; Fla. Op. 06-2; Az. 07-03. Maryland and the District of Columbia follow the ABA position: D.C. Op. 341; Md. 2007-09.
4. SCR 3.530 (2).
5. ALI-ABA, The Practical Lawyer, Vol. 53, No. 2, p. 15 at 18 (April 2007). A copy of this article is available for $15.00 at the ALI-ABA website – Google *The Practical Lawyer* (last viewed on 3/17/2008).
6. Last viewed on 3/10/2008.
7. Last viewed on 3/17/2008.
8. 2007 WL 2287742.