The Speed of Normal: Conflicts, Competency, and Confidentiality in the Digital Age

by
*David Hricik**

Table of Contents

I. INTRODUCTION ..... 74 R
II. RECEIVING DIGITAL CONFIDENTIAL INFORMATION FROM PROSPECTIVE CLIENTS ..... 74 R
A. The Conflict Arising from Receipt of Confidences ..... 74 R
B. Are These Website Disclaimers Legally Necessary? ..... 77 R
C. Effective Process ..... 79 R
D. Effective Substance ..... 80 R
E. Model Language to Adapt to Your Jurisdiction and Practice ..... 81 R
III. INTENTIONAL DISCLOSURE THROUGH LAW FIRM NEWSLETTERS AND ARTICLES ..... 82 R
IV. RECEIPT AND DISCLOSURE OF DIGITAL CLIENT CONFIDENCES, CHATROOMS, BULLETIN BOARDS AND LISTSERVS ..... 84 R
V. AUTHORIZED ACCESS TO DIGITALLY STORED CLIENT CONFIDENCES ..... 87 R
A. Competent Electronic Storage of Client Data ..... 87 R
B. Physical Security of Stored Client Data ..... 89 R
1. Nonmobile Hardware ..... 89 R
2. Mobile Technology ..... 90 R
VI. SECURITY OF NETWORK-ACCESSIBLE STORED CLIENT DATA ..... 91 R
A. Information Stored on an Unprotected Website ..... 91 R
B. Sharing Office Space ..... 93 R
C. Storing Client Data with Application Service Providers ..... 94 R
VII. UNAUTHORIZED ACCESS TO STORED CLIENT DATA ..... 95 R
A. Hacking, Viruses, and Spyware ..... 95 R
B. Wi-Fi Risks ..... 97 R
VIII. MISCELLANEOUS ISSUES ..... 98 R
A. Billing for Computer-Aided Legal Research ..... 98 R
B. E-mail Tracking: Is it Unethical? ..... 98 R
C. Using Legends on E-mails ..... 98 R
IX. CONCLUSION ..... 99 R

* Professor David Hricik is an Associate Professor at Mercer University School of Law. The title is from John Wesley Harding's compact disc, John Wesley Harding's New Deal (1996).

I. INTRODUCTION

Digitalization has increased the speed of communications in all areas, including law. Although in many ways technology has made practice easier, quicker, and more efficient, the dawn of the digital age has increased the need for lawyers to focus on legal ethics. As always, lawyers must be concerned about confidentiality, conflicts, and competency. Those fundamentals remain unchanged. However, the vast increases in storage capacity, the lightning-quick speed of communication, and the ability to allow access to data over the Internet have each made it more important for lawyers to focus on the impact of technology on these core principles of legal ethics.

Digitalization means that breach of a duty of confidentiality can have far greater consequences because more information can be stored today in smaller spaces than ever before. Where once it would have taken a truck and an army of burglars to steal an important but voluminous file, today it can be accomplished by the palming of a memory stick, the taking of a CD, or the theft of a laptop computer. Although lawyers still must be concerned that a brief case or an important folder of papers might be stolen or misplaced, lawyers in the digital world must recognize that a file cabinet full of documents can be lost if a laptop, or even a single CD, is lost or stolen. Similarly, with the ease and speed of digital communications, a conflict of interest can arise in a nanosecond by opening an email.

The ethical duties of confidentiality, competency, and loyalty have not changed, but the means and speed by which they can be breached differ in the digital age. Courts and bar associations have, as yet, given little practical guidance to lawyers on these and other issues. This article describes how lawyers can meet their obligations of loyalty, confidentiality, and competency when working at the lightning fast speeds that have become the speed of normal in the digital age.

II. RECEIVING DIGITAL CONFIDENTIAL INFORMATION FROM PROSPECTIVE CLIENTS

A. The Conflict Arising from Receipt of Confidences

Not too long ago, a person wanting to hire a lawyer had to call him on the phone or stop by to see him. In that initial interview, the lawyer had to be certain that undertaking the representation would not create a conflict of interest with an existing or former client.[1] To avoid both personal and imputed disqualification, the lawyer in the initial interview had to—and still must—control disclosure of information by the prospective client so that only information necessary to check conflicts was obtained from the prospective client. This is because many states hold that a person who, in a good faith effort to hire a lawyer, discloses confidential information to one lawyer in a firm, can

1. *See, e.g.*, Bridge Prods., Inc. v. Quantum Chem. Corp., 1990 WL 70857 (N.D. Ill. 1990) (firm disqualified after a one-hour meeting with prospective client).

disqualify that entire firm to the same extent as if an attorney-client relationship had been consummated.[2]

E-mail makes it easier for conflicts to arise because it changes the nature of communication. A lawyer who is *talking* to a prospective client can control the disclosure. Before hearing information that might disqualify him from continuing to represent a client, for example, the lawyer can ask the prospective client who the adverse party will be, inquire as to the general nature of the matter, and perform a conflicts check. However, in the digital age, there is less control over receipt of confidences, and greater opportunity for firm disqualification. A web page listing lawyer e-mail addresses allows putative clients to send an e-mail to a lawyer that discloses important confidential information that could lead to imputed disqualification of the firm. For example, a person could read a law firm web site, conclude that the firm

2. *See, e.g.*, Gilmore v. Goedecke, 954 F. Supp. 187 (E.D. Mo. 1996) (disqualifying an entire law firm from representing its client of 50 years because one lawyer had learned information from opposing party when, as putative client, it disclosed information during a brief phone call). Courts had so widely recognized this duty that a form of it is expressly codified in the 2003 version of the American Bar Association Model Rules of Professional Conduct. Model Rule 1.18 generally prohibits firms from being adverse to such putative clients in matters where the information that had been disclosed to the firm could be used to significantly harm the then-prospective client:

> (a) A person who discusses with a lawyer the possibility of forming a client-lawyer relationship with respect to a matter is a prospective client.
> (b) Even when no client-lawyer relationship ensues, a lawyer who has had discussions with a prospective client shall not use or reveal information learned in the consultation, except as Rule 1.9 would permit with respect to information of a former client.
> (c) A lawyer subject to paragraph (b) shall not represent a client with interests materially adverse to those of a prospective client in the same or a substantially related matter if the lawyer received information from the prospective client that could be significantly harmful to that person in the matter, except as provided in paragraph (d).
> (d) When the lawyer has received disqualifying information as defined in paragraph (c), representation is permissible if:
> (1) both the affected client and the prospective client have given informed consent, confirmed in writing, or:
> (2) the lawyer who received the information took reasonable measures to avoid exposure to more disqualifying information than was reasonably necessary to determine whether to represent the prospective client; and
> (i) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and
> (ii) written notice is promptly given to the prospective client.

MODEL RULES OF PROF'L CONDUCT R. 1.18 (2003).

would be an excellent choice to represent her, and then send the firm an e-mail discussing the potential strengths and weaknesses of the case and requesting a meeting.

If an entire law firm can be disqualified by imputation because one of its lawyers received information from a prospective client during a face-to-face meeting or phone call, can it likewise be disqualified to the same extent if it reviews the same information sent by e-mail from a client seeking in good faith to hire the firm?[3] This scenario actually occurred in California. A woman seeking to hire a divorce lawyer filled out a questionnaire with some confidential information about her case and sent it to a firm which already happened to be already representing her husband in that matter.[4] If receipt of such email is no different than receipt of "too much" information during an initial interview, then an entire firm can be disqualified by imputation.[5]

Law firms recognize this possibility. Accordingly, law firms are posting many different kinds of contractual "terms of use"—terms which are often called "disclaimers"—on their web sites. Many sites state that any information sent by e-mail before the firm agrees to represent the transmitting party will not be held to be confidential by the firm.[6] Others say that no attorney-client relationship will be formed by submitting the information.[7]

These website disclaimers appear designed to avoid imputed disqualification by receipt of information from prospective clients. Read literally, they would preclude a person who sent an e-mail to a firm in a good faith effort to hire the firm from relying on the confidentiality of the information to cause imputed disqualification.

---

3. As one commentator posited:

> Suppose an online visitor submits an inquiry to an attorney along with the requisite information, and, before responding, the attorney determines that a partner or other member of the firm already represents the opposing party. The attorney is now in receipt of information that could create an impermissible conflict such that the online visitor making the inquiry can attempt to force a withdrawal of representation of opposing party.

Thomas E. Lynch, *Ethical Problems with Legal Computer Advertising and Affiliations*, 34 MD. B.J. 11, 12 (2001).

4. St. B. of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Proposed Formal Op. Interim 03-0001 (2005) *at* http://www.calbar.ca.gov/state/calbar/calbar_generic.jsp?cid=10145&n=61041 (last visited Oct. 15, 2005).

5. Under the Model Rules, if one lawyer in a firm is disqualified from being adverse to a former client due to possession of confidential information, generally all lawyers in that firm are "imputed" with that conflict. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1 (2003).

6. *See, e.g.*, www.velaw.com (last visited Oct. 15, 2005) ("Any information sent to Vinson & Elkins . . . is on a non-confidential and non-privileged basis.").

7. *See* Barton v. U.S. District Court, 410 F.3d 1104, 1107 n.5 (9th Cir. 2005) (quoting firm's disclaimer).

For practical reasons, the existence of a law firm web site increases the need for these disclaimers, since having a website creates an easy means to transmit unsolicited information to law firms. Significantly, it can be done unilaterally and even contrary to the intent of the lawyer. Further, while a lawyer who receives an unsolicited telephone call can simply stop the prospective client from disclosing additional information as soon as the lawyer recognizes a conflict exists, an e-mail is sent instantaneously, and opened in full at once.

B. Are These Website Disclaimers Legally Necessary?

The need for advanced agreements arose in the context of old-world contacts, by face-to-face meeting or telephone call. There was obviously mutual assent to the exchange of information. In addition, by continuing the conversation, a lawyer who continues a phone call accepts the prospective client's invitation to consider forming an attorney-client relationship. Has a lawyer who merely opens an unsolicited e-mail done something to indicate to its sender that the lawyer assents to receive information in confidence or is open to representing that person?[8] Should an e-mail sent unilaterally by a prospective client through a law firm website be treated any differently than a phone call placed to a lawyer, or a meeting held between lawyer and prospective client? Is e-mail different enough from these "old-world" forms of communication so that a different rule should apply, and so these advance waivers are unnecessary?

The opinions so far conclude that by posting a website, a lawyer has manifested an intent to offer to form attorney-client relationships and to keep submitted information confidential. On the one hand, the Arizona Bar Association concluded that a lawyer who did not have a website, but had an e-mail address, did not implicitly invite submission of information by prospective clients.[9] According to the committee, such lawyers owed no duty of confidentiality to prospective clients, since the absence of a website indicated no willingness to accept clients by e-mail.[10] On the other hand, that Arizona opinion reasoned that "if the attorney maintains a website without any express limitations on forming an attorney-client relation, or disclaimers explaining that information provided or received by would-be clients will not be held confidential," then the lawyer has implicitly agreed to consider forming an attorney-client relationship with those who submit e-mail.[11] The As-

8. *See* St. B. of Ariz. Comm. on the Rules of Prof'l Responsibility, Ethics Op. 02-04 (2002) *at* http://www.myazbar.org/Ethics/pdf/02-04.pdf (last visited Oct. 15, 2005).

9. *Id.*

10. *Id.*

11. *Id.*

sociation of the Bar of the City of New York reached a similar conclusion.[12] As part of a lengthy analysis, it reasoned:

> We believe that prospective clients who approach lawyers in good faith for the purpose of seeking legal advice should not suffer even if they labor under the misapprehension that information unilaterally sent will be kept confidential. Although such a belief may be ill-conceived or even careless, unless the prospective client is specifically and conspicuously warned not to send such information, the information should not be turned against her. Indeed, we see no reason that the other client should be benefited by the fortuitous circumstances that the lawyer approached by the prospective client turned out to be the same lawyer retained by the adverse party. Nor do we believe that zealous advocacy compels a different result.[13]

A California opinion reached essentially the same conclusion.[14] There, a firm site had links that allowed prospective clients to submit information in order to learn their rights. The committee found this was an offer to consult with the lawyer.[15]

Under this approach, lawyers who have websites need to both effectively disclaim any intention to form an attorney-client relationship and effectively warn prospective clients of the lawyers' intention not to hold transmitted information in confidence.[16] The dominant reasoning, so far, is that having a website invites formation of a confidential relationship, and the lawyer must disabuse the client of that intent. Thus, disclaimers are necessary.

---

12. Ass'n of the Bar of the City of New York, Op. 2001-1 (March 1, 2001) *at* http://www.abcny.org/Ethics/eth2001-01.html (last visited Oct. 15, 2005).

13. *Id.*

14. *See* St. B. of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Proposed Formal Op. Interim 03-0001 (2005) *at* http://www.calbar.ca.gov/state/calbar/calbar_generic.jsp?cid=10145&n=61041 (last visited Oct. 15, 2005).

15. *Id.*

16. New Model Rule 1.18 differs even further in its approach to this issue. Even where there is no advance agreement, only the lawyer who actually received the information is disqualified if he reviewed the information only to the extent necessary to determine whether to represent the client, took steps to avoid further dissemination of the information, and the prospective client is given notice. *See* MODEL RULES OF PROF'L CONDUCT R. 1.18 (2005). If this is acceptable to a firm, then it somewhat reduces the need for specific agreement. However, Model Rule 1.18 is not yet in effect in many jurisdictions.

C. Effective Process

If the lawyer has a website and is required to negate any intent to form a confidential attorney-client relationship, there are two levels that must be considered: (1) making the process for obtaining consent effective and (2) making the consent substantively effective and appropriate. This subsection addresses the former; the next subsection, the latter.

Contracts require assent.[17] As a matter of contract law, simply relying, as many firms do, on passive "terms of use" accessible through a "disclaimer" or "legal notices" link on the bottom of the law firm's homepage probably does not create an enforceable agreement.[18] There is no assent by the prospective client. In addressing web-contracts, courts are holding that terms which are merely somewhere on a website are not part of a contract formed by a website user. Instead, only terms which are affirmatively "clicked" and thereby assented to, are part of the agreement. In the leading case of *Specht v. Netscape Communications Corp.*,[19] for example, an arbitration clause was on Netscape's website on a page of "user terms," but users were not required to "click" acceptance to the clause before downloading software.[20] Instead, the user was merely asked to "please review" terms and conditions which included the arbitration clause.[21] Following the approach of other courts, the *Netscape* court held that there was no proof that the user had assented to the arbitration clause; hence, there was no agreement to arbitrate.[22] These courts recognize that where the user affirmatively "clicks" agreement to the term—a so-called "click wrap" agreement—the term could be enforced.[23] Nevertheless, they rejected attempts to create "browser wrap" agreements: attempts to bind users of a site merely because they opened it in their browser.[24]

Thus, having a "disclaimer" or "terms of use" link on their homepage which links to a page that contains the term of use regarding the confidential-

17. "The fundamental idea of a contract is that it requires the assent of two minds." Dexter v. Hall, 82 U.S. 9, 20 (1872).

18. *See, e.g.*, *www.Jonesday.com/admin/terms.aspx?sType=Terms+of+Use* (last visited Oct. 15, 2005).

19. 306 F.3d 17 (2d Cir. 2002).

20. *Id*.

21. *Id*.

22. *Id*. at 40. *See* Kevin P. Cronin & Ronald N. Weikers, *Data Security & Privacy Law: Combating Cyberthreats* § 10:29 (2003) (discussing click wrap and other forms of web-based agreements). *See also* Ticketmaster Corp. v. Tickets.com, 2003 Copr. L. Dec. ¶ 28,607 (C.D. Cal. March 7, 2003) (discussing other assent issues concerning Internet usage).

23. *Netscape*, 306 F.3d at 40.

24. *See generally*, Jennifer Femminella, *Online Terms and Conditions Agreements: Bound by the Web,* 17 ST. JOHN'S J. LEGAL COMMENT. 87 (2003).

ity of e-mail sent by prospective clients is likely not an effective process to create an enforceable agreement with any prospective client. "Click wraps" are the only certain way to ensure that a court will hold that the prospective client manifested assent to the term. Thus, law firm websites should be coded so that prospective clients must affirmatively assent to the term before transmitting an e-mail to the law firm.

D. Effective Substance

In addition to an effective procedure, the language should substantively accomplish the law firm's goal of avoiding disqualification, but not create other problems. A casual perusal of several law firm websites reveals that by far the two dominant approaches that firms currently use are either to disclaim any intent to form an attorney-client relationship, or disclaim any obligation of confidentiality of unsolicited information.[25] Neither approach is satisfactory.

Disclaimers which state that any information will not be held in confidence are unhelpful because they are overbroad. While no doubt a prospective client who agrees by "clicking" to such terms would be precluded from disqualifying the recipient law firm due to its receipt of that information, the term destroys the ability of the submitting party to claim privilege. Suppose, for example, that the firm decides after receiving an unsolicited disclosure of key information to represent the sender as a client. In most jurisdictions, the client could not claim privilege because when the client transmitted the information, it knew the information would not be held in confidence.[26] Indeed, the existence of these clauses may preclude firms from agreeing to represent the client, since the firm has arguably caused the client to lose privilege.

While these "no confidentiality" provisions go too far, a "we do not represent you" clause does not go far enough. In a recent case, the Ninth Circuit held that a plaintiff could still claim privilege over information it submitted through a law firm site even though when it did so it acknowledged it was not forming an attorney-client relationship.[27] It held the information could still be claimed as privileged, since the client had never explicitly agreed that the information would not be held confidential.[28] Likewise, a California bar opinion concluded that only if the prospective client had expressly agreed that information would not be held in confidence could a firm avoid an obligation of confidentiality.[29] The bar association reasoned

25. Several firms have both statements. *See, e.g.*, www.velaw.com/admin/contactus.asp (last visited Oct. 15, 2005).

26. *See generally* In re Eddy, 304 B.R. 591, 596 (Bankr. D. Mass. 2004).

27. *Barton*, 410 F.3d at 1107 n.5.

28. *Id.*

29. St. B. Cal. Standing Comm. on Prof'l Responsibility & Conduct, Proposed Formal Op. Interim 03-0001 (2005) *at* http://www.calbar.ca.gov/state/calbar/calbar_generic.jsp?cid=10145&n=61041 (last visited Oct. 15, 2005).

that even though the client had clicked an agreement that "no confidential relationship would be formed," it was insufficient to constitute an acknowledgement that the firm would not keep the prospective client's information confidential.[30] The opinion concluded that it would be sufficient only if the disclaimer had stated: "I understand and agree that Law Firm will have no duty to keep confidential the information I am now transmitting to Law Firm."[31]

Taken together, the decisions demonstrate that a "no attorney-client relationship" disclaimer is not enough to avoid an obligation of confidentiality. If, however, the firm uses an appropriately-worded "no confidentiality" approach, it avoids an obligation of confidentiality, but risks waiving a claim of privilege, even if the prospective client becomes a real one.

In my view, neither disclaimer is the right one. The goal for most firms is not to avoid creating an attorney-client relationship,[32] or to deny confidentiality, but to avoid disqualification. The approach of Model Rule 1.18 is instructive. It does not state that there is no attorney-client relationship between the putative client and would-be law firm, nor that information submitted in good faith will not be held in confidence. Instead, it provides that receipt of the information by one lawyer in the firm will not preclude the entire firm from representing another party in the matter.[33] Thus, the rule still requires firms to keep information confidential and does not let the firm disclose to an adversary critical information received from a prospective client.

E. Model Language to Adapt to Your Jurisdiction and Practice

The lesson of Rule 1.18 is that any term should do what it needs to do, but no more. An agreement by which an unsophisticated party supposedly gives up all right of confidentiality to information which it submitted in good faith to the firm may also be too severe to be enforced by a court or found ethical by a bar association. Likewise, an agreement which might destroy the ability of a party who eventually becomes a client to claim privilege over information goes too far in the other direction, and could require a firm to turn away a client who submitted information through the firm's web site.

---

30. *Id.*

31. *Id.*

32. The argument that a client can create an attorney-client relationship by submitting an email to a firm that would impose a duty on the firm to act to protect the client's interests in any way other than by maintaining the confidentiality of information seems beyond far-fetched. *See generally*, Togstad v. Vesely, Otto, Miller & Keefe, 291 N.W.2d 686 (Minn. 1980) (finding that the firm had duty to advise person it declined to represent but had advised on the strength of the person's claim of applicable statute of limitations). A lawyer who has someone shout at him "I was injured" does not have to tell the person to get a lawyer.

33. MODEL CODE OF PROF'L CONDUCT R. 1.18 (2003).

Law firms should adopt language that does what they want it to do: *i.e.*, prevent even those who in good faith seek to hire the firm from disqualifying it from representing another party where that information can be used against the prospective client. The following examples of language seek in varying degrees to balance the legitimate but competing needs of the firm and its clients, as well as those of prospective clients.

> By clicking "accept" you agree that our review of the information contained in e-mail and any attachments will not preclude any lawyer in our firm from representing a party in any matter where that information is relevant, even if you submitted the information in a good faith effort to retain us, and, further, even if that information is highly confidential and could be used against you, unless that lawyer has actual knowledge of the content of the e-mail. We will otherwise maintain the confidentiality of your information.

The foregoing seeks to eliminate firm-wide disqualification. While doing so, it could still result in the disqualification of an individual lawyer from a matter. Another approach:

> By clicking "accept", you agree that we may review any information you transmit to us. You recognize that our review of your information, even if you submitted it in a good faith effort to retain us, and, further, even if it is highly confidential, does not preclude us from representing another client directly adverse to you, even in a matter where that information could and will be used against you.[34]

III. Intentional Disclosure through Law Firm Newsletters and Articles

Another consequence of the power of dissemination created by the web comes, not from receipt of information by a firm, but by its dissemination through the availability of "articles" on law firm web sites. It is common for firms to have an "articles" or "presentations" web page containing the text of

34. In jurisdictions which follow Arizona's analysis, the following may be sufficient, with the last sentence added to remove any doubt:

> E-mail addresses of our attorneys are not provided as a means for prospective clients to contact our firm or to submit information to us. By clicking "accept", you acknowledge that we have no obligation to maintain the confidentiality of any information you submit to us unless we have already agreed to represent you or we later agree to do so. Thus, we may represent a party in a matter adverse to you even if the information you submit to us could be used against you in the matter, and even if you submitted it in a good faith effort to retain us.

articles or speeches written by firm attorneys.[35] No doubt, firms perceive that this material makes the firm more marketable. It also serves a useful educational function.

However, information in these articles can be used against the firm or its clients. For example, a client could use a firm's article against the firm in a malpractice suit, arguing that the firm failed to follow its own advice in representing the client. This actually happened when a legal malpractice plaintiff alleged that his lawyer had failed to hire an expert for his case. She was able to get into evidence the fact that her lawyer previously had written in a CLE article that a lawyer should "always" hire such experts.[36]

The lawyer's article could also be quoted back against the lawyer's clients. It seems unlikely that articles on a firm's web site would be admissible against a lawyer's client under most circumstances, since they would not have been made by the party, and so would not constitute party admissions. Nevertheless, the writings of a lawyer can be used against a client in briefs and motions, where the rules of admissibility do not apply.

Articles create other risks. A lawyer serving as an expert could be impeached by having his articles used against him in depositions and at hearings outside the presence of the jury. Another possibility is third party malpractice claims, where a third party claims to have relied on "legal advice" contained in an on-line article. There is, however, no reported case in which an attorney was sued for allegedly giving incorrect legal advice in an article.

Despite the lack of any objective evidence that a lawyer-author should be concerned, many lawyer-authors put disclaimers in their works warning the reader not to rely upon them. One model form reads:

> This book is presented with the understanding that the publisher does not render any legal, accounting, or other professional service. Due to the rapidly changing nature of the law, information contained in this publication may become outdated. As a result, an attorney using this material must always research original sources of authority and update this information to ensure accuracy when dealing with a specific client's legal matters. In no event will the authors, the reviewers, or the publisher be liable for any direct, indirect, or consequential damages resulting from the use of this material.[37]

Including a disclaimer such as this in web-based articles seems prudent. It would also be wise to include a statement that the article does not reflect

35. *See, e.g.*, Kilpatrick Stockton LLP, Articles, *at* www.kilpatrickstockton.com/publications/articles.aspx (last visited Oct. 15, 2005).

36. *McGuiness v. Barnes*, 683 A.2d 862, 863 (N.J. Super. Ct. Law Div. 1994).

37. Ellen Claire Newcomer & Gregory W. Black, *Liability for Errors and Omissions in CLE Speeches and Publications*, 37 CLE J. & REG. 5, 5 (Jan. 1991).

the views of the author's firm or client. The ABA has come out with a list of "best practices" for law firm web sites. Among other things, it suggests:

- Including contact information;
- Dating substantive legal material;
- Identifying which jurisdiction any substantive legal material pertains to; and
- Stating that the legal information is not legal advice.[38]

Finally, to be effective, it may be necessary that the site be structured to require users to affirmatively agree to the terms of the disclaimer.[39] As noted above, without an affirmative "click" indicating acceptance, the disclaimer may not be a part of the "contract" with the site's user.

IV. Receipt and Disclosure of Digital Client Confidences, Chatrooms, Bulletin Boards and Listservs

Chatrooms, bulletin boards, and listservs are similar in that they all allow lawyers to interact with third parties by both sending and receiving information. They thus carry the same risks that e-mail does: the risk that someone in the chatroom will disclose information that could disqualify the firm. In addition, they enhance the risk of inadvertently creating an attorney-client relationship through giving specific legal advice during interactive and sometimes real-time discussions. The former is little different from the risk of receiving email, as discussed above. This section explores the latter issue.

The enhanced risk of creating an inadvertent attorney-client relationship arises from the way these technologies allow for interaction, sometimes in real-time. Chatrooms allow for synchronous, real-time "conversation," while bulletin boards and listservs generally allow asynchronous communication – the former generally through websites, the latter generally through e-mail. While each technology has rough analogs in the real world – since they are somewhat like the interchange that might occur at a CLE meeting or in casual cocktail party discussions – they differ in two ways.

First, the number of participants and the frequency of interaction differ. One listserv I participate in, for example, has several dozen participants, each of whom is deeply involved in legal ethics issues. On a daily basis, the Internet allows for the exchange of ideas and information among these people; in the analog world, such an exchange could take place only on rare, isolated occasions. In essence, there is a daily cocktail party consisting of people who may be representing or consulting conflicting clients. Other listservs may include opposing counsel or opposing parties as participants. Thus, on any given day, a lawyer on a listserv might communicate inadver-

38. American Bar Association, *Best Practice Guidelines for Legal Information Web Site Providers*, *at* http://www.elawyering.org/tools/practices.shtml (last visited Oct. 15, 2005).

39. Putting the disclaimer in the article itself, as opposed to on the site, would also accomplish the same goal.

tently with opposing parties about a subject matter in which they are both involved.

A second difference is that the "real world" dialog is not ephemeral. Conversations at a cocktail party or a CLE conference may not be recorded. In contrast, what occurs in chatrooms, on bulletin boards and in listservs is often maintained in digital form on the web itself, and that record is often searchable.[40]

These differences suggest the need for greater caution. While there have been very few difficulties prior to the advent of the Internet, those two differences may suggest that the Internet creates greater risk. The conclusions of the few bar opinions that have addressed the ethical issues arising from posting responses to third party questions on message boards or listservs confirms that observation.

The North Carolina State Bar, for example, concluded that lawyers could answer questions posted by third parties on a company's web site,[41] but that they should:

- Avoid giving advice concerning jurisdictions in which they were not licensed;
- Warn that responses should not be considered as legal opinions or as a conclusive answer to the question posted, and recognize that "there may be other facts and law relevant to the issue;"
- State where the lawyers were licensed (to avoid misleading the users into believing the lawyer lives in the state where the user resides);
- State "clearly and specifically" that the lawyer did not want to create an attorney-client relationship with the user; and
- Warn users not to post confidential information in their questions.[42]

In another opinion, the New Mexico Bar Association addressed various aspects of listservs and related technologies.[43] In addition to focusing on some of the same issues as the North Carolina opinion, it emphasized the unique nature of the listserv:

---

40. For example, one law review article quoted a post I had made to a listserv several years earlier. *See* Justin D. Leonard, *Cyberlawyering and the Small Business: Software Makes Hard Law (But Good Sense)*, 7 J. SMALL & EMERGING BUS. LAW 323, 373 n.251 (2003) (also noting the "negative aspect of electronic communication—with the unseen permanence of this 'electronic tattooing', anything you say can be found again—even years later.")

41. N.C. St. Bar Ass'n, 2000 Formal Ethics Op. 3 (July 2000), *at* http://www.ncbar.com/eth_op/ethics_sel.asp?ID=306 (last visited Oct. 15, 2005).

42. *Id*.

43. N.M. St. B. Ass'n, Advisory Op. 2001-1 (2001), *at* http:www.nmbar.org/Content/NavigationMenu/Attorney_Services_Practice_Resources/Risk_Management/Topical_Index/2000-2002_opinions/2001-1.doc (last visited Oct. 15, 2005).

> At the outset, the Committee recognizes that the party placing the question on the Listserve has already divulged information in a less that private setting. As such, the confidentiality of any information in an initial query is unlikely to exist. However, the party's expectation of privacy may be based upon a misunderstanding of the nature of the Listserve. The expectation of privacy may exist, rightly or wrongly, in the mind of the party. Any lawyer proceeding to respond to such a question should be mindful of this and cautious with regard to any response. Specifically, the lawyer should not respond in any fashion which solicits additional information of a confidential character. . . .
>
> Specific questions (e.g., "I have failed to inform my partners of my borrowing of funds from the partnership. . . what do I do now?") create more difficult situations. The difficulty is that, by making legal information available on its Listserve, such access to Listserve lawyers may unintentionally encourage the placement of confidential information on the Listserve thereby causing the information to lose its confidential character.
>
> The Internet remains a relatively new frontier. To date, there also remains various concepts of the level of privacy resulting from use of the Internet. As a result, it would be important for any lawyer involved in such a Listserve arrangement to insist that the Listserve administrator clearly and unambiguously inform users that any material placed on the service will or may lose its confidential character.[44]

These opinions suggest that lawyers who participate on listservs should recognize the increased risk of creating attorney-client relationships with participants. They also suggest that merely posting disclaimers will not always be sufficient. Likewise, the opinions suggest that an attorney should consider the question of confidentiality before posting information and, according to the New Mexico opinion, whether he must insist that the listserv owner warn participants not to disclose confidences.

Clearly, firms should consider adopting policies that address lawyer participation in chatrooms, bulletin boards, and the like, to reduce the likelihood of conflicts or malpractice liability, or at least poor client relations. One aspect of such a policy is to require the use of disclaimers—statements that the lawyer's e-mail does not constitute legal advice, for example, and that no attorney-client relationship is formed thereby. These efforts may help. However, the New Mexico Bar Association emphasized that reliance upon these boilerplate disclaimers may not be enough: "any statement which would suggest to a reasonable person that, despite the disclaimer, a relationship is being

---

44. *Id*. *See also* D.C. Bar Ass'n, Op. 316 (July 2002), *at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinions316.cfm (last visited Oct. 15, 2005).

or has been established, would negate the disclaimer. In short, the lawyer must be vigilant and cautious if the intention is to not create an attorney-client relationship."[45]

Another aspect of chat rooms is the question of whether they constitute improper solicitation. Generally, there are few constraints on public legal advertisements, but significant constraints on in-person contacts with people that a lawyer knows is in need of legal services.[46] The authorities so far have concluded that real-time communications over the Internet in a chat room constitute improper solicitations.[47] Some states characterize them as "telephonic communications", while others find they are "in person" communications, subject to the most stringent ethical constraints.[48] Thus, in addition to being concerned about conflicts and confidentiality, lawyers must also be concerned about solicitation.

The dynamic nature of chatrooms in particular suggests that educating lawyers about the various risks is the best approach for firms to take. Lawyers should understand the permanent nature of these seemingly ephemeral forms of electronic communication, recognize the need to avoid creating conflicts, avoid improperly soliciting prospective clients, and generally acknowledge the vast uncharted territory in this area.

V. Authorized Access to Digitally Stored Client Confidences

A. Competent Electronic Storage of Client Data

Model Rule 1.15 requires lawyers to "appropriately safeguard" client files.[49] Lawyers ethically may store files digitally.[50] However, doing so creates at least three issues.

First, the files must be accessible to the client and lawyer. It should by now be common practice for lawyers when writing a brief or memo on a computer to "save" the work every few minutes in case the computer crashes.

---

45. N.M. St. B. Ass'n, Advisory Op. 2001-1 (2001), *at* http:www.nmbar.org/Content/NavigationMenu/Attorney_Services_Practice_Resources/Risk_Management/Topical_Index/2000-2002_opinions/2001-1.doc (last visited Oct. 15, 2005).

46. *See* Model Rules of Prof'l Conduct R. 7.2 (2005).

47. *See* Cal. St. B. Standing Comm. on Prof. Resp. & Conduct, Formal Op. No. 2004-166 at 6 (2004), *at* http://calbar.ca.gov/calbar/pdfs/ethics/2004-166_02-0002.pdf (last visited Oct. 15, 2005) (collecting bar opinions from Florida, Utah, Michigan, Virginia, West Virginia and Arizona). States characterize chat room communications differently, however. *See id.*

48. *See id.* at 4, n.6.

49. Model Rules of Prof'l Conduct R. 1.5(a) (2005).

50. *See* Me. Bd. of Overseers of the Bar, Op. 183 (Jan. 28, 2004), http://www.meoverseers.org/Ethic%20Opinions/Opinion%20183.htm. (last visited Oct. 15, 2005).

Saving work is only half the process. Competent practice requires making backups of critical information. It is probably overstated to say that "[f]ailing to back up your data is an act of negligence,"[51] but backing up important client data plainly is something every lawyer ought to do.[52]

The details of a backup plan will vary. Putting a copy of critical files onto a CD will help, but leaving the CD on the computer will accomplish nothing in the event of an office fire. Thus, assigning a person to back up files and then to remove the backups may be a useful approach. The frequency of a backup is also a variable: need it be nightly, weekly, or at some other interval? There is no set rule. How much work can your clients or you afford to lose is the critical question that lawyers must ask.[53]

Second, the files must be secure. Files stored on Internet-accessible computers raise critical security issues. Third parties, such as computer maintenance companies, could view these files, even if they are not network accessible. Although it is ethical for lawyers to permit third parties to have access to computer systems in order to maintain files and computer and storage systems those third parties should sign confidentiality agreements.

> A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information. Should a significant breach of confidentiality occur, the lawyer might be obligated to disclose it to the client.[54]

In addition, lawyers should obtain "a written statement of the service provider's assurance of confidentiality."[55] Permitting third parties access is not an ethical violation so long as the obligation of confidentiality is maintained.[56]

---

51. Albert Barsocchini, *ABCs of Computer Security*, LAW TECH. NEWS 27, 27 (Nov. 2000), *at* http://ltn-archive.hotresponse.com/november00/security_spotlight_p27.html (last visited Oct. 15, 2005).

52. See Jason Krause, *Guarding the Cyberfort* 89 A.B.A. J. 42 (July 2003) ("Probably the most important thing a lawyer can do to avoid document disaster is to have an effective backup plan."). An interesting question is whether a lawyer can charge a client for time spent recreating work product lost as a result of a computer malfunction. No authority on that issue exists.

53. *Id*. Lawyers should consider rotating tapes or CDs, for example. *See* Steven Atherton, *Protecting Your Firm's Critical Data*, 27 VT. B. J. & L. DIG. 17, 17 (2001).

54. Am. B. Ass'n Formal Op. 95-398 (Oct. 27, 1995).

55. *Id.*

56. *See* N.C. St. Bar, RPC 209 (Jan.12, 1996), *at* http://www.ncbar.com/eth_op/ethics_sel.asp?ID=209 ("[A] lawyer should store a client's file in a secure location where client confidentiality can be maintained."); N.Y. St. Bar Ass'n,

For these reasons, anyone who can access stored client confidences should be required to sign confidentiality obligations similar to the lawyers' own.[57] Particularly because digitalization makes it easier for theft to occur, sometimes without warning or indications it has occurred, and with greater consequences, lawyers need to pay particular attention when they give third parties access to digitized client confidences.

Third, lawyers must ensure legacy access. Storage technology can become obsolete, preventing ready access to data. For example, it is very difficult to find disk drives that can read 8-inch floppy disks, yet they were common not that long ago. Storage media, even CDs, may also degrade over time.[58] For these reasons, lawyers must ensure that data stored on "old" media remains accessible by updating the media or maintaining hardware that allows for legacy access.

There are other, more mundane issues to consider as well, such as using battery backups for critical equipment. Not only will taking reasonable steps avoid the loss of unsaved data when the power goes out, it will also ensure access to data at all times, so that, for example, court deadlines can be met.[59]

B. Physical Security of Stored Client Data

1. Nonmobile Hardware

The physical security of any point of access to digitized client confidences ought to be a critical focus of any information security approach.[60] If someone can walk into the lobby of a law office and use an unattended PC to

---

Opinion 643 (Feb. 16, 1993), *at* http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_643.htm ("We also see no ethical impropriety in storing closed files . . . so long as client confidences . . . are protected from unauthorized disclosure. The files should be stored in a secure location and should be available only to the client, the client's present or former lawyer, or another with the client's informed consent.") (citation omitted); Mich. St. Bar Ass'n, RI-100, (Sept. 30, 1991), *at* http://www.michbar.org.opinions/ethics/numbered_opinions/ri-100.hmt (lawyer may "[s]tore client representation files and other law firm files which are not to be destroyed in a facility which protects client confidences and secrets, safekeeps property, and complies with record-keeping requirements").

57. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3 (2005) (requiring lawyers who directly supervise nonlawyers exercise reasonable care to ensure the non lawyer's conduct is compatible with the lawyer's ethical obligations).

58. Some studies conclude CDs may last only two years. *See* Bob Starrett, *Do Compact Discs Degrade?*, *at* http://www.roxio.com/en/support/discs/dodiscsdegrade.html (last visited Oct. 15, 2005).

59. *See generally*, Paul Bernstein, *Loss and Recovery,* 37 J. TRIAL L. ASS'N 59, 59 (2001).

60. The same obviously holds true for file rooms and other physical storage sites.

access client files, the firm has a security problem. Likewise, if an opposing counsel can use a computer in a conference room to access networked client files, real security risks exist.

The obvious first step is to train employees to be aware of these risks. Employees who man publicly accessible computers, such as in lobby waiting areas, should know not to leave the computer running in such a way that allows access to client information. "Logging out" and using password access may be required any time the computer is left unattended, for example. Similar precautions are needed in areas where opposing counsel (or third parties) can physically access computers which contain or can access digitized client files.

2. Mobile Technology

Mobile technology creates even greater risks. Where once it would have taken a truck and an army of burglars to steal an important but voluminous file, today's burglars can accomplish the same heist merely by palming a memory stick, swiping a CD, or stealing a laptop computer. Employees with devices that contain digitized client confidences should be advised that they can hold critical information, and in large amounts.

A written policy is in order. Anyone carrying a laptop containing client confidences, for example, should be advised of the various scams reported at airport metal detectors: where one person steps in front of the laptop owner, sets off the metal detector, while his compatriot on the other side takes advantage of the distraction to make off with the computer.[61]

There are also services that can locate stolen laptops when the thief uses them to connect to the Internet. For example, the makers of "Stealth Signal"[62] claim the program will secretly contact the company, providing the computer's location and even allowing its owner to delete files from the laptop, so long as the owner reports the computer as missing.[63] The site states that the software cannot be removed or even detected.[64] Lawyers whose laptops carry extremely sensitive information should consider acquiring and using this software.

There are more mundane ways to secure digitized client files. It is possible to give password protection to files (Microsoft Word allows this, for example) so that the file cannot be easily opened.[65] Even greater protection

61. *See* Josh Ryder, *Laptop Security, Part One: Preventing Laptop Theft*, *at* http://www.securityfocus.com/infocus/1186 (visited July 14, 2005).

62. *See* Stealth Signal, *at* http://www.computersecurity.com/stealth/index.html (last visited Oct. 15, 2005)

63. *See* Stealth Signal, *at* http.//www.computersecurity.com/stealth/computer_tracker.html (last visited Oct. 15, 2005).

64. *Id.*

65. In the "Save As" window in Word, click the "Tools" drop down and then go to "Security Options" to password protect a file.

through encryption programs is also available for individual files[66] as well as entire sectors of hard drives.[67] Depending on the importance of the information, such steps may be necessary.

VI. Security of Network-Accessible Stored Client Data

A. Information Stored on an Unprotected Website

State ethics rules generally prohibit *ex parte* contacts with persons who are known to be represented by counsel in a matter.[68] Is a visit to an opponent's website during litigation a violation of such rules? Put another way, does anything prevent an adversary during litigation from accessing an opponent's web page and gleaning information from it, and then using it against the site owner?

The Oregon Bar Association addressed this issue.[69] It recognized that the digital nature of the contact was irrelevant. If the contact was prohibited in the real world, then it was prohibited in digital one, too.[70] Thus, since a lawyer can obviously read a 10-K filed by its opponent, or its annual report, a lawyer who reads information posted on a website is not violating the rule.

While a passive review of publicly accessible information does not violate the rule against *ex parte* contacts, websites are often interactive. The Oregon Bar Association distinguished between different degrees of interactivity as follows:

> Some web sites allow the visitor to interact with the site. The interaction may consist of providing feedback about the site or ordering products. This kind of one-way communication from the visitor to the Web site also does not constitute communicating "with a person" as that phrase is used in DR 7-104. Rather, it is the equivalent of ordering products from a catalog by mailing the requisite information or by giving it over the telephone to a person who provides no information in return other than what is available in the catalog. . . . . .
>
> A more interactive Web site allows the visitor to send messages and receive specific responses from the Web site or to participate in a "chat room." A visitor to a Web site who sends a message with the expectation of receiving a personal response is communicating with the responder. The visitor may not be able to ascertain the identity of the responder, at least not before the response is

66. Use the same steps noted in the note above, but encrypt the file.

67. *See generally*, Phil Morris, *Hard Drive Encryption Software*, *at* http://www.techsupportalert.com/pdf/r1178.pdf (last visited Oct. 15, 2005).

68. *See, e.g.*, Model Rules of Prof'l Conduct R. 4.2.

69. Oregon St. B. Ass'n. Op. No. 2001-164 (Jan. 2001), *at* http://www.osbar.org/_docs/ethics/2001-164.pdf (last visited Oct. 15, 2005).

70. *Id.*

> received. In that situation, a lawyer visiting the Web site of a represented person might inadvertently communicate with the represented person. If the subject of the communication with the represented person is on or directly related to the subject of the representation, the lawyer violates DR 7-104.
> For example, assume Lawyer B's client is a retailer in whose store a personal injury occurred. Lawyer A could visit the store and purchase products without the consent of Lawyer B, and could ask questions about the injury of clerks and other witnesses not deemed represented for purposes of DR 7-104. Lawyer A could not, however, question the store owner or manager or any clerk whose conduct was at issue in the matter. That same analysis applies if Lawyer B's client operates an "e-store." Lawyer A could visit the "e-store" site and review all posted information, purchase products, and respond to surveys or other requests for feedback from visitors. Lawyer A could not send a demand letter or an inquiry through the Web site requesting information about the matter in litigation unless Lawyer A knew that the inquiry would be answered by someone other than Lawyer B's client (or, if the client is a corporation, someone deemed represented).[71]

Thus, passively entering an opponent's website does not implicate the rule against *ex parte* contacts. Information on a web page is not "confidential" and can be used against a client in a matter. Only if the contact crosses into an improper "interactive inquiry" can the rule be violated.

There is one error—an important one—in the Oregon opinion. Under the Oregon opinion, a lawyer may not contact a person through the Internet unless the lawyer knows the person is *not* represented. This is incorrect, loose language.

The rule specifically provides that contacts are permitted unless the lawyer *knows* the person is represented.[72] It has been interpreted that way by the courts. Numerous courts have held that Model Rule 4.2 cannot bar a contact unless the lawyer knows the person is represented. For example, in *Jorgensen v. Taco Bell Corp.*,[73] the court rejected even a "should have known" standard, stating:

> Taco Bell's proposal has wide and troubling implications. Under it, counsel for a plaintiff who is a tort victim would risk disciplinary action by interviewing adverse parties or their employees, if that counsel "should have known" such interviewees would be represented by some unidentified counsel after a complaint is filed. Reasonable investigations by counsel in advance of suit be-

71. *Id.*

72. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2002).

73. 58 Cal. Rptr. 2d 178 (Cal. 1996).

> ing filed to determine the bona fides of a client's claim would be precluded.
>
> Every plaintiff's attorney should know, for example, that some defense counsel will, with rare exceptions, be provided by a liability insurance carrier to represent its insured after the filing of a complaint alleging acts within the ambit of the coverage. Similarly, every defense counsel should know that frequently an injured plaintiff who may, without counsel, preliminarily negotiate with the liability carrier's representative, will ordinarily retain counsel to file suit if no settlement is reached.
>
> In these situations, Taco Bell's proposed expansion of the application of rule 2-100 [California's version of Model Rule 4.2] would arguably mean that both plaintiff and defense attorneys would be subjected to disciplinary action for violating rule 2-100 if they directed interviews of claimants or alleged tortfeasors, although no determination to file suit had been made and no lawyer to file or defend it had been retained.
>
> Taco Bell contends that it had unidentified "house counsel," as Jorgensen's attorney "should have known," available to communicate with Jorgensen's attorney before her investigator conducted interviews of its employees. Taco Bell reasons that Jorgensen's lawyer had to first identify its house counsel and seek that counsel's permission to interview Taco Bell's employees to avoid violation of rule 2-100. Numerous corporations in America have full or part-time house counsel. That knowledge or presumptive knowledge does not trigger the application of rule 2-100, unless the claimant's lawyer knows in fact that such house counsel represents the person being interviewed when that interview is conducted.[74]

Thus, the Oregon Bar Association's opinion takes the prohibition against *ex parte* contacts too far. Unless the lawyer knows the person with whom she is interacting is "represented" in terms of Model Rule 4.2, the contact should be proper.

B. Sharing Office Space

For economic reasons, some lawyers who are not members of the same firm share office space.[75] Because each does not owe an obligation of confi-

74. *Id*. at 180.

75. *See generally*, George C. Rockas, *Lawyers for Hire and Associations of Lawyers: Arrangements that are Changing the Way Law is Practiced*, 40–DEC B. B. J. 8, 18 (Nov./Dec. 1996).

dentiality to the other, it is important that physical client files be maintained in confidence.[76]

The same is true for stored client data. It is "impermissible for unaffiliated attorneys to have unrestricted access to each other's electronic files (including e-mail and word processing documents) and other client records.[77] "If separate computer systems are not utilized, each attorney's confidential client information should be protected in a way that guards against unauthorized access and preserves client confidences and secrets."[78]

Thus, if lawyers share a common server with lawyers who are not in the same firm, they should ensure that only the lawyer and his employees can access client files. Likewise, employees should be instructed to log off computers and not leave networked computers unattended.[79] Finally, using encryption features of popular word processing software like Word may be helpful.

C. Storing Client Data with Application Service Providers

Application Service Providers (ASPs) sell services to assist lawyers, *e.g.*, virtual deal rooms, online collaboration tools, online document assembly, on-line billing services, e-mail, file storage, file back-up services and other products and services available to lawyers over the Internet.[80] Because they are strangers to the privilege, lawyers must ensure that these web-based companies comply with the ethical obligations of the lawyer.[81]

Thus, for example, if the lawyer stores digital client data with an ASP, the lawyer has an obligation to ensure that the data is maintained in protected

76. *See* N.Y. St. Bar Ass'n Comm. of Prof'l Ethics, Op. 680 (1990), *at* http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_680.htm (last visited Oct. 15, 2005).

77. D.C. Bar Legal Ethics Comm. Op. No. 303 (2001), *at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion303.cfm (last visited Oct. 15, 2005).

78. *Id*.

79. *See generally*, Colo. Ethical Op. 89 (1991), *at* http://www.cobar.org/group/display.cfm?GenID=1810 (last visited Oct. 15, 2005); Neb. Ethical Op. 89-2 (1989), *at* http://www.nebar.com/ethics/Opinions/89-2.htm (last visited Oct. 15, 2005); N.Y. County Ethical Op. 692 (1993), *at* http://www.nycla.org/library/ethics.htm (last visited Oct. 15, 2005); Robert W. Martin Jr., *Practicing Law in the 21st Century: Fundamentals for Avoiding Malpractice Liability*, 33 LAND & WATER L. REV. 191 (1988).

80. *See generally*, Carole Levitt, *Application Service Providers are Gaining Acceptance*, 24-JUN L.A. LAW. 56 (June 2001).

81. David Hricik and Peter Krakaur, *ASPs. Very Dangerous? You Go First*, *at* http://www.legalethics.com/articles.law?auth=snake.txt (last visited Oct. 15, 2005).

systems, and that those who have authorized access to the data (such as employees of the ASP) have an obligation of confidentiality that mirrors, or is similar to, that owed by the lawyer.[82] ASP employees are no different in that respect from computer consultants who have access to the firm's own computer systems.[83]

In addition, the reliability of the ASP ought to be investigated by the lawyer. Does it have multiple backups of the data, stored at different locations? Can it guarantee that it will be online virtually all of the time? These and other issues need to be explored.[84]

VII. Unauthorized Access to Stored Client Data

A. Hacking, Viruses, and Spyware

A 2001 ABA study reported that 13% of law firms had been hacked.[85] Any computer hooked to the Internet via DSL or cable modem is *networked* to the Internet. That is, someone on the Internet could access your computer directly. Unfortunately, a recent survey showed that the computer systems used by small firms and solo practitioners were especially vulnerable to attack.[86] Only about one in ten used antivirus software, and one in five used firewalls.[87] Attacks can come in the form of hacks, viruses, and spyware.

The potential for a hacker gaining access through a virus to a computer connected to the Internet is real. The fact that thousands of PCs are surreptitiously used by spammers as "attack zombies" to send spam demonstrates the ease with which a third party can commandeer a PC.[88] A recent case provides an even more interesting example of the risks that hackers create to networked computers. In *U.S. v. Steiger,*[89] a Turkish citizen posted a program that appeared to be useful on a site frequented by pedophiles. The program, once downloaded by the pedophile, did not only provide the useful functions to the pedophile, it also allowed the Turkish citizen to review every file on the downloader's computer, and to track every site the person visited

82. *See generally*, Andrew S. Breines, *Security is key as ASPs Make Inroads into the Legal Market*, 18 No. 4 GPSolo 24, 26-27 (June 2001).

83. *See id.* at 27.

84. *See id.*; *see also* Carole Levitt, *supra* note 80.

85. *See* Jason Krause, *Guarding the Cyberfort*, 89-JUL A.B.A. J. 42 (July 2003).

86. Gareth T. Yearick, *ABA Survey Shows Computer Systems Used by Many Solo and Small Firm Practitioners are Vulnerable to Hackers*, 29 Litig. News 3 (Jan. 2004), *available at* http://www.abanet.org/litigation/litigationnews/jan2004/jan2004/LTNonlline29_2-vulnerable.pdf (last visited Oct. 15, 2005).

87. *Id.*

88. By one estimate, attack zombies account for 80% of all spam. *See Zombie PCs generate 80 per cent of spam*, *at* http://www.whatpc.co.uk/vnunet/news/2125121/zombie-pcs-generate-80-per-cent-spam (last visited Oct. 15, 2005).

89. 318 F.3d 1039 (11th Cir. 2003).

as well as track every password the person used.[90] Another recent virus locked up computer users' files through encryption and required the user to pay money to get the files back.

Spyware is similar to a virus in that it can in some forms permit third parties to monitor web activities, e-mail, and in some forms, file contents.[91] Other forms of spyware gather passwords and personal information, or reset or hijack a user's browser.[92]

In order to avoid becoming a zombie box or having data, web activities, and passwords made accessible to a hacker, lawyers need to take precautions. The three principal safety features to use are firewalls, anti-virus software, and anti-spyware software.

Firewalls are hardware or software barriers–walls–between a computer and the Internet.[93] A firewall protects a user's computer against intruders. A basic firewall will essentially hide the address of the user's computer from third parties and block "ports" on PC's from being used by the hackers.[94]

Essentially, antivirus software examines downloaded files and e-mail attachments to identify and disarm known "malware," software that allows hackers to take control of a PC. For example, if a user downloads a file from the Internet that contains a "Trojan Horse," like the kind in the *Steiger* case, the program will alert the user and allow them to stop the virus. A good policy for virus protection includes these elements:

> First, purchase a good anti-virus software (e.g., Norton AntiVirus or McAfee's) from a reputable company that you expect has the resources to respond quickly to new threats. Second, update your software daily using the Internet. For firms having two or more attorneys, I recommend purchasing network anti-virus software that automatically checks for updates daily and distributes them seamlessly across the network without requiring user intervention. Third, implement firm wide policies for use of floppy disks, downloading of files over the Internet, and for handling attachments, as it is through such functions that viruses tend to spread.

90. *Id*. at 1043-44.

91. *See* Sharon D. Nelson & John Simek, *Spyware: Is Your Computer Looking Back at You?* L. PRAC. MAG. 19 (April/May 2005), *available at* http://www.senseient.com/default.asp?page=publications/article32.htm. (last visited Oct. 15, 2005).

92. *Id*.; *see also* Jason Krause, *Beware of Spyware*, 91-JUN A.B.A. J. 51 (June 2005).

93. There is a huge amount of information available on the Internet describing firewalls. One of the most detailed and neutral that I have found was prepared by the National Institutes of Standards and Technology, and is available at http://csrc.nist.gov/publications/nispubs/800-10/node31.html (Last visited Oct. 15, 2005).

94. *See* Atherton, *supra* note 53.

> A simple policy would require that: (1) all floppy disks used on computers outside of your network be scanned for viruses by a designated person; (2) people obtain permission before downloading any program (such as screen savers, audio players or demos) over the Internet; and (3) any email attachments coming from unknown persons or without any text in the body of the message be deleted or scanned for viruses by a designated person before opening.[95]

Unfortunately, many antivirus software programs do not detect, let alone remove, spyware.[96] Thus, special anti-spyware software which costs $30 to $40 must be used.[97]

B. Wi-Fi Risks

The use of wireless technologies to communicate creates special risks. With wi-fi, an "access point" is wired to the Internet, and laptops or desktops communicate by radio frequencies with the access point much like a cordless phone base station and handset.

There are two distinct ways wi-fi can be used. First, a law firm may create a wireless network within the firm office.[98] Second, when lawyers are outside the firm they may use third party access points to connect to the Internet. Both circumstances create risks because in both situations, there is a broadcast of data between the computer and the access point.[99]

Nevertheless, when setting up a network, the law firm can choose to encrypt the broadcast. However, on most hardware the default setting allows for unencrypted transmissions. Thus, when setting up a law firm wi-fi network care must be given to ensuring that the access point communicates with the computers only through encrypted means. This prevents electronic eavesdropping.

Encryption of the broadcast will not work where a public wi-fi connection is used. Thus, lawyers should be educated about the risk that public wi-fi use creates. Anyone within the range of the wireless card can pick up the transmission. Lawyers need to know of this risk and to understand that it may mean public wi-fi is not an appropriate means to transmit certain client confidences.

---

95. *Id.*

96. *See* Nelson & Simek, *supra* note 91.

97. *Id.*

98. *Id.*

99. There is another risk that does not implicate confidentiality. An unsecured access point can be used by third parties to access the Internet. There are maps on the Internet of where such free access is available.

VIII. Miscellaneous Issues

A. Billing for Computer-Aided Legal Research

Lawyers who charge clients for costs incurred with third-party legal research services such as Westlaw or Lexis, should disclose that fact in engagement letters.[100] This is especially true if they are adding on any sort of mark-up to the charge.[101]

B. E-mail Tracking: Is it Unethical?

Technology permits the sender of an e-mail to track its subsequent route and to also receive copies of comments made as the e-mail is forwarded around. Some call it "e-mail wiretapping."[102] There are patches and other efforts that lawyers can take to reduce the ability of such tracking to occur.[103]

The only opinion to address this issue concluded that using this software is unethical *if its use is illegal*:

> Although our jurisdiction does not extend to questions of law, we note that the misuse of some aspects of this technology, particularly the use of e-mail "bugs," may violate federal or state law prohibiting unauthorized interception of e-mail content. In that event, such conduct would, of course, be unethical *per se*.[104]

Whether this sort of software violates the ECPA or SCA is an interesting question, and one beyond the scope of this article, but there is no settled answer. It may be legal, and therefore ostensibly ethical to track e-mail that a lawyer sends. The point here, though, is much broader. Because this sort of technological monitoring is possible, forwarding an e-mail received from the Internet creates risk, whether it is from opposing counsel or some third party.

C. Using Legends on E-mails

Many law firms have programs which automatically place legends below the "signature" which purport to claim privilege over the contents and to

100. *See Guerrant v. Roth*, 777 N.E.2d 499, 507 (Ill. App. 2002) (costs of computer research were, under ambiguous contingent fee agreement, held to be "attorneys fees" and so firm could not recover them from client as "expenses").

101. *See* ABA Comm. on Prof'l Ethics and Professional Responsibility, Formal Op. 93-379 (1993).

102. *See* Richard M. Smith & David Martin, *E-mail Wiretapping*, *at* http://www.privacyfoundation.org/privacywatch/report.asp?id=54&action=0 (Feb. 2001) (last visited Oct. 15, 2005).

103. *See id*.

104. N.Y. St. B. Ass'n. Comm. Prof'l Ethics Op. 749 (Dec. 14, 2001) (citations omitted), *at* http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_749.htm (last visited Oct. 15, 2005).

impose various duties on the recipient.[105] The efficacy of these things remains to be seen.

There are reasons not to use them. First of all, the characterization by a lawyer of a message as privileged or confidential is not going to bind a court, and its absence will not preclude claiming privilege. Perhaps more importantly, putting "privileged" on every e-mail—particularly those sent to opposing counsel—may in fact work against the lawyer. Suppose, for example, that every time a lawyer has sent an email to opposing counsel it says "privileged." Eventually, the lawyer accidentally sends one which *is* privileged to that opposing counsel. Is a court going to find the undisciplined and indiscriminate claim of privilege helps, or hurts? If legends are used, they should only be used when, in fact, the message is privileged.

IX. CONCLUSION

There is no going back. Clients expect and so lawyers need access to digital modes of communication and storage. They offer tremendous utility and rewards, but with digitalization and the speed and bandwith it offers come greater risks. Operating at the speed of normal today, as a consequence, requires awareness of those risks and active risk management by lawyers and law firms.

105. *See generally*, David F. Gallagher, *When E-mail Messages Come with a Tail of Legalese*, *at* http://partners.nytimes.com/library/tech/00/03/cyber/cyberlaw/17law.html (last visited Oct. 15, 2005).