THE SPEED OF NORMAL: CONFLICTS, COMPETENCY, AND CONFIDENTIALITY IN THE DIGITAL AGE

Presented By:

DAVID HRICIK*, Macon, GA
Walter F. George School of Law
Mercer University

BRIAN DOUGLAS MELTON, Houston
Susman Godfrey

W. AMON BURTON, Austin
Adjunct Professor
University of Texas at Austin
School of Law

Written By:

DAVID HRICIK*, Macon, GA
Walter F. George School of Law
Mercer University

State Bar of Texas
19TH ANNUAL INTELLECTUAL PROPERTY LAW COURSE
March 2-3, 2006
San Antonio

CHAPTER 20
PROFESSOR DAVID HRICIK, B.A., J.D.

Assistant Professor of Law, Mercer University School of Law, Macon, GA (2002-).
B.A., 1984, University of Arizona; J.D., 1988, Northwestern University School of Law.

Professor Hricik teaches Patent Law & Litigation; Professional Responsibility; Civil Procedure; and Remedies, and also serves as an expert witness and consultant to patent malpractice, disqualification, and litigation matters.

He is the Chair of the Professionalism & Ethics Committee of the American Intellectual Property Law Association (2005-) and chaired the Ethics & Professional Responsibility Committee of the Intellectual Property Section of the American Bar Association (2002-03). He also served as a member of the Texas Disciplinary Rules of Professional Conduct Committee of the Texas State Bar (1997-2002). Professor Hricik has taught law at the University of Houston Law Center and the University of Texas School of Law and other courses at St. Edward’s Graduate School of Management.

Prior to becoming a full-time professor of law, Professor Hricik practiced law, principally in patent and complex commercial litigation, first with Baker Botts (Associate, 1988-96; Special Counsel, 1997-99), then as a founding partner of Slusser & Frost (Partner, 1999-2000), and finally with Yetter & Warden (Of Counsel, 2000-2002).

He has numerous publications and presentations on legal ethics and patent practice and his website, www.Hricik.com, contains various ethics and intellectual property resources.
Brian D. Melton
Partner

Houston, Texas
Phone: 713.653.7825
Fax: 713.654.6692
bmelton@susmangodfrey.com*

BRIAN D. MELTON - born Shreveport, Louisiana; admitted to bar, 1999, Texas.

Brian Melton is a partner in the Houston office of Susman Godfrey L.L.P. Mr. Melton’s practice concentrates on litigation of all types. He has successfully litigated for both plaintiffs and defendants in complex commercial cases. Mr. Melton has been recognized by H Magazine as a “Lawyer on the Fast Track” in 2004, “Houston’s Best Lawyers Under 40” in 2004, and as a “Professional on the Fast Track” in 2005. Texas Monthly magazine named him a “Texas Rising Star for 2006.”

EDUCATION

- United States Military Academy at West Point, New York (B.S. 1991)
- University of Houston (J.D., summa cum laude, 1999)

HONORS & DISTINCTIONS

- Law Clerk to The Honorable Tom Stagg, United States District Court for the Western District of Louisiana (1999-2000)

PROFESSIONAL AFFILIATIONS

- State Bar of Texas
- American Bar Association

*Internet mail is not fully secure or private. Therefore, please do not transmit confidential information via Internet mail. Transmission of information is not intended to and does not create an attorney-client relationship. Please do not assume that your communications sent using Internet mail is privileged or confidential. Please do not send Susman Godfrey any confidential information via the Internet without previously consulting one of our attorneys.
Amon Burton teaches legal ethics at The University of Texas School of Law. He presently serves on the MPRE board that drafts the national professional ethics examination used by states in the licensing of lawyers, and is a member of the State Bar Committee presently drafting proposed changes to the Texas Disciplinary Rules. He served for 12 years on the Texas Supreme Court committee that writes ethics opinions interpreting the Texas Disciplinary Rules. He has been a visiting lecturer in legal ethics at Cornell Law School. His latest article, "Reexamining the Role of In-House Lawyers After the Conviction of Arthur Andersen," (co-authored with Prof. John S. Dzienkowski) appeared in the book, *Enron: Corporate Fiascos and Legal Implications* (Foundation Press 2004).
# TABLE OF CONTENTS

I. INTRODUCTION ..................................................................................................................... 1

II. RECEIVING DIGITAL CONFIDENTIAL INFORMATION FROM PROSPECTIVE CLIENTS .......... 1
   A. The Conflict Arising from Receipt of Confidences ................................................................. 1
   B. Are These Website Disclaimers Legally Necessary? .............................................................. 2
   C. Effective Process .................................................................................................................. 3
   D. Effective Substance .............................................................................................................. 4
   E. Model Language to Adapt to Your Jurisdiction and Practice .............................................. 5

III. INTENTIONAL DISCLOSURE THROUGH LAW FIRM NEWSLETTERS AND ARTICLES .......... 5

IV. RECEIPT AND DISCLOSURE OF DIGITAL CLIENT CONFIDENCES, CHATROOMS, BULLETIN
    BOARDS AND LISTSERVs ......................................................................................................... 6

V. AUTHORIZED ACCESS TO DIGITALLY STORED CLIENT CONFIDENCES ............................ 8
   A. Competent Electronic Storage of Client Data ......................................................................... 8
   B. Physical Security of Stored Client Data ................................................................................ 9
      1. Nonmobile Hardware ......................................................................................................... 9
      2. Mobile Technology ........................................................................................................... 9

VI. SECURITY OF NETWORK-ACCESSIBLE STORED CLIENT DATA ........................................ 10
   A. Information Stored on an Unprotected Website ...................................................................... 10
   B. Sharing Office Space ........................................................................................................... 11
   C. Storing Client Data with Application Service Providers ..................................................... 11

VII. UNAUTHORIZED ACCESS TO STORED CLIENT DATA ....................................................... 12
    A. Hacking, Viruses, and Spyware ............................................................................................ 12
    B. Wi-Fi Risks ......................................................................................................................... 13

VIII. METADATA: THE TRANSMISSION AND RECEIPT OF INVISIBLE
     CONFIDENTIAL INFORMATION ............................................................................................ 13
    A. What Metadata Is ................................................................................................................ 13
    B. The Available Means to Reduce Metadata ........................................................................ 14
    C. Adverse Use of Metadata: Unethical? ................................................................................ 14
    D. Conclusion ......................................................................................................................... 15
THE SPEED OF NORMAL: CONFLICTS, COMPETENCY, AND CONFIDENTIALITY IN THE DIGITAL AGE

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 each has 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 today be stored 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, the ease and speed of digital communications means that a conflict of interest can be created 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 who wanted 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 to make sure that undertaking the representation would not create a conflict of interest with an existing or former client. 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 from the prospective client necessary to check conflicts is obtained. 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 disqualify that entire firm to the same extent as if an attorney-client relationship had been consummated.

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.
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. In the digital age, there is less control over receipt of confidences, and greater opportunity for them to be received by firms. 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 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? 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. 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.

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. Others say that no attorney-client relationship will be formed by submitting the information.

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 good faith in an effort to hire the firm from relying on the confidentiality of the information to cause imputed disqualification.

For practical reasons, 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? 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

---

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.


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 Rule 1.10(a).

6 See, e.g., www.velaw.com (“any information sent to Vinson & Elkins … is on a non-confidential and non-privileged basis.”).


form attorney-client relationships and to keep submitted information confidential. On the one hand, 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. 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. 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. The Association of the Bar of the City of New York reached a similar conclusion. 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.

A California opinion reached essentially the same conclusion. 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.

Under this approach, lawyers who have websites need both to effectively disclaim any intention to form an attorney-client relationship and to effectively warn prospective clients of the lawyers’ intention not to hold transmitted information in confidence. 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.

C. Effective Process

If the lawyer has a website and is required to negate an intent to form a confidential attorney-client relationship, there are two levels that need to 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. 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. There is no assent by the prospective client. Courts in addressing web-contracts 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 agreed to are part of the agreement. In the leading case of Specht v. Netscape Communications Corp., 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. Instead, the user was merely asked to “please review” terms and conditions which included the arbitration clause. 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.

---

9 Id.
10 Id.
13 Id.
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. 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.
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).
The courts recognize that where the user affirmatively “clicks” agreement to the term – so-called “click wrap” agreement – the term could be enforced, but rejected attempt to create “browser wrap” agreements – binding users of a site merely because they opened it in their browser.21

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 confidentiality 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 e-mail.

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.22 Neither approach is satisfactory.

Disclaimers which state that any information will not be held in confidence are unhelpful because they go too far. 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.23 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. These “no confidentiality” provisions go too far.

On the other hand, 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 following an attorney-client relationship.24 It held the information could still be claimed as privileged, since the client had never explicitly agreed the information would not be held confidential. 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.25 The bar association concluded 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. 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.”26

Taken together, the decisions show that it is not enough to avoid an obligation of confidentiality by receiving confidential information with only a “no attorney-client relationship” disclaimer. If the firm uses an appropriately-worded “no confidentiality” approach, it avoids an obligation of confidentiality, but there then likely can be no 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 relationship27, 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

21 See generally, Jennifer Femminella, Online Terms and Conditions Agreements: Bound by the Web, 17 St. John’s Legal Comment 87 (2003).
22 Several firms have both statements. E.g., www.velaw.com.
24 Barton, supra.
26 Id.
27 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) (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.
party in the matter. Thus, the rule still requires firms to keep information confidential. It does not let the firm disclose to an adversary critical information disclosed by 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.

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 that 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.

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 articles or speeches written by firm attorneys. No doubt, firms perceive that this material makes the firm more marketable. They also serve 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 has already happened in the real world. A legal malpractice plaintiff alleged that her lawyer had failed to hire an expert for her 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.

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. Even so, 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 for her 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.

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. Even so, 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 for her 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.

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

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.

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.

See, e.g., www.kilpatrickstockton.com/publications/articles.aspx


28 Model Rule 1.18.

29 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.

30 See, e.g., www.kilpatrickstockton.com/publications/articles.aspx

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 to 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.  

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

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. 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 each allows 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 on, 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 cocktail party every single day of people who may be representing or consulting conflicting clients. Other listservs may have as participants opposing counsel or opposing parties. Again, it could be that on a daily basis, a lawyer on a listserv communicates with opposing parties discussing a subject matter that relates to the subject matter that interests them both.

A second difference is that the dialog is not ephemeral. What might be said at a cocktail party will not be recorded, and even an answer given in response to a question at 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.

---

33 http://www.elawyer.org/tools/practices.shtml
34 Putting the disclaimer in the article itself, as opposed to on the site, would also accomplish the same goal.
35 For example, one law review article quoted a post I had made to a listserv many 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
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 website, but that they should:

- Avoid giving advice concerning jurisdictions in which they were not licensed;
- Warning 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;”
- Stating where the lawyers were licensed (to avoid misleading the users into believing the lawyer lives in the state where the user resides);
- Stating, “clearly and specifically” that the lawyer did not want to create an attorney-client relationship with the user; and
- Warning not to post confidential information in their questions.37

In another opinion, the New Mexico Bar Association addressed various aspects of listservs and related technologies.38 In addition to focusing on some of the same issues as the North Carolina opinion, it emphasized the unique nature of the listserv:

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.39

These opinions suggest that lawyers who participate on listservs properly recognize the increased risk of creating attorney-client relationships with participants. They also suggest that merely posting disclaimers will not always be sufficient. Likewise, they suggest that an attorney consider the question of confidentiality before posting information -- and according to the New Mexico opinion, consider 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 email 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 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.”40

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

37 Id.
38 N.M. St. B. Ass’n Advisory Op. 2001-1 (2001)
39 Id. See also D.C. Bar Op. 316 (July 2002).
40 Id.
contacts with people that a lawyer knows is in need of legal services.41 The authorities so far have concluded that real-time communications over the Internet in a chat room constitute improper solicitations.42 Some states hold they are to be characterized as “telephonic communications”, while others hold they should be characterized as “in person” communications and so be subject to the most stringent ethical constraints.43 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 as to 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;
- be advised of the need to avoid creating conflicts;
- be warned not to improperly solicit prospective clients;
- and generally be aware that there is much unchartered territory in this area.

V. AUTHORIZED ACCESS TO DIGITALLY STORED CLIENT CONFIDENTIALITY

A. Competent Electronic Storage of Client Data.

Model Rule 1.15 requires lawyers to “appropriately safeguard[]” client files.44 Lawyers ethically may store files digitally.45 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. 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,”46 but backing up important client data plainly is something every lawyer ought to do.47

The details of a backup plan will vary. Putting a copy of critical client files onto a CD will help, but leaving the CD on the computer will accomplish nothing if there is 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.48

Second, the files must be secure. Where files are stored on Internet-accessible computers, critical security issues arise.49 Even files that are not network accessible may be viewed by third parties, such as computer maintenance companies. 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, but confidentiality agreements should be obtained:

A lawyer who gives a computer maintenance company access 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.50

In addition, lawyers should obtain “a written statement of the service provider’s assurance of confidentiality.”51 Permitting third parties access is not an ethical violation so long as the obligation of confidentiality is maintained.52

---

41 See Model Rule 7.1(b).
43 See id.
44 Model Rule 1.15(a).
47 See Jason Krause, Guarding the Cybefort 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.
48 Id. Lawyers should consider rotating tapes or CDs, for example. See Steven Atherton, Protecting Your Firm’s Critical Data 27 Vt. B. J. 17 (March 2001).
49 These are discussed infra, notes ___ to ___ and accompanying text.
51 Id.
52 See N.C. Eth. Op. 209 (Jan.12, 1996) (“[A] lawyer should store a client’s file in a secure location where client confidentiality can be maintained.”); N.Y. Eth. Op. 643 (Feb. 16, 1993) (“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. Eth. OP. RI-100 (Sept. 30, 1991) (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”).
For these reasons, lawyers should ensure that anyone who has access to stored client confidences should be required to have confidentiality obligations compatible with the lawyers’ own. \(^{53}\) Particularly because digitalization makes it easier for theft to occur, to occur without warning or indications it has occurred, and with greater consequences, greater care needs to be given when third parties are given access to digitized client confidences.

Third, lawyers must ensure legacy access. Over time, storage media becomes obsolete or degrades. For example, even CDs degrade over time. \(^{54}\) Storage technology can also become obsolete, so that data stored on media can no longer be readily accessed. 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. 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 losing unsaved data when the power goes out, it will ensure access to data at all times, so that, for example, court deadlines can be met. \(^{55}\)

**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. \(^{56}\) If someone can walk into the lobby of a law office and use an unattended PC to 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 as to allow access to client information. “Logging out” and using password access may be required any time the computer is left unattended, for example. Likewise, in areas where opposing counsel

   \(^{53}\) See Model Rule 5.3(b) (requiring lawyers who directly supervise nonlawyers exercise reasonable care to ensure the non lawyer’s conduct is compatible with the lawyer’s ethical obligations).


   \(^{56}\) The same obviously holds true for file rooms and other physical storage sites.

   (or third parties) have physical access to computers which contain or can access digitized client files, similar precautions are needed.

2. **Mobile Technology**

   Mobile technology creates even greater risks since client data leaves the relatively safe confines of the office. With today’s technology, more information can be stored 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. 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 of the metal detector, while his compatriot on the other side makes off with the computer, taking advantage of the distraction. \(^{57}\)

   There are also services that are designed to locate stolen laptops when they are later used by the thief to connect to the Internet. For example, one program is called “Stealth Signal.” \(^{58}\) According to the company’s website, after a computer is reported missing, the program secretly will contact the company with the computer’s location and will even allow the owner to delete files from the laptop. \(^{59}\) The site states that the software can not be removed or even detected. \(^{60}\) 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. \(^{61}\) Even greater protection through encryption programs is also available -- for individual files \(^{62}\) as well as entire

---


\(^{59}\) [http://www.computersecurity.com/stealth/computer_tracke‌‌‌r.htm](http://www.computersecurity.com/stealth/computer_tracker.htm)

\(^{60}\) Id.

\(^{61}\) In the “Save As” window in Word, click the “Tools” drop down and then go to “Security Options” to password protect a file.

\(^{62}\) Use the same steps noted in the note above, but encrypt the file.
sctors of hard drives.\textsuperscript{63} 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 \textit{ex parte} contacts with persons who are known to be represented by counsel in a matter.\textsuperscript{64} Is a visit to an opponent’s website during litigation a violation of such rules? Put the other 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.\textsuperscript{65} 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.\textsuperscript{66} 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 \textit{ex parte} contacts, websites are often interactive. The Oregon Bar Association distinguished between different degrees of interactivity:

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 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).\textsuperscript{67}

Thus, passively entering an opponent’s website does not implicate the rule against \textit{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 -- and it is important -- 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 \textit{knows} the person is represented.\textsuperscript{68} 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 \textit{Jorgensen v. Taco Bell Corp.},\textsuperscript{69} the court rejected even a “should have known” standard, stating:

\begin{quote}
Taco Bell's proposal has wide and troubling implications. Under it, counsel for the real world, then it was prohibited in digital one, too.


\textsuperscript{64} \textit{E.g.}, Model Rule 4.2.


\textsuperscript{66} \textit{Id.}

\textsuperscript{67} \textit{Id.}

\textsuperscript{68} See Model Rule 4.2.

\textsuperscript{69} 58 Cal. Rptr.2d 178 (Cal. 1996)
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 being 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 2100 [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. 70

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. 71 Because each does not owe an obligation of confidentiality to the other, it is important that physical client files be maintained in confidence. 72

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. 73 “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.” 74

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. 75 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. 76 Because they are strangers to the privilege, lawyers must ensure that these web-based companies comply with the ethical obligations of the lawyer. 77

---

70 Jorgensen, 58 Cal. Rptr.2d at 180
71 See generally, Rockas, Lawyers for Hire and Associations of Lawyers: Arrangements that are Changing the Way Law is Practiced, 40 Boston B. J. 8, 18 (Nov/Dec 1996).
73 D.C. Bar Legal Ethics Committee Opinion No. 303.
74 Id.
76 See generally, Carole Levitt, Application Service Providers are Gaining Acceptance, 24 L.A. Law. 56 (June 2001).
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 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. ASP employees are no different in that respect from computer consultants who have access to the firm’s own computer systems.

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.

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. 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. Only about one in ten used antivirus software, and one in five used firewalls. 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. A recent case provides an even more interesting example of the risks that hackers create to networked computers. In U.S. v. Steiger, a Turkish citizen posted a program that looked 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 as well as track every password the person used. Another recent virus locked up your files through encryption and required you to pay money to get them back.

Spyware is similar to a virus in that it can in some forms permit third parties to monitor web activities, email, and in some forms, file contents. Other forms of spyware gather passwords and personal information, or reset or hijack your browser.

In order to avoid becoming a zombie box or having the contents of a computer, web activities, and your 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. What firewalls do is protect your computer against intruders. A basic firewall will essentially hide the address of your computer from third parties and block “ports” on your PC from being used by them.

Essentially, antivirus software examines downloaded files and email attachments to identify and disarm known “malware” -- software that allows hackers to take control of a PC. For example, if you download a file from the Internet that contains a “Trojan Horse” like the kind in the Steiger case, the program will alert you and allow you 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

78 See generally, Andrew S. Breines, Security is key as ASPs Make Inroads into the Legal Market, 18 No. 4 GPSolo 24(June 2001).
79 See discussion, supra
80 See id. See also Carole Levitt, Application Service providers are Gaining Acceptance, 24 L.A. Lawyer 56 (June 2001).
81 See Jason Krause, Guarding the Cyberfort 89 A.B.A. J. 42 (July 2003).
82 See Jason Krause, Guarding the Cyberfort 89 A.B.A. J. 42 (July 2003).
83 See id.
84 See id.
85 By one estimate, attack zombies account for 80% of all spam. See http://www.whatpc.co.uk/vnunet/news/.2125121/zombie-pcs-generate-80-per-cent-spam 318 F.3d 1039 (11th Cir. 2003).
86 Id.
88 Id. See also Jason Krause, Beware of Spyware, A.B.A. J. 59 (June 2005).
89 There’s 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.
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. 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.91

Unfortunately, many antivirus software programs do not detect, let alone remove, spyware.92 Thus, special anti-spyware software which costs $30 to $40 must be used.93

B. Wi-Fi Risks.

The use of wireless technologies to communicate creates special risks. There are two distinct ways wi-fi can be used. With wi-fi, an “access point” is wired to the Internet, and laptops or desktops communicate by radio frequencies with the access point. It is much like a cordless phone base station and handset.

One way is as a means to create a wireless network within a law firm.94 The other way is if lawyers are outside the firm and use third party access points to connect to the Internet. Both circumstances create risks because there is a broadcast between the computer and the access point.95

When setting up a law firm network, the broadcast can be encrypted. 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 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.

VIII. METADATA: THE TRANSMISSION AND RECEIPT OF INVISIBLE CONFIDENTIAL INFORMATION

A. What Metadata Is.

Many documents created by software contain far more than the visible text.96 Documents written with Microsoft Word, for example, contain what is called “metadata” -- information about who wrote the document, when it was revised, by whom, and additional information. Likewise, documents saved with WordPerfect can be "unedited" through using multiple "undo" commands to reveal critical changes to a document. Excel creates similar issues.97

Microsoft goes on to explain that, "Metadata is created in a variety of ways in Word documents. As a result, there is no single method to remove all such content from your documents."98

91 Id.
92 See Nelson & Simek, supra, at 21.
93 Id.
95 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.
96 This section was written along with Robert R. Jueneman and originally appeared at legalethics.com.
97 A Microsoft support document explains the problems particular to Word:
Whenever you create, open, or save a document in Word 2002, the document may contain content that you may not want to share with others when you distribute the document electronically. This information is known as metadata. Metadata is used for a variety of purposes to enhance the editing, viewing, filing, and retrieval of Microsoft Office documents.
Some metadata is easily accessible through the Word user interface. Other metadata is only accessible through extraordinary means, such as by opening a document in a low-level binary file editor. The following are some examples of metadata that may be stored in your documents:
• Your name
• Your initials
• Your company or organization name
• The name of your computer
• The name of the network server or hard disk where you saved the document
• Other file properties and summary information
• Non-visible portions of embedded OLE objects
• The names of previous document authors
• Document revisions
• Document versions
• Template information
• Hidden text
• Comments
• Time spent editing the document
• File numbers, case numbers, etc.
98 Id.
Lawyers obviously have a duty to avoid disclosing information that could harm the client.\textsuperscript{99} Indeed, the ethical rules of most states is far broader, requiring lawyers to take reasonable steps to ensure that no information relating to the representation of a client is disclosed, absent the client’s consent.\textsuperscript{100}

B. The Available Means to Reduce Metadata

To comply with their duty of confidentiality, lawyers should take steps to remove metadata from documents exchanged with opposing counsel or disclosed to the public. However, this is not a one-click operation. As one commentator put it: “The problem is not that metadata is added to documents. The problem is that it cannot be easily removed from documents.”\textsuperscript{101}

There are various ways to remove metadata, all of unequal effectiveness.

C. Adverse Use of Metadata: Unethical?

Suppose now armed with this knowledge about the existence of metadata, you examine a Word document that opposing counsel has sent to you, and discover an abundance of metadata. Can you review it?

At least one bar association has taken the position that it is unethical to examine this hidden information.\textsuperscript{102} In that opinion, the bar association recognized that, although the transmitting party intended to transmit the "visible" document, "absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the 'hidden' material or information."\textsuperscript{103} Based on this premise - that the transmitting lawyer was unintentional in his disclosure of the meta data - the bar association concluded that the metadata could not be accessed: "it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets.” \textit{Id.}

While agreeing with the commendable “gentlemen do not read someone else’s mail” spirit of that doctrine, the technologist co-author disagrees with the implied premise that all metadata is merely an undesirable artifact, created by evil software companies as a trap for the unwary. Although the “trap of the unwary” is definitely something for counsel to worry about, the support for such metadata in the form of title, subject, keywords, author, company, and many other such information are included either to make the storing and retrieving of such documents in a large organization more feasible, and/or to simplify the editing and production of those documents.

The “fact” that counsel did not intend the lawyer to receive the ‘hidden’ information is therefore not at all obvious, since by exercising reasonable care the counsel would have reviewed and removed such material at her discretion. After all, we are not talking about opposing counsel using binary editors or other specialized forensic tools, any more than a consumer (as opposed to an art historian) would normally expect to use X-rays to reveal what mistakes an artist painted over. We are only expecting counsel to be reasonably familiar with the tools he or she uses every single day, if necessary by actually reading the manual or the Help files.

Whether the premise advocated by the N.Y. Bar holds true or is adopted by others is an interesting question, and one on which the authors of this section do not totally agree. The difficulty facing lawyers is that the proposition that lawyers have a duty to avoid using metadata will be tested in cases where, for example, the internal evidence contained in metadata clearly showed that the defendant had been aware of a particular fact at a much earlier date than the apparent date on the document. Counsel would presumably have a professional responsibility to discover that fact and make it known. A court would be sanctioning fraud were it to preclude use of metadata under those circumstances. Likewise, if the metadata showed that a document was amended after the date on which it had apparently concluded, that might also be highly relevant to a case, and difficult for a court to exclude.

Given the extraordinary measures being taken today to gather electronic evidence, the alleged ethical duty not to review metadata will be a factor in many cases involving electronic discovery.

For those reasons, whether an ethical duty will be recognized is an open question and not an easy one to predict. Clearly, even if there is such a duty, however, a lawyer would be free to argue to a court that protection over the metadata was waived by its disclosure. By approaching a court before unilaterally concluding that no ethical duty existed, a lawyer may best protect himself from accusations of unethical conduct, and yet zealously represent his client within the bounds of the law.

Even if there is an ethical prohibition against the misuse of metadata (and that may be a dubious proposition), lawyers must caution clients about such information when they are preparing a document or, later, transmitting it. As a practical matter, and even assuming that there is an ethical prohibition against using it, the ability to detect a violation of this rule is extremely low. How will you know that opposing counsel is gathering information about your drafting techniques, and so on?

\begin{itemize}
  \item \textsuperscript{99}See Model Rule 1.6.
  \item \textsuperscript{100}See id.
  \item \textsuperscript{102}N.Y. St. B. Ass’n. Op. 749 (Dec. 14, 2001).
  \item \textsuperscript{103}Id.
\end{itemize}
D. Conclusion

Understanding the presence of metadata and working to reduce its dissemination may reduce risk to you and your clients. On the other hand, metadata is not some kind of diabolical, arcane incunabula or form of secret writing, but in fact can be readily accessed using the same tools that lawyers use every day in the production of documents. Arguing that counsel has some ethical responsibility to wear blinders and not make use of such readily available tools information to assist their clients would seem to be shirking their professional duties.

Having said that, and appreciating the impact of a rule against review of metadata might have, on your own activities as a lawyer, in day to day practice and in the realm of e-discovery, attorneys might want to consider taking a proactive stance by informing opposing counsel that they reserve the right to use whatever readily available tools and techniques are available to examine any and all documents that are provided during discovery or negotiations.