An Ethical IP Lawyer Meets the Internet

David Hricik
Professor of law
Mercer University School of Law
Macon, GA

TABLE OF CONTENTS

I. Linking to and From Law Firm Websites

One benefit of the Internet is the ability to provide hypertext links ("links") from one web page to another. These links can take many forms, ranging from internal links within a law firm's website, to links from the law firm's site to those of third parties, to third party links to a firm's site.

Obviously, a link that only takes a visitor to a different page in a law firm website does not create additional issues beyond the fact that the linked-to page must comply with the same rules that apply to all pages of a firm website.[1] But, a link on a law firm website that takes a visitor from the law firm's website to websites that are either independently operated by a third party, or owned or controlled by the firm or an entity controlled by the firm, can create ethical issues. Similarly, independent third parties, and entities controlled by or affiliated with, the firm can also link to the firm's web page. A client, for example, who is particularly happy with a firm could post a link in a blog post extolling the virtues of the firm. Or, the firm could create a site that it controls, but which does not on its face appear to be a law firm website, that contains links to the law firm's website.

This Section identifies the ethical issues that arise when a firm links to other pages, as well as when other sites link to a firm's web page.[2]

A. Ethical Issues that Can Arise When a Third Party Links to a Law Firm Website

At the outset, it is important to emphasize that nothing in the disciplinary rules does, or can, regulate what a client or third party may put on its web site, or how the client may otherwise describe a lawyer. However, the rules govern not only the conduct of lawyers, but of efforts by lawyers to circumvent the rules through the acts of others.[3] Thus, a line exists between unilateral actions of a client or third party – which the lawyer is not responsible for – and those actions which the lawyer is responsible for, which includes acts that the lawyer induces

---

1 *See* S.Ct. Ohio Bd. of Comm'rs on Grievances & Discipline, Ohio Adv. Op. 2000-6 (Dec. 1, 2000).

2 Other issues can arise from linking. For example, if an attorney sends an otherwise innocuous email, but it contains a link to the attorney's firm, do the advertising rules and federal statutes concerning spam e-mail kick in? *See* William R. Denny, *Electronic Communications with Clients: Minding the Ethics Rules and the CAN-SPAM Act,* 62 Bench & B. Minn. 17, 21 (Dec. 2005) (concluding that if the primary purpose of inclusion of the link in the e-mail was "commercial," then the CAN SPAM act would apply, as would advertising provisions in the ethics rules).

3 *See* Model Rule 8.4(a) (stating that it is professional misconduct for a lawyer to "violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another.")

through third parties. Though somewhat easily stated, in the context of linking, the boundary is not always clear.

1. Bare Links with No Commentary are Proper, so Long as they are Not Referrals.

A simple descriptive link from a third party site to the law firm's site – *e.g.,* a link on a third party's page that, without payment from the lawyer or any other contact, simply says "click here to go to BakerBotts.com" – would not create any apparent issues if there is no comment made about the firm. Thus, for example, a client's placement of a firm's logo on its webpage would not constitute a violation of the ethics rules (assuming no payment or improper referral arrangement.)[4] At least where the link to the firm's site consists of nothing more than the law firm's name or logo and is truly placed by an independent party who gratuitously links to the firm's page, the authorities are recognizing that the lawyer is not subject to discipline.[5]

2. Difficult Questions Arise if the Third Party Makes Statements about the Firm that the Firm Itself Could not Make.

When the third party makes statements about the firm that the firm could not make itself – "Smith & Jones is the best and most reliable patent law firm in the universe, so click here to visit its site" – difficult issues can arise. While the Internet did not create the ability of third parties, such as clients, to make statements that a lawyer could not ethically make,[6] it certainly has increased the ease with which such statements can be made and, as a result, the difficulty that lawyers face in policing them, if policing they need do.

In part the whether content posted by a third party with a link to the firm's website (or not, for that matter) turns on whether the posting is truly that of a third

---

[4] S.Ct. Ohio Bd. of Comm'rs on Grievances & Discipline Op. No. 2004-7 (Aug. 6, 2004) ("Communication to the public of a law firm's name and logo on a business client's Web site is acceptable because it is not a false, fraudulent, misleading, deceptive, self-laudatory, or unfair statement."); Eth. & Prof. Resp. Comm. of the Cincinnati B. Ass'n Op. No. 96-97-01 (1997) ("A client of an attorney or law firm may list the attorney or law firm on the client's Internet Home Page and may provide a link to an attorney's or law firm's Home Page on the client's Internet Home Page if the attorney does not request the link and does not provide compensation or anything of value to the client in return for the client listing the attorney or law firm as their attorney or law firm and providing the link on the client's Internet Home Page.")

[5] *See* Ala. R. Prof. Conduct R. 7.4, cmt. ("This rule is not triggered merely because someone other than the lawyer gratuitously links to, or comments on, a lawyer's Internet web site.")

[6] *See generally,* Kathryn A. Thompson, *Client Web Sites and the Lawyer Ethics Rules: What Your Client Says About You Can Hurt You,* 16 Prof. Lawyer 1 (2005).

party, done unilaterally, or instead whether it is induced by the lawyer. This chapter now turns to that issue.

a. Is the Improper Commentary Posted by a Truly Independent Third Party, and not due to Inducement by the Lawyer?

A threshold question that any firm must address in analyzing the propriety of a third party linking with commentary to a firm website is whether in fact the linking website is not under the control of a law firm. Control can be direct or indirect, and may involve a question of degree.

Obviously, a firm that posts a link on a site with content that the firm could not place on its own site cannot avoid the strictures of the advertising rules by hiding the fact of control. What may to the public appear to be an arms' length statement of praise about a firm could instead be a self-serving misleading statement by the firm, for example. Hiding the fact that the lawyer is making the improper statement does not make it right.

Even if a firm does not literally control the content from the linking page, the firm could have a relationship with the third party site owner that could violate the rules. For example, although not controlling the linking site, the firm could be making an improper payment for the posting of the link.[7]

Even where there is no improper payment or referral arrangement, and even if the site is truly run by a third party and not the firm, questions can arise about whether a lawyer has any ethical obligation to act that, in most jurisdictions, there are as yet no clear answers. For example, a third party could make a statement on its website that clearly could not be made by the lawyer himself. For example, a client could make a statement that could constitute "false or misleading" information in terms of Model Rule 7.1. Or, an existing client could solicit additional clients to join a pending suit in which the firm represents the client and, in doing so, make statements that the lawyer could not make. Under these circumstances, does the lawyer have any responsibility?

In large measure the answer to that question turns on whether the lawyer has induced the third party to act; however, as noted below, it is not clear in some jurisdictions that it is limited to that circumstance.

Lawyers cannot, of course, violate the rules through the act of another. Thus, a lawyer cannot direct a third party to make a statement that the lawyer

---

[7] *See* Kathryn A. Thompson, *Client Web Sites and the Lawyer Ethics Rules: What Your Client Says About You can Hurt You,* 16 Prof. Lawyer 1 (2005) (discussing other issues, mostly related to improper referral fees). *See, e.g.,* Va. Jud. Eth. Adv. Comm. Op. A-0117 (Sept. 19, 2006) (discussing distinction between online directory and lawyer referral service); Oh. Adv. Op. 99-3 (June 4, 1999) (same).

could not himself make.[8] But control or the ability to direct the content is not required. Under Rule 8.4(a), the lawyer may not "induce" or "assist" in improper advertising.

These words connote questions of degree. A lawyer who obviously writes the content for the third party and directs its placement on the third party's website is responsible for the content because the lawyer clearly assisted the third party to post the information.[9] Because "inducement" and "assistance" are in some measure subjective, lawyers should be careful about even encouraging clients to post matter that violates the state ethics rules, for the reason that encouragement might be viewed as assisting or inducing the third party to violate the ethics rules.[10]

If a firm cooperates or works with a client or third party to establish the link, the law firm may be subject to the claim that it induced the third party. No doubt for that reasons, two bar associations have suggested that a law firm has an affirmative obligation to ensure that, at least with respect to postings by clients of the firm made in cooperation with the firm, that the postings comply with the ethical rules.[11] For example, the Pennsylvania Bar Association wrote that the lawyer "should review the website to insure that there is nothing on it that would constitute any other violation of the advertising Rules…."[12]

In sum, a lawyer clearly has no obligation to monitor the Internet for improper postings by third parties that relate to the lawyer's services. At the same time, if the lawyer works with the third party, the lawyer should be careful to ensure that, if the posting goes beyond a naked link to the firm's website, that the content comply with the lawyer advertising rules. Although the client is not subject to those rules, the lawyer runs the risk of being accused of "assisting" or "inducing" the violation.

B. What Should the Lawyer Do if a Third Party Unilaterally Posts Material that, if Posted by the Lawyer, Would Violate the Ethical Rules?

---

[8] *See* Model Rule 8.4(a) (stating that it is professional misconduct for a lawyer to "violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another.")

[9] *See* Model Rule 8.4(a).

[10] *See* S.Ct. Ohio Bd of Comm'rs on Grievances and Discipline Op. No. 2004-7 (Aug. 6, 2004) ("Lawyers should not encourage others" to make statements that violate the ethical rules).

[11] S.Ct. Ohio Bd of Comm'rs on Grievances and Discipline Op. No. 2004-7 (Aug. 6, 2004) (suggesting that lawyers should examine client web pages and counsel those clients whose commentary violates the advertising rules); Pa. B. Ass'n Comm. on Legal Eth. & Prof. Resp. 2007-13 (Dec. 2007) (same). These opinions are discussed more fully below.

[12] Pa. B. Ass'n Comm. on Legal Eth. & Prof. Resp. 2007-13 (Dec. 2007).

This is a difficult question, particularly if the third party is not a client of the lawyer. The bar opinions have addressed the question of what a lawyer must do if the website belongs to a client, but not when it belongs to a non-client. The answers under both circumstances are less than satisfactory.

1. Posts and Links by Clients

With respect to clients, both bar associations that have addressed the question have come to the same conclusion: the lawyer should "counsel" the client "about any omissions and advise the client about how the web page could be changed to comply with those rules."[13] If the client refuses to make the changes, the committees recommended that the lawyer "give serious consideration to withdrawal from representation to avoid any impression that the lawyer has authorized or adopted the client's continued use of the web page."[14]

While no doubt discussing the problem with the client may be advisable, whether a lawyer must withdraw from representing a client who, unilaterally, makes statements that are proper for the client to make, but unethical for the lawyer to make, seems a strained conclusion. After all, the client has a First Amendment right to make the statements, and the only reason the lawyer cannot make them is because he is subject to the lawyer advertising rules.

More pertinent here, it is difficult to see how the lawyer is violating Rule 8.4, since he did not ask the client to make the statement, and has asked the client to take down the offending statement. Such conduct cannot fairly be characterized as assisting or inducing the client to violate the ethical rules, and the suggestion that the lawyer may be viewed as "endorsing" the web page if it stays up over the lawyer's demand does not appear to violate any ethical rule: lawyers are not responsible for the unilateral acts of third parties. Further, there is no conflict between the lawyer and the client for the same reason: the lawyer cannot be held responsible for the client's action. Thus, while both bar associations suggested that withdrawal might be required, it is not clear other authorities would agree.

2. Posts and Links by Nonclients

When the third party is not a client, the issue becomes somewhat more complex. Model Rule 4.3 prevents a lawyer from engaging in certain conduct with respect to third parties. Specifically, that rule provides in full:

> In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the

---

[13] S.C. B. Op. 99-09 (1999); S.Ct. Ohio Bd of Comm'rs on Grievances and Discipline Op. No. 2004-7 (Aug. 6, 2004) (same).

[14] S.C. B. Op. 99-09 (1999); S.Ct. Ohio Bd of Comm'rs on Grievances and Discipline Op. No. 2004-7 (Aug. 6, 2004) (same).

> lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding. The lawyer shall not give legal advice to an unrepresented person, other than the advice to secure counsel, if the lawyer knows or reasonably should know that the interests of such a person are or have a reasonable possibility of being in conflict with the interests of the client.[15]

Under this rule and to the extent it applies (*e.g.,* there is not a multi-state matter involved, or the matter is not pending in many federal courts), the lawyer should be able to communicate with the non-client, since the communication is not in connection with dealing on behalf of a client, and the interests of the third party would not, absent unusual circumstances, be in possible conflict with the interests of the lawyer's client in some matter. But, some states have adopted broader versions of Rule 4.3, and so care should be given to make sure any required communication complies with applicable state rules.

If the third party refuses to change the web page, it would not seem the lawyer has to take any further action; there is no representation to withdraw from, for example.[16]

C. Links from the Lawyer's Site to Third Party Sites

There are a range of fact patterns that could implicate ethical rules where a lawyer links from his site to a site controlled or operated by a third party.

However, there are several concerns and limitations.

First, although there is no uniform rule,[17] prudence dictates that "[l]inks to outside sites should, of course, clearly indicate to the web browser that they are not maintained by the Law Firm."[18] There are several reasons for caution.

---

15 Model Rule 4.3

16 A somewhat related and interesting question is whether a law firm could post on its own web page a link to another firm's webpage and make statements about that other firm, gratuitously, but which would violate the rules if made by that other firm. In other words, must a lawyer abide by the advertising rules when he makes statements about another law firm's website? *See In re Moran,* 840 N.Y.S.2d 847 (N.Y. Sup. Ct. App. Div. 2007) (concluding that lawyer who posted link to disciplinary investigation of rival firm engaged in conduct that was prejudicial to the administration of justice and which adversely reflected on his fitness as a lawyer because disciplinary proceedings were confidential).

17 *See* Louise L. Hill, *Electronic Communications and the 2002 Revisions to the Model Rules,* 16 St. John's Legal Comment 529, 542 (2002) ("It is unclear whether lawyers are responsible for labeling linked material….").

18 Ass'n of the B. of N.Y.C. Comm. on Prof. & Jud. Eth Formal Op. No. 1998-2 (Dec. 21, 1998).

Foremost, the lawyer does not "control the completeness, accuracy, or timeliness of the content in the linked Internet sites."[19] In addition, without a disclaimer or other indication of lack of responsibility for the content of the linked to site, risk of negligent referral arise if the site is one to which the firm is referring prospective or actual clients.[20]

Second, the lawyer should not make it appear that a link from his website is to that of an independent third party when, in fact, the site linked to is controlled or owned by the lawyer. "Information on external sites to which links are provided from the lawyer's web site are not considered part of the lawyer's web site unless the external site is also controlled by the lawyer."[21] Thus, not only would it be deceptive for the lawyer to portray the linked to site as "independent," but the lawyer is responsible for ensuring that its content complies with the advertising rules.

Third, a lawyer cannot incorporate content even from an independent third party's website into his website – such as by quoting it or "framing" the content – if the content violates the lawyer advertising rules, such as by being false or misleading.[22]

Fourth, many states require lawyers to maintain copies or files of their websites. The only located opinion to have addressed the issue held that the lawyer did not need to maintain copies of sites belonging to third-parties and merely linked to from the lawyer's website.[23]

Fifth, it is doubtful that lawyers have an obligation to monitor third party sites that link to the lawyers site to ensure that they do not contain improper content. The "burden on lawyers to monitor the linked material would be an onerous one. If such material… can be updated and changed with relative ease, the obligation on the lawyer to keep abreast of changes to linked material could effectively eliminate the ability of a lawyer to link."[24]

---

19 J.T. Westermeier, *Ethics and the Internet,* 17 Geo. J. Legal Eth. 267, 308 (2004).

20 *Id.*

21 Utah St. B. Eth. Adv. Op. Comm. Op. No. 97-10, n.5 (Oct. 24, 1997).

22 *See* Donald R. Lundberg, *An Advertising Primer: Part 2,* 49 Res Gestae 32 (Nov. 2005), discussing *In re Philpot,* 820 N.E.2d 141 (Ind. 2005). According to Mr. Lundberg, executive secretary to the disciplinary commission in Indiana, the lawyer in *Philpot* "incorporated content from another Web site that the Court found to be deceptive and prejudicial to the administration of justice because it advocated that parents… in mediations lie and use improper tactics like making false demands." 49 Res Gestae at 32. It is not apparent from the reported decision, however, that this was the case.

23 Ass'n of the B. of N.Y.C. Comm. on Prof. & Jud. Eth Formal Op. No. 1998-2 (Dec. 21, 1998) ("We do not believe that Law firm need retain copies of the contents of outside sites linked to its web page.")

24 Louise L. Hill, *Electronic Communications and the 2002 Revisions to the Model Rules,* 16 St. John's Legal Comment 529, 542 (2002) ("It is unclear whether lawyers are responsible for labeling linked material….").

Sixth, and related to the foregoing, a lawyer who knows that a third party's site contains information that violates the ethical rules is at great risk if he links from his website to that site. Likewise, a lawyer cannot ask a third party to post material that would be improper for the lawyer to post himself. Although it is unlikely that lawyers have an obligation to monitor third party sites for improper content and to "demand" that they take down improper content, a lawyer who knowingly links to such improper content may be accused of circumventing the advertising rules.[25]

Seventh, and related to the prior to points, some bar associations have suggested that if the firm cooperates with the third party to establish the link, that the lawyer in fact does have an obligation to monitor the linked site to ensure that its content does not violate the lawyer advertising rules.[26]

D. Conclusion

Bar associations and disciplinary authorities are only beginning to address linking issues. Absent controlling authority in the jurisdiction, the obvious risk-averse path is to follow the most stringent view of the issues, or to seek an opinion from bar counsel as to the propriety of proposed conduct before undertaking it.

II. Social Networking Sites and The Ethical Issues they Create

A. What are Social Networking Sites?

If you are reading this section, you need to get out more; or perhaps others do. Social networking sites have become ubiquitous in professional and private lives as a means for people to connect with, reconnect with, and communicate with friends, family and fellow professionals. Each site is somewhat different in its approach and clientele, ranging from the "friend"-oriented Facebook site, to the entertainment-oriented MySpace, to the more business oriented LinkedIn and Plaxo sites, among others.

B. What Ethical Issues Arise from using Social Networking Sites?

1. Making False or Misleading Communications

---

[25] *See* Model Rule 8.4; Louise L. Hill, *Electronic Communications and the 2002 Revisions to the Model Rules,* 16 St. John's Legal Comment 529, 542 (2002) (analyzing this issue and describing the uncertainty around it).

[26] Pa. B. Ass'n Comm. on Legal Eth. & Prof. Resp. Op. No. 2007-13 (Dec. 2007) ("The Committee also cautions that since websites are advertising… the inquirer should review the website to insure that there is nothing on it that would constitute any other violation of the advertising rules… as regards his participation thereon.").

A. By the Lawyer

Lawyers are prohibited under most jurisdiction rules from making statements about their legal services that are false or misleading. It is important to recognize that this prohibition applies to all forms of communication in most states.[27] Thus, what a lawyer cannot put in an ad, he cannot put in an e-mail or blog post.[28]

Thus, a lawyer's "profile" or other published description may be deemed to run afoul of lawyer advertising rules. Obviously, this is less of a concern on facebook and other "social" sites than it is on LinkedIn, Avvo, and other sites, which tend to be more business-oriented. Lawyers should assume that if they are a member of one of these organizations with the purpose of obtaining business, that the information must comply with the lawyer advertising rules.

It is important to note that even the announcement on Facebook of a jury verdict could, conceivably at least, be deemed to violate the ethical rules of many states, since they prohibit lawyers from stating the results of a specific case without a disclaimer that the results will vary in each case, or similar language. It would not be proper to post that information on a firm web page, absent the disclaimers or other disclosures, and so a bar association might hold it is also improper to post it on a LinkedIn status update.

B. By Others About the Lawyer

As discussed above in the section concerning links to and from law firm websites, some opinions are requiring lawyers to ask those who post information about the lawyer that he himself could not ethically post to take the information down and, potentially if the post is made by a client, to withdraw from representing the client. Many social networking sites, such as LinkedIn, permit members to "recommend" others and praise their work. There is no principled reason why, if a state requires lawyers to prevent others from making false statements about the lawyer on a link to a firm webpage, that the lawyer should also not be required to undertake the same action with respect to these "recommendations."

One state bar association has already so held. Specifically, the South Carolina Bar Association stated:

---

[27] *E.g.*, Model Rule 7.1.

[28] *See, e.g.,* S.C. Ethics Advisory Op. 09-10 (2009) ("While mere participation in these websites [like LinkedIn and Avvo] is not unethical, all content in a claimed listing must conform to the detailed requirements of Rule 7.2(b)-(i) and must not be false, misleading, deceptive, or unfair.").

> Client comments may violate Rule 7.1 depending on their content. 7.1(d) prohibits testimonials, and 7.1(d) and (b) ordinarily also prohibit client endorsements. *See* Cmt. 1. In the Committee's view, a testimonial is a statement by a client or former client about an experience with the lawyer, whereas an endorsement is a more general recommendation or statement of approval of the lawyer. A lawyer should not solicit, nor allow publication of, testimonials. A lawyer should also not solicit, nor allow publication of, endorsements unless they are presented in a way that is not misleading nor likely to create unjustified expectations. "The inclusion of an appropriate disclaimer or qualifying language *may* preclude a finding that a statement is likely to create unjustified expectations or otherwise mislead a prospective client." Cmt. 3 (emphasis added).[29]

2. Improperly Soliciting Clients

Many social networking sites have various forms of synchronous and asynchronous forms of communication, such as in the former case e-mail like communication and in the latter, chatrooms. These create particular issues if used to solicit clients.

Courts generally view e-mail sent to prospective clients, which would seem most analogous to an "in-mail" or other asynchronous form of communication on some social networking sites as targeted mailings that must comply with the jurisdiction's rules concerning targeting mailing. Thus, a lawyer using "in-mail" on LinkedIn or Facebook's proprietary e-mail system would apparently need to comply with the advertising rules when soliciting clients.

There is less authority on whether synchronous communications, such as in chatrooms, is to be treated as targeted mailing or in-person solicitation, but the trend is to treat them as if they were in-person solicitations.[30] Care, of course, must be given if there is no controlling approach or if the prospective client is in another state: the lawyer's rules may not control.

And, of course, there are unpredictable variations that can arise, and the lack of controlling law.[31] Others have commented that "[c]ommunications sent to the profiles of prospective clients on social networking sites … could be considered a hybrid between e-mail solicitation and contemporaneous communications one would find in an Internet chat room, as members of the

---

[29] S.C. Ethics Advisory Op. 09-10 (2009).

[30] *See* Cydney Tune & Marley Degner, *Blogging and Social Networking: Current Legal Issues,* 962 PLI/Pat 113 (Apr. 2009).

[31] *See id.* (imagining a scenario where lawyer and prospective client happened to be logged onto a blog at the same time, and so essentially engage in synchronous commentary).

social networking sites have the capability to respond to messages more or less instantly."[32] The only clear lesson is to be thoughtful about the environment and recognize that real world rules apply in the virtual world of the Internet.

3. Engaging in the Unauthorized Practice of Law.

So far, the authority that exists in related contexts holds that merely answering a question at a CLE conference does not constitute the provision of legal advice. From that premise, and at least in a non-private exchange on a facebook page or other semi-public area, the provision of "generic" legal advice likely will not be deemed to be the practice of law. Normally, lawyers don't provide legal advice in public, and so generally many believe that an informed court will not hold that generic advice given in a relatively public forum will constitute "legal advice."

But if the lawyer goes beyond generic discussions of the law, or purports to provide state-specific (or federal-specific) answers to particularized questions, the risk of engaging in the unauthorized practice of law increases. Even so, however, most states do not prohibit the occasional provision of legal advice into the state, so long as the lawyer does not have a physical presence or provide systematic or continuous advice into the state. Thus, even if the lawyer gives legal advice, chances of the unauthorized practice of law occurring are slim.

The next section shows, however, that lawyers can create attorney-client relationships or relationships that, though falling short of fully-formed attorney-client relationships nonetheless create obligations of confidentiality that can disqualify the lawyer and, in some instances, his entire firm. In addition, malpractice liability is possible.

4. Inadvertently Creating Attorney-Client Relationships or Relationship that Can Disqualify The Lawyer and his Firm or Cause Malpractice Liability

It takes very little to create an attorney-client relationship, and lawyers are duties to prospective clients under some circumstances. Both issues are possibilities when communicating on social networking sites.

First, even absent an attorney-client relationship, courts have long recognized that an initial interview between a lawyer and a person who in good faith is seeking to hire the lawyer creates an obligation of confidentiality not unlike that which accompanies that of a former client. During the late 1980's and onward, many states either by rule, bar opinion, or judicial decision held that a person who, in a good faith effort to hire a lawyer, discloses confidential

---

[32] Maxwell E. Kautsch, *Attorney Advertising on the Web: Are We in Kansas Anymore?,* 78 J. Kan. B.A. 35 (Oct. 2009).

information to one lawyer in a firm can disqualify that entire firm essentially to the same extent as if an attorney-client relationship had been consummated.[33]

More recently, the ABA adopted Model Rule 1.18, which several states, but not all, have adopted. That rule in full provides:

> (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

---

[33] *See, e.g., Applehead Pictures LLC v. Perelman,* 2008 N.Y. Slip. Op. 07594 (Oct. 7, 2008) (exchange of email and informal breakfast did not establish confidential relationship to support disqualification); *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); *Bridge Prods., Inc. v. Quantum Chem. Corp.*, 1990 WL 70857 (N.D. Ill. 1990) (firm disqualified after a one-hour meeting with prospective client); A.B.A. Formal Eth. Op. 90-358 (1990); N.C. St. B. Formal Eth Op. 14 (Apr. 20, 2007); Del. Eth. Op. 1990-1 (1990); R.I. Eth. Op. 91-72 (1991); Vt. Eth. Op. 96-90 (1996); *B.F. Goodrich Co. v. Formosa Plastics Corp*., 638 F. Supp. 1050 (S.D. Tex. 1986); *Hughes v. Paine, Webber, Jackson & Curtis Inc*., 565 F. Supp. 663 (N.D. Ill. 1983); *INA Underwriters Ins. Co. v. Rubin*, 635 F. Supp. 1 (E.D. Pa. 1983). *See generally,* Susan Martyn, *Accidental Clients*, 33 Hofstra L. Rev. 913, 921-29 (2005); Kenneth D. Agran, *The Treacherous Path to the Diamond-studded Tiara: Ethical Dilemmas in Legal Beauty Contests*, Note, 9 Geo. J. Legal Ethics 1307 (1996); Debra Bassett Perschbacher & Rex R. Perschbacher, *Enter at Your Own Risk: The Initial Consultation & Conflicts of Interest*, 3 Geo. J. Legal Ethics 689 (1990).

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.

Thus, a lawyer who communicates about a matter with person who is seeking legal advice can "learn too much" and so become disqualified from representing the opposing party.[34] Potentially, the lawyer's entire firm can be disqualified.

If the lawyer gives advice, then liability arises. Two cases illustrate the ease with which advice can be given in the real world. The social networking world makes it even easier.

In the first, *Togstad v. Vesely, Otto, Miller & Keefe*,[35] Mrs. Togstad went to an attorney for legal advice, but was told she had no claim and relied on that advice in not bringing it. The court held that this advice created an attorney-client relationship. Later, she learned that in fact she had a claim, but it had become time-barred. Based on the testimony of the lawyer's own witness, ordinary care and diligence required the lawyer to inform Mrs. Togstad of the eventual running of the statute of limitations, and the jury found that the lawyer had failed to perform research that an ordinary prudent attorney would do before reaching the conclusion that he did. As a result, be careful in nonengagement letters to say that the client has no claim; inform the client, instead, that although you do not believe the claim is one that is worth your time and effort, another lawyer may disagree and that limitations is a concern and, if you know when it with certainty will run, let the person know that fact.

In the second, *Flatt v. Superior Court*,[36] a lawyer (Flatt) had a one-hour initial consultation with a prospective client, Daniel during which Daniel

---

[34] 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-DEC Md. B.J. 11, 12 (Nov/Dec. 2001).

[35] 291 N.W.2d 686 (Minn. 1980).

[36] 9 Cal. 4th 275 (1994).

disclosed confidential information about the alleged malpractice of his prior attorney, Hinkle. After hearing the story, Flatt advised Daniel that he definitely had a legal malpractice claim against Hinkle. However, Flatt learned through a conflicts check that her firm represented Hinkle's firm. Accordingly, Flatt advised Daniel that the firm could not represent him adverse to Hinkle's firm.

However, Flatt did not advise Daniel of the fact that his claim would become barred by the statute of limitations, or of the need to act promptly in seeking other counsel. Two years later, when Daniel finally did sue Hinkle, the statute of limitations had run. Daniel then sued Flatt for legal malpractice, arguing Flatt had breached a duty to advise Daniel to seek other counsel promptly.

The issue, then, was which duty "won:" the duty to advise a prospective client of limitations, or the duty of loyalty to a current client. The California Supreme Court held that the duty of undivided loyalty that Flatt's firm owed to Hinkle, the existing client, won out over the duty to advise Daniel of the statute of limitations.

Thus, care should be given when "advising" anyone through social networking sites, or random conversation or communication, of their legal rights. Your firm may not get paid for the advice, but may be accepting liability if it turns out to be inaccurate.

5. Other Ethical Issues

As noted above, lawyers have been admonished not to use deception when attempting to investigate on social networking sites. In addition, some ethical rules apply to even "non-lawyer" conduct. For example, a lawyer was reprimanded because he hid his real identity and posted as if he were a teacher a post on classmates.com that another teacher had engaged in sex with students.[37]

C. User Beware: Using Social Networking Sites Exposes Personal Information and Your Communications to Third Parties, Who May Disclose it to Others.

1. Protect Yourself

Recently, a lawyer blogged about an adverse ruling, and in doing so called the judge, an "Evil, Unfair Witch."[38] The Florida bar reprimanded him and fined him for the post. In another case, an Illinois lawyer lost her job of 19 years for posting to a blog about "Judge Clueless" and including thinly veiled descriptions

---

[37] *In re Carpenter,* 95 P.3d 203 (Or. 2004).

[38] John Schwartz, "A Legal Battle: Online Attitude vs. Rules of the Bar," New York Times (on-line ed. Sept. 13, 2009)

of pending matters.[39] And, of course, Judge Kozinski was investigated for having risqué photographs on a site that the public could access.[40]

As is explained more fully in the next section, if you have a profile – even a "private" profile – you may be giving access to opposing counsel or third parties to information you post, even without knowing it. Care needs to be given.

And, of course, employers are also monitoring and checking social networking sites when considering employment decisions, a fact which gives an entirely different but personally more important reason to be careful.[41]

2. Use Sites to Investigate Others

Social networking sites on their face seem "private" to some extent. That is, for example, on facebook your actual page is, unless you choose to make it publicly available, only viewable by those you "friend." However, there is a significant amount of information available to non-friends. For example, there is a "DLA Piper" group on facebook, which I freely joined and was able to identify some 430 members, and view their friends and gain some other additional information.

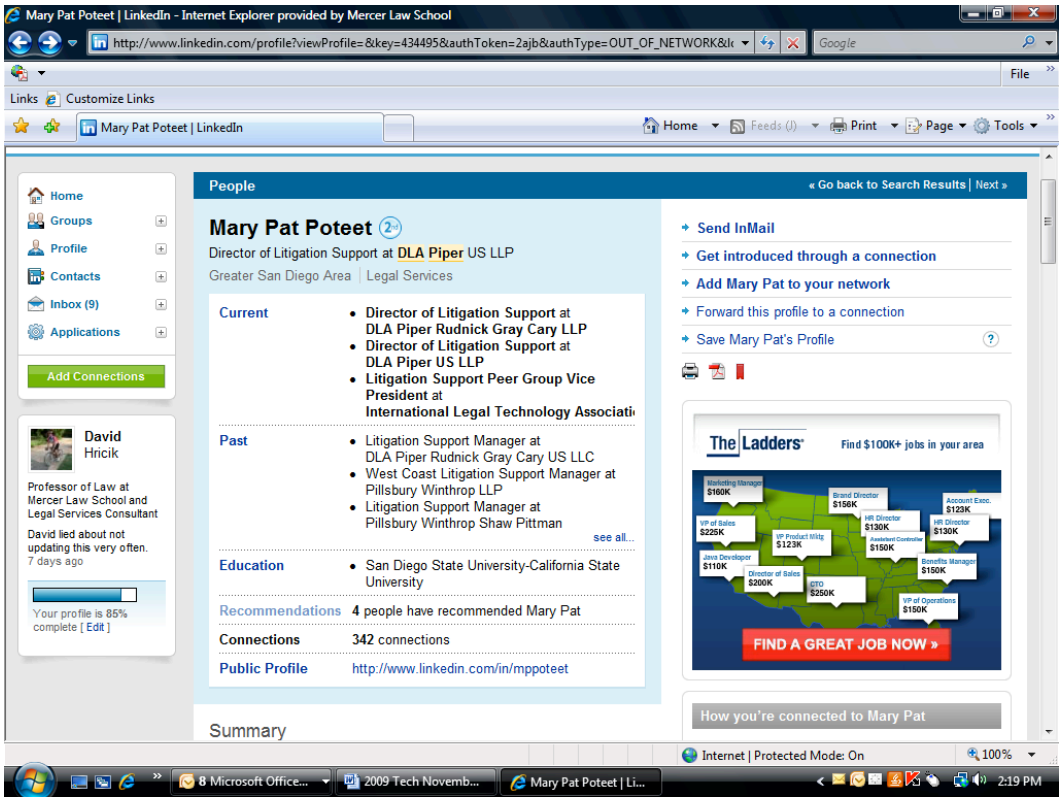
LinkedIn provides even more opportunities to learn about opposing counsel or potential witnesses or parties. For example, I ran an "advanced search" of "DLA Piper" and was able to view the complete profiles of anyone who popped up:

---

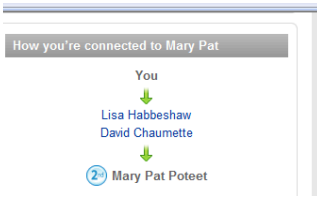
[39] *Id.* As of August, 2009, a complaint was pending against the attorney before the Hearing Board of the Illinois Attorney Registration and Disciplinary Commission.

[40] *Id.*

[41] Ian Byrnside, Note, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants,* 10 Vand. J. Ent. & Tech. L. 445 (Winter 2008); Dina Epstein, *Have I Been Googled?: Character and Fitness in the Age of Google, Facebook, and Youtube,* 21 Geo. J. Legal Ethics 715 (Summer 2008).



Based upon the circle next to her name, I realized I know someone who knows her, and I do:



Thus, had I wanted to find out even more information about Ms. Poteet, I could contact my friends and ask about her. You can use this tool about others; they can use it about you, your clients, and your witnesses and experts.

III. Unsolicited E-mail and Other Client Intake Concerns

In September 2008, the Virginia Bar Association released Legal Ethics Opinion No. 1842, which describes the obligations of lawyers who receive confidential information from law firm websites or through voicemail left by prospective clients. The committee addressed three separate scenarios

A. Voicemails from Prospective Clients.

With respect to voicemail, the bar association analyzed the question of whether a lawyer who was representing one defendant in a multi-defendant criminal matter was disqualified because he received an unsolicited voicemail from a co-defendant who, in good faith, was seeking representation in that same matter and which disclosed confidential information. The lawyer had a yellow page ad, but had not otherwise solicited prospective clients to leave confidential information on the voicemail. The bar association concluded the lawyer "was under no ethical obligation to maintain its confidentiality and further, may use the information in representing an adverse party."

B. E-mail from Prospective Clients.

With respect to e-mail, the bar association analyzed whether the firm could continue to represent the wife in a divorce proceeding even though it received an email from the husband, which disclosed confidential information. Again, the committee held there was no obligation of confidentiality simply because the lawyer had his e-mail address on the firm's web page. "The mere inclusion of an e-mail address on a web-page is not an agreement to consider formation of an attorney-client relationship…."[42]

However, the committee warned that "other factors" could give rise to an expectation of confidentiality, including "the specific nature and content of the invitation to contact the firm, including language in the advertisement or on the website that would imply the lawyer is agreeing to accept confidential information or an invitation in the lawyer's outgoing voicemail message asking the caller to provide as much detailed information about his/her case as possible."[43] (It is unclear whether the reference to "voicemail" should be to "web page," but that is what the opinion says.) But, absent these additional factors, no duty of confidentiality arose by simply having a web page with firm e-mail addresses.

C. Information Submitted through On-Line Forms

The third scenario the opinion addressed was the use by a firm of an on-line form for prospective clients to submit information. The committee was asked to address whether the firm could continue to represent a passenger when the driver of the car filled out the form and admitted having had several glasses of wine prior to the accident. The committee reasoned that because the firm invited submission of the information, the firm owed the sender a duty of confidentiality; thus, it had to withdraw from representing the driver since it could not disclose the confidential information to the driver, and thus was materially limited in its ability to represent the driver.

D. Recommendations

---

42 *Id.*

43 *Id.*

Despite generally finding no duty of confidentiality absent additional circumstances, the bar association concluded:

> [T]o avoid any inference that an attorney-client relationship has been established or that the information a prospective client provides will be kept confidential, a law firm may wish to consider the inclusion of a disclaimer on the website or external voicemail warning the person to not disclose confidential or sensitive information. The website disclaimer might also state, for example, that no attorney-client relationship is being formed when a prospective client submits information and that the firm has no duty to maintain as confidential any information submitted. The disclaimer should be clearly worded so as to overcome a reasonable belief on the part of the prospective client that the information will be maintained as confidential. In addition, the Committee recommends the use of a "click-through"(aka "click-wrap") disclaimer, which requires the prospective client to assent to the terms of the disclaimer before being permitted to submit the information.[44]

IV. Adventures in E-mail

A. Misdirected E-mail

1. It Still Happens to the Best of Us

Misdirected emails have made headlines, and no doubt many others go unreported or unnoticed by the sending lawyer.[45] Some recent headlines:

- **High-Profile Skadden Litigator Goofs, Sends Private E-mail to Reporters**[46]

---

[44] Id. citing David Hricik, To Whom it May Concern: Using Disclaimers to Avoid Disqualification by Receipt of Unsolicited E-mail from Prospective Clients, 16 Prof. Lawyer (2005).

[45] *See also Vithlani v. McMahon,* 2008 WL 2843524 (Ct. App. Cal. July 24, 2008) (lawyer submitted emails to court to support his motion for summary judgment that were from client and which disclosed attorney-client privileged information).

[46] http://www.abajournal.com/weekly/high_profile_skadden_litigator_goofs_sends_private_e_mail_to_reporters

- **Lilly's $1 Billion E-Mailstrom: A secret memo meant for a colleague lands in a Times reporter's in-box**[47]

- **Misdirected E-Mail Set the Stage for Clear Channel Suits**[48]

The only response to these issues is to be extremely careful when responding to email (reply to all can have a radically different result than reply, for example), and to forwarding it, particularly where the names are common and so misdirection is more likely.

Finally, inclusion of a "this e-mail is privileged" legend or disclaimer remains of questionable value, at least where it is indiscriminately used. In *dicta,* one judge recently noted as follows: "[M]ost law firms and corporate and government legal departments include this warning on all of their emails as a matter of course. This does not mean, however, that all of the information contained in those emails is confidential, or has continued to remain confidential."[49]

2. Mobile Lawyers and Privilege Waiver

A misdirected email can cause embarrassment and problem as common sense and the headlines above show. It can also implicate the privilege, because in some states even an unintentional disclosure can waive privilege. Lawyers who practice in those states obviously must take that into account.

A new case raises another possibility: suppose a lawyer from a "reasonable steps" state reads an email while, say, in an airport in a "strict waiver" state and accidentally forwards it to opposing counsel, not his client. Which state's law applies?

A recent case addressed choice of law, though it was not confronted with the strict/reasonable approach. In *Delta Financial Corp. v. Morrison*,[50] the e-mails involved "boorish" and "colorful" language that, sadly, was deleted by the

---

[47] http://www.portfolio.com/news-markets/top-5/2008/02/05/Eli-Lilly-E-Mail-to-New-York-Times?TID=st092007ab

[48] http://abajournal.com/news/misdirected_e_mail_set_the_stage_for_clear_channel_suits/

[49] *Commonwealth of Pa. Dep't. of Public Welfare v. U.S.,* 2006 WL 3792628, *22 (W.D. Pa. Dec. 21, 2006).

[50] 831 N.Y.S.2d 352 (N.Y. Sup. Ct. Oct. 24, 2006).

court prior to publication of its opinion. It's not hard to guess at what they might have said, however, because of the facts. A client wrote to an e-mail complaining of conduct of opposing counsel in discovery; the lawyer wrote the colorful e-mail but then sent it not to the client, but directly to opposing counsel. It did not describe opposing counsel as merely uncooperative, it is fair to assume. Once the sending lawyer realized his mistake, he immediately asked that the email be "destroyed," but opposing counsel argued that privilege had been waived over it.

The case is worth special note not because of its resolution – the court analyzed whether the email was privileged and was clearly inadvertently sent (it was, since it began with salutation to the client not opposing counsel and included, along with the colorful language, some legal advice), but for the choice of law issue and for its implications for mobile lawyers: the client and recipient were based in New York, but the lawyer had been in South Carolina on vacation when he actually opened the e-mail. The court held that South Carolina law applied to the questions of privilege and waiver because of New York court's approach to choice of law in privilege issues.

The iceberg under the water here is this: in some states, any waiver – no matter how inadvertent – waives privilege. As a result, it could be that, if South Carolina had been a "strict waiver" state, the mere fact of misdirecting the e-mail while in Hilton Head could vitiate privilege! While that circumstance did not arise here (South Carolina was a "no waiver so long as reasonable steps are taken" state), it could happen any time a lawyer misdirects an e-mail while in one of these strict-waiver states.

The problem for lawyers is that there is no uniform approach and, because of the general unavailability of appellate review, often no circuit-wide answer to this question. Instead, "the question is under what circumstances, if any, an inadvertent disclosure of privileged communications constitutes a waiver of the privilege. Courts across the country approach this question in any of three different ways."[51] Somewhat oversimplified, the three approaches are:

> a. The 'never waived' approach, which is that a disclosure that is merely negligent can never effect a waiver;
>
> b. The 'strict accountability' rule, which is that disclosure automatically effects a waiver regardless of the intent or inadvertence of the privilege holder; and
>
> C. The 'middle test' in which waiver is decided by consideration of (1) the reasonableness of the precautions taken to prevent inadvertent disclosure, (2) the amount of time it took the producing party to recognize its error, (3) the scope of the

[51] *Amgen Inc. v. Hoechst Marion Roussel, Inc.,* 190 F.R.D. 287, 290 (D.Mass.2000).

production, (4) the extent of the inadvertent disclosure, and (5) the overriding interest of fairness and justice."

Turner v. Brave River Solutions, Inc., 2003 WL 21418540 (D.N.H. June 18, 2003). Plan your travel plans accordingly!

B. Ensuring Client Confidentiality

It is now seemingly settled that lawyers can communicate with clients using e-mail to the extent that a reasonable expectations of confidentiality exists even though, at least theoretically, a third party could view the email while in transit. Sending the email will not, in other words, waive any privilege subsisting in the contents while the e-mail is in transit.

But issues are not too far below the surface. For example, some monitoring techniques have been held not to amount to "searches" within the meaning of the Fourth Amendment.[52]

And there are plenty of ways that email causes problems with confidentiality as to the contents. One recent case turned in significant measure on the difficult issues that arise when e-mails contain both legal and business advice, as is more often likely to happen with email, given its informal nature, than with a formal memoranda, where in-house counsel is more likely to be cognizant of the principle that only "primarily legal" communications are protected. *See In re Vioxx Products Liability Litig.,* 501 F. Supp.2d 789 (E.D. La. 2007) (providing a detailed analysis of the privilege and applying it to thousands of e-mails and other documents).

But there are other risks points, including in particular the ability of third parties to access the email. Several fact patterns are arising, with differing results and approaches, as the following section shows.

---

[52] *See, e.g., United States v. Forrester*, 512 F.3d 500, 509-11 (9th Cir. 2008) (government's monitoring of only the "to" and "from" addresses of e-mail messages, the Internet Protocol addresses of the web sites visited, and the total volume of data transmitted to and from an individual's e-mail account was comparable to pen register at issue in Smith and was not a search subject to Fourth Amendment); *Quon v. Arch Wireless Operating Co.,* 529 F.3d 892 (9th Cir. 2008) (no confidentiality over "to" and "from" of text message). *See also United States v. King*, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (no Fourth Amendment search had occurred where the claimant had connected to shared military network in which everyone on the network had access to all of his files and was able to observe them, just as the government investigator did); *Guest v. Leis*, 255 F.3d 325, 333, 335-36 (6th Cir. 2001) (monitoring of group electronic bulletin boards did not amount to search under Fourth Amendment); *United States v. Stults*, 2007 WL 4284721, *1 (D. Neb. Dec. 3, 2007) (finding that defendant did not have a reasonable expectation of privacy in computer files that were shared with and accessible to all users of a computer network), *aff'd.,* ___ F.3d __, 2009 WL 2476695 (8th Cir. Aug. 14, 2009).

1. Employers' Computers

b. The Cases

A number of courts have addressed the question of whether an employee can claim privilege over email communications sent from the employee while using the employer's computer where the employer had in place a policy that admonished the employee that computers were monitored by the employee and there was no confidentiality. The cases reach different results depending largely upon the wording of the policy and whether the employee had clear notice of it.

The Western District of Virginia weighed in on this issue when applying federal privilege law.[53] In *Sprenger v. Rector and Board of Visitors of Va. Tech.,*[54] a woman sued Virginia Tech alleging it did not accommodate her migraine headaches. The defendant sought production of emails on the woman's husband's work computer that related to the case. Although recognizing that the attorney-client privilege was not identical to the spousal communication privilege, the court relied upon and summarized the recent cases on whether the husband could still claim the communications were confidential even though they were sent from his workplace computer, which was subject to a "no privacy" policy. Specifically, the policy stated that "no user should have any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by use of the Commonwealth's equipment and/or access" and that state agencies had the right to monitor e-mail sent or received by agency users, such as her husband. It also stated that monitoring could occur "at any time, without notice, and without the user's permission." Finally, the policy did not allow work computers to be used for personal use.

The question for the court was whether to quash the subpoena. The court provided a useful summary of existing case law on this issue:

> Whether e-mails that are sent to or from a work e-mail account using a work computer are privileged is an issue of first impression in the Fourth Circuit. The Southern District of New York has addressed the matter in *United States v. Etkin,* and held that, in light of the employer's computer use policy, defendant could not claim the marital communications privilege. No. 07-CR-913, 2008 WL 482281 (S.D. N.Y. Feb. 20, 2008). Defendant, an employee of the New York State Police ("NYSP") moved to preclude introduction of an e-mail at trial which was sent using his government-issued e-mail account, asserting the marital communication privilege. *Id.* at *1. In *Etkin,* the defendant was

[53] State constitutions may afford broader privacy protections. *See State v. Reid,* 914 A.2d 310 (Super. Ct. N.J. 2007) (stating that, unlike most states, New Jersey's constitution recognized a right to "informational privacy").

[54] 2008 WL 2465236 (W.D. Va. June 17, 2008).

notified of the NYSP's computer policy every time he logged in to his computer. *Id.* at *3. The log-in screen notified the defendant that by logging in, he accepted the terms of the notification, which provided for the monitoring of the computers and further notified users that they had no legitimate expectation of privacy in any use of the computers. *Id.* The court was particularly persuaded by the flash-screen warning in holding that any expectation that his e-mail to his wife would remain confidential was "entirely unreasonable" and therefore, the communication was not confidential. *Id.* at *5.

The court in *Etkin* also relied on decisions by Seventh and Ninth Circuits which held that marital communications taking place while one of the spouses was incarcerated are not privileged because the spouses knew that prison officials could monitor their communications. *See United States v. Griffin,* 440 F.3d 1138 (9th Cir. 2006); *United States v. Madoch,* 149 F.3d 596 (7th Cir. 1998). The underlying message in these cases was that "there can be no confidential communication where spouses are on actual or constructive notice that their communications may be overheard, read, or otherwise monitored by third parties." *Etkin,* 2008 WL 482281 at *3 n. 5.

The attorney-client privilege is similar to the marital communications privilege in that its basis lies in encouraging "full and frank communication between attorneys and their clients." *Upjohn Co. v. United States,* 449 U.S. 383, 389 (1981). Courts have analyzed the confidentiality of e- mails and documents sent from work computers in applying the attorney-client privilege. Two federal courts have examined this issue. *See Curto v. Med. World Commc'ns, Inc.,* 2006 WL 1318387 (E.D.N.Y.2006) (holding the privilege was not destroyed by e-mails sent from a work computer when employee worked at home and employer had no means to monitor activity on the computer); *In Re Asia Global Crossing, Ltd.,* 322 B.R. 247 (Bankr.S.D.N.Y.2005). In *Asia Global,* the court laid out four factors to consider to measure the employee's expectation of privacy in his computer use

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies.

In that case, Asia Global did not appear to have a formal policy regarding use of computers and e-mail. On that basis, the court

ruled that the use of the work e-mail to communicate with a personal attorney did not destroy the attorney-client privilege.

Asia Global and *Etkin* both looked toward the Fourth Amendment reasonable expectation of privacy standard to determine the reasonableness of intent that the communication remain confidential. Recognizing that the "question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable," the court in *Asia Global* expressly equated the question to whether there was an objectively reasonable expectation of privacy. *Asia Global,* 322 B.R. at 258.

Many federal cases involving Fourth Amendment reasonable expectation of privacy and computers take place in the environment of the workplace. In *O'Connor v. Ortega,* 480 U.S. 709 (1987), the Supreme Court held that public employees did have Fourth Amendment rights in their offices, but that their reasonable expectations of privacy could be "reduced by virtue of actual office practices and procedures, or by legitimate regulation." *Id* . at 717.Because of the many different types of public work environments, the Court noted that questions of public employees' reasonable expectation of privacy should be addressed on a case-by-case basis. *Id.* at 718.

The Fourth Circuit has held that a public employee has no reasonable expectation of privacy in his internet use in light of the employer's computer use policy. *United States v. Simons,* 206 F.3d 392, 398 (4th Cir.2000). The defendant in *Simons* worked for the Federal Bureau of Information Services ("FBIS"), a division of the Central Intelligence Agency. *Id.* at 395.FBIS had a policy which "clearly stated that the FBIS would 'audit, inspect, and/or monitor' employees' use of the Internet, including all file transfers, all websites visited and all e-mail messages." *Id.* at 398.The policy further restricted use strictly to official government business. *Id.* at 395. Even if the defendant had a subjective expectation of privacy, this expectation was not objectively reasonable considering FBIS' policies. *Id.* It is unclear whether the FBIS policy was presented in the same flash-screen warnings as the court in *Etkin* found so convincing, but the court in *Simons* does note that the defendant did not contend that "he was unaware of, or that he had not consented to, the Internet policy." *Id.* at 399 n. 8.

In two very similar cases to *Etkin* involving computers with flash-screen warnings and Fourth Amendment rights, courts held that defendants had no reasonable expectation of privacy in their work computers. *See United States v. Angevine,* 281 F.3d 1130

> (10th Cir.2002) (upholding a seizure of a state-owned computer because defendant had no reasonable expectation of privacy in the computer in light of flash-screen warning); *United States v. Bailey,* 272 F.Supp.2d 822 (D.Neb.2003) (holding that defendant had no reasonable expectation of privacy in his work computer because he consented to a flash-screen warning every time he used the computer). The Seventh Circuit has also held that an employee had no reasonable expectation of privacy after the employer had announced that it could inspect laptops which were lent to employees. *Muick v. Glenayre Elecs.,* 280 F.3d 741 (7th Cir.2002).
>
> The Second and Fifth Circuits have held on particular facts that employees did have a reasonable expectation of privacy in their office computers. *See Leventhal v. Knapek,* 266 F.3d 64, 73 (2nd Cir.2001) (employer only had an anti-theft policy prohibiting use of computers for personal business and computers were subjected to "infrequent and selective search[es] for maintenance purposes"); *United States v. Slanina,* 283 F.3d 670, 676 (5th Cir.2002) (employer did not have a policy notifying employees that computers were monitored). The Court of Appeals for the Armed Forces has also held that an employee had a reasonable expectation of privacy in her work computer even though there was a flash screen warning at log-in. *United States v. Long,* 64 M.J. 57, 64 (C.A.A.F.2006). The court distinguished *Simons* on the basis that the policy in *Simons* was "very specific," restricted use to official business, and notified the user that the system was subject to inspection. *Id.* at 65.The log-on banner in Long also omitted the notification that users had no expectation of privacy in use of the system. *Id.* All these factors added up to a qualification of defendant's privacy expectation in her e-mails, but not an elimination of an objectively reasonable expectation of privacy. *Id.*[55]

The court held the communications remained privilege – the defendant had not established that the privilege had been waived, reasoning:

> Under the factors laid out in *Asia Global,* the court only has facts to meet one of the factors, that personal use of the work computer is allowed. While the Policy was tendered to the court, no affidavit or other evidence was offered as to knowledge, implementation, or enforcement of the Policy. There is no showing that Mr. or Mrs. Sprenger were notified of the Policy by a log-on banner, flash screen, or employee handbook and whether Mr. or Mrs. Sprenger were ever actually aware of the Policy. It is unclear whether third parties had a right of access to the e-mails. The

[55] *Id.*

> record also does not show whether the Policy was regularly enforced and whether the state employees' computer use was actually monitored. Given the nature of the martial communications involved, the burden is on the defendants to demonstrate that the privilege has been waived. *See Blau v. United States,* 340 U.S. 333-34 (1951) (holding that defendant had not overcome the presumption that marital communications are privileged). Based on the exceedingly thin record that exists at this time, defendants have not met this burden. Accordingly, the motion to quash the WWRC subpoena is hereby **GRANTED.** If defendants wish to pursue this matter further, they shall contact the Clerk of the Court to set up an evidentiary hearing on the issue of waiver.[56]

c. The Response from Employers

The clear lessons from the cases are several. First, is to ensure that the employer has a policy that clearly explains that confidentiality does not exist, even as to communications between the employee and his lawyer involving a dispute with the employer. Second, is to ensure that the policy is enforced and is not merely some "paper" policy or some amorphous practice that the employer may never actually use. Finally, third, is to ensure that there is proof that the employee has notice of the policy. Seemingly the best way to accomplish this is through log-in "splash screens" or warnings that the user must click through each time the user accesses the employer's computer.

One thing that may be important to explain to the employee is that to the extent the employer has unrestricted access to files, it also has the authority to consent to government search of those files.[57]

---

[56] *Id. See also Brown-Criscuolo v. Wolfe,* 601 F. Supp.2d 441 (D. Conn. 2009) (employee had reasonable expectation of privacy based on policy in place) *Mason v. ILS Technologies, LLC,* 2008 WL 731557 (W.D.N.C. Feb. 29, 2008) (e-mailing employee lacked knowledge of policy and so could claim attorney-client privilege); *Long v. Marubeni Am. Corp.,* 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006) (employee could not claim privilege; employee prepared handbook that had "no confidentiality" policy in it). *See generally,* Merri A Baldwin et al., *Ethical Aspects of Privacy and Information Security for Lawyers,* PLI Order No. 19129 (June 2009) (collecting cases). *But cf. Quon v. Arch Wireless Operating Co.,* 529 F.3d 892 (9th Cir. 2008) (even though employer policy stated text messages were not confidential, and even though they were likely "public records" under state law, because informal policy was not to review messages, sender of text message had reasonable expectation of privacy).

[57] *See U.S. v. Andrus,* 483 F.3d 711 (10th Cir. 2007) (father could consent to search of his 51-year old son's computer for child pornography even though it was located in son's bedroom)

d. The Response from Employees' Lawyers

Obviously, any time a lawyer is communicating with a client the lawyer should admonish the client not to use an employer's computer. The lack of confidentiality would seemingly impact not just the ability of the employee to claim privilege against the employer in a dispute, but as against the world. It may be prudent, at least until the law settles, for lawyers to advise individual clients never to communicate from their places of employment, as a result.

2. Spouse's Computers

Where the spousal privilege is recognized, there would not appear to be loss of privilege with respect to disputes between one spouse and a third party where the spouse in litigation uses the other spouse's personal computer to communicate by email. However, where the dispute is between the spouses, obvious care needs to be taken, as both a practical and legal matter.[58]

3. Significant Other's Computers

An interesting and probably fairly common fact pattern arose in *Geer v. Gilman Corp*.[59] There, a woman used her boyfriend's computer to email her lawyer about an employment dispute. In addition, she had him provide some edits and other input into her communications. The court recognized that, if the couple had been married, then the spousal privilege would apply, but that it was clear that the spousal privilege did not apply to pre-marital communications.

Nonetheless, the court held the communications confidential, reasoning:

> Given the facts of this case, the Magistrate Judge finds that plaintiff's attorney-client privilege in communications with her counsel was not waived by virtue of her having used her fiance's computer and e-mail address, by having him review and edit limited documents she prepared for her attorney, and by having him copy and deliver documents to plaintiff's counsel. As both plaintiff and Bourne have averred, plaintiff

---

[58] *Cf. United States v. Buckner*, 407 F.Supp.2d 777, 779-81 (W.D. Va. 2006) (defendant had a reasonable expectation of privacy in password-protected computer files, but search was valid because defendant's wife had a legitimate, substantial interest in all aspects of the computer sufficient to validate her unrestricted consent to search and so had apparent, but not actual, authority to consent to search), *aff'd,* 473 F.3d 551 (4th Cir. 2007). *See also Trulock v. Freeh,* 275 F.3d 391, 403 (4th Cir. 2001) (Fourth Amendment rights were violated where FBI searched claimant's password-protected computer files based on his roommate's consent; roommate had authority to consent to the search of shared computer but not of claimant's password-protected files); *United States v. Barth*, 26 F.Supp.2d 929, 936-37 (W.D.Tex.1998) (defendant manifested a reasonable expectation of privacy in data placed in files on his hard drive and did not waive Fourth Amendment protection by granting limited access to computer repair person).

[59] 2007 WL 1423752 (D. Conn. Feb. 12, 2007)

> requested that these communications remain confidential, and were, in fact, kept confidential; thus plaintiff took affirmative steps to maintain the confidentiality of the attorney-client communications. Moreover, the limited number of communications to which Bourne potentially had access on his computer or e-mail, or which he reviewed, do not constitute "any significant part of the communication" between plaintiff and her counsel…. Bourne can be considered an "agent" of plaintiff, because by providing his computer and e-mail to plaintiff, he became a "conduit" for plaintiff's communications with her attorney….. [P]laintiff and Bourne maintained an extremely close relationship, dating continuously since December 2004 and having become engaged in June 2005, with plaintiff clearly spending some time at Bourne's residence. The result obviously would have been different if plaintiff were a college student, sharing a summer sublet with three other college students, casually sharing laptops and e-mails as needed.[60]

4. Partial Access Issues

In all of the above fact-patterns, a recurring fact pattern involves a computer that is jointly used, and the person granting consent to the search has unrestricted access to only some files on the computer, while other files are password protected by the other user. The circuits that have addressed this issue have held that a person with only partial unrestricted access may not consent to search of the password protected files.[61] On the other hand, to the extent each joint user shares access to the computer's files, either one can consent to a search of the whole computer. [62]

5. Yahoo Email on Employers' Computers

This is a fascinating case: *Nat'l Economic Research Assocs., Inc. v. Evans, LECG Corp.*[63] The plaintiff moved to compel production of emails from one of the defendants sent by him to his attorney. The plaintiff-employer argued that the defendant-former employee had waived the privilege because he used his employer-owned computer in communicating. However, he had not used "outlook" or the employee-given software, but instead had gone on line to yahoo and used his yahoo email account. Unbeknownst to him, however, "all the information that is accessed is copied via a 'screen shot' onto a temporary Internet

---

60 *Id.* (citations omitted). *See Antonelli v. Sherrow,* 246 Fed. Appx. 381 (7th Cir. 2007) (before going to prison, plaintiff gave his computer to his ex-wife so she and his children could use it while he was incarcerated; court found that she had "joint access to and control of the computer generally" and so could consent to its search).

61 *See Antonelli v. Sherrow,* 246 Fed. Appx. 381 (7th Cir. 2007).

62 *U.S. v. Morgan,* 483 F.3d 711, 719-22 (10th Cir. 2007); *U.S. v. Morgan,* 435 F.3d 660, 663-64 (6th Cir. 2006).

63 21 Mass. L. Rptr. 337 (Mass. Super. Ct. Aug. 3, 2006).

file on that computer's hard drive. Therefore, each of the attorney-client communications… that were sent or retrieved… were stored in the hard drive of that laptop even though [defendant] never sought to copy any of these e-mails onto his hard disk or forward them to his Intranet [*i.e.,* employer-owned] e-mail address." *Id.* Using specialized software, and not just a browser, a computer forensic expert was able to extract these attorney-client communications.

The employer-defendant had a "no confidentiality" policy in place in a policy manual that stated, among other things, that deleted email in the ordinary course of business could be retrieved. It then stated:

> Any e-mail or voice mail sent or Internet site visited using Company resources is a reflection on the Company. Misuse of these resources can result in damage to the Company's reputation and even legal action. *The personal use of e-mail, the Internet and telephones should be kept to a minimum* for both productivity and financial reasons. All computer resources are the property of the Company. *To the extent permitted by law and any applicable agreements, the Company may, from time to time and at its discretion, review any information sent or stored using these resources. Be aware that e-mails are not confidential and the Company may read them during routine checks.*[64]

Elsewhere, employees were instructed:

- NERA does permit the use of Internet resources (dedicated or via dial-up) for personal use provided such use results in personal time savings that can be (at least partially) applied toward work.... Please note that all Internet access is logged by user and the logs are archived for at least 30 days. We do not make a habit of prying but any misuse of Internet resources can be easily traced.

- A log may be kept of users' network activities to monitor network usage. This may include logins, Internet sites visited, and electronic mail sent or received and telephonic and voice-mail usage.

- At times, it may be necessary for computer or law enforcement personnel to monitor network traffic or desktop activities, including electronic mail.[65]

Despite these fairly robust warnings, the court held that the yahoo-based e-mails were still protected with a reasonable expectation of confidentiality, but it also explained how an employer could vitiate any expectation of confidentiality over this form of "ghost" email:

---

64 *Id*. (emph. added).

65 *Id.*

Based on the warnings furnished in the Manual, Evans could not reasonably expect to communicate in confidence with his private attorney if Evans e-mailed his attorney using his NERA e-mail address through the NERA Intranet, because the Manual plainly warned Evans that e-mails on the network could be read by NERA network administrators. The Manual, however, did not expressly declare that it would monitor the *content* of Internet communications. Rather, it simply declared that NERA would monitor the Internet *sites* visited. Most importantly, the Manual did not expressly declare, or even implicitly suggest, that NERA would monitor the content of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer. Nor did NERA warn its employees that the content of such Internet e-mail communications is stored on the hard disk of a NERA-issued computer and therefore capable of being read by NERA.

NERA contends that any reasonable person would have known that the hard disk of a computer makes a "screen shot" of all it sees, which the computer then stores in a temporary file, including e-mails retrieved from a private password-protected e-mail account on the Internet. NERA further contends that any reasonable person would have known that these temporary files, although not readily accessible to the average user, may be located and retrieved by a forensic computer expert. This Court does not agree that any reasonable person would have known this information. Certainly, until this motion, this Court did not know of the routine storing of "screen shots" from private Internet e-mail accounts on a computer's hard disk. Moreover, this Court notes that the American Bar Association issued its Formal Ethics Opinion 99-413 on March 10, 1999, entitled "Protecting the Confidentiality of Unencrypted E- Mail," which outlined the various ways in which e- mails may potentially be seen by third parties, but nonetheless concluded that "lawyers have a reasonable expectation of privacy when communicating by e- mail maintained by an [on-line service provider]," such as Yahoo. The ABA Ethics Opinion did not even mention the possibility that such e-mails may be seen by anyone with access to the computer by examining the "screen shot" temporary file on the hard disk. Since a reasonable person in Evans' position would not have recognized that e-mail communications with his private attorney made from a private Internet e-mail account could be read by NERA simply by examining the hard disk of his NERA laptop, he cannot reasonably have understood that these attorney-client communications could be "overheard" by NERA. Therefore, this Court finds that these

attorney-client communications are protected by the attorney-client privilege.

> Evans has not waived this privilege.... He did not engage in these attorney-client communications through the NERA Intranet but through his private, password-protected Yahoo e-mail account that he accessed through the Internet. He did not forward these communications to his Intranet e-mail address or save and store them as Word or Wordperfect documents in his My Documents (or equivalent) file on the NERA laptop. He attempted to delete all personal documents on his NERA laptop before returning it, and even ran a "disk defragmenter" program in an attempt to ensure that these personal documents could not be retrieved. The totality of these efforts are "adequate steps" to protect the confidentiality of his privileged communications with his Nutter attorney.
>
> If NERA's position were to prevail, it would be extremely difficult for company employees who travel on business to engage in privileged e-mailed conversations with their attorneys. If they used the company laptop to send or receive any e-mails, the e-mails would not be privileged because the "screen shot" temporary file could be accessed by the company. If they used the hotel computer to avoid this risk, the communication would still not be privileged because the hotel could access the temporary file on its computer. Pragmatically, a traveling employee could have privileged e-mail conversations with his attorney only by bringing two computers on the trip-the company's and his own. NERA's attorney at the hearing appeared to recognize the impracticality of this consequence by arguing that the employee would still enjoy the privilege with respect to attorney-client conversations he reasonably believed the company would not be interested in reading. This attempted limitation is equally impractical, because a client should know *before* speaking with his attorney whether the conversation will be privileged. The client-employee cannot reasonably be expected to foresee whether the anticipated conversation would, at some time in the future, be of interest to the company or whether the conversation might stray into areas of company interest.[66]

The court then explained "that, if an employer wishes to read an employee's attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company's Intranet, the employer must plainly communicate to the employee that:

---

[66] Id.

> 1. all such e-mails are stored on the hard disk of the company's computer in a "screen shot" temporary file; and
>
> 2. the company expressly reserves the right to retrieve those temporary files and read them.

Id.

6. Gmail on Anyone's Computer

Google's gmail system scans email and places content-oriented ads in the email. This raises the question of whether third-party "access" by Google's computers vitiates confidentiality. The New York State Bar Association concluded that it did not.[67] It wrote:

> We would reach the opposite conclusion if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission (or a lawful judicial order). Merely scanning the content of e-mails by computer to generate computer advertising, however, does not pose a threat to client confidentiality, because the practice does not increase the risk of others obtaining knowledge of the e-mails or access to the e-mails' content. A lawyer must exercise due care in selecting an e- mail service provider to ensure that its policies and stated practices protect client confidentiality. Unless the lawyer learns information suggesting that the provider is materially departing from conventional privacy policies or is using the information it obtains by computer-scanning of e- mails for a purpose that, unlike computer-generated advertising, puts confidentiality at risk, the use of such e- mail services comports with DR 4-101.[68]

7. The Related issue of Files in File Sharing Arrangement

Persons who use "lime wire" and other P2P file sharing systems have generally been found to lack any reasonable expectation of privacy over files shared over such systems, since by definition those files are available to third parties.[69]

V. Informal Investigations and the Internet

---

[67] N.Y. St. B. Ass'n. Comm. Prof. Eth. Op. 820 (Feb. 8, 2008).

[68] *Id.*

[69] *See U.S. v. Stults,* __ F.3d __, 2009 WL 2476695 (8th Cir. Aug. 14, 2009) (collecting numerous cases).

A. Using Deception to Gain Access to a Facebook Page

The degree to which lawyers may, if ever, use "deception" to uncover wrong-doing is a complex issue that implicates the wording of several ethical rules as well as their purpose and underpinnings. *See* Va. Legal Eth. Op. No. 1845 (June 2009) (concluding that, like government lawyers, members of the Virginia State Bar who are charged with uncovering the unauthorized practice of law may use false names to ferret out wrong-doing due to a "government lawyer" exception to the general principle that deception is improper).

A Pennsylvania bar opinion recently addressed this issue in the context of Facebook, the popular social-networking site. Pa. Eth. Op. 2009-02 (March 2009). The inquirer was a lawyer who had deposed a woman who stated in her deposition that she had a facebook page. The lawyer believed the page would reveal information that he could use to impeach her testimony. Knowing, however, that she would not "friend" him on facebook, he proposed to have an assistant use a fake name and hope to gain access to her page, and to then provide the information to him, which he would then use at trial to impeach her.

The Pennsylvania bar association briskly said no to his request, labeling his plan "deceptive." It reached this conclusion even assuming she let every other person who asked to be her friend onto her page: "Even if, by allowing virtually all would-be 'friends' onto her FaceBook… pages, the witness is exposing herself to risks like that [identifying information that is disclosed to the world], excusing deceit on that basis would be improper. Deception is deception, regardless of the victim's wariness in her interactions on the internet and susceptibility to being deceived."[70]

On a related note, and although I could locate no reported cases, lawyers should take note that communicating in cyberspace is regulated by rules regarding lawyer advertising. Improper real-time solicitation and the unauthorized practice of law are potential dangers. Treating facebook, texting, and other forms of communication as if they did not "count" or were ephemeral is simply misguided.

B. Just Gathering Evidence from a Website May be Unethical

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.[71] It recognized that the digital nature of the contact was irrelevant: if the contact was prohibited in the

---

70 *Id.*

71 Oregon St. B. Ass'n. Op. No. 2001-164 (Jan. 2001).

real world, then it was prohibited in digital one, too.[72] 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:

> 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 witnessed 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

---

72 *Id.*

be answered by someone other than Lawyer B's client (or, if the client is a corporation, someone deemed represented).[73]

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 -- 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. *See* below. 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,[74] the contact should be proper.

C. Reliability of Information on the Internet

One district court recently observed that, "While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation…. [A]nyone can put anything on the Internet."[75] Care and caution are required in evaluating information found on the Internet before it is used in Court. No one knows you're a dog on the Internet.

D. Judges and Facebook and Google

Although slightly off topic, in a recent bar opinion from North Carolina, a judge was reprimanded for having communications with defense counsel, during trial, on his facebook page, where the two were "friends." The judge also "Googled" the plaintiff, and admitted that what he found influenced his opinion of the plaintiff. As a result, the judge was reprimanded.[76]

VI. Tracking: It's Worse Than You Think

Many people believe that deleting "cookies" generally denies websites the ability to track and gather personal information through browsing. According to a recent article in Wired magazine, however, more than half of the Internet's top

---

[73] *Id.*

[74] Model Rule 4.2 provides in full: "In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order."

[75] *St. Clair v. Johnny's Oyster & Shrimp, Inc.,* 76 F.Supp.2d 773, 774-75 (S.D. Tex. 1999).

[76] Jinny M. Ray, *Rules Struggle to Catch up with Technology,* 10 For the Def. 72 (Oct. 2009).

websites use a tracking capability built into Adobe's Flash plug-in that allows the sites to track users and store information about them.[77]

[77] Ryan Singel, *You Deleted Your Cookies? Think Again* (Aug. 2009), available at www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/