LEGAL ETHICS IN THE DIGITAL AGE

Susan David deMaine
Ruth Lilly Law Library
Indiana University Robert H. McKinney School of Law
October 31, 2012

INTRODUCTION: MOBILE TECHNOLOGY, CLOUD COMPUTING, AND GLOBALIZATION.

We all know – because we are told every day – that technology is changing rapidly. In fact, it is changing more rapidly all the time. With the changes come many choices about how we do our work, many of which can be mind-numbing, overwhelming, or downright befuddling. As lawyers, we try to keep up. We have to understand the changes in technology in order to advise our clients and run our firms. This understanding includes a thorough grounding in the ethical implications that arise when information is created, stored, and shared digitally and the precautions that we have to take.

It used to be that a lawyer could lock a file cabinet or a local computer and be reasonably sure that confidential information was secure. But all that has changed as our computers go with us everywhere, using software that exists elsewhere, sending bits of data around the world. It has become the norm to be able to work anywhere, accessing and editing the same documents no matter where we are.

Some mobility was possible before through local and firm-wide networks, but cloud computing has ramped up mobility seemingly overnight. The term "cloud computing" is used to refer to the use of software or data storage on computers that are located somewhere else and belong to someone else. Most of us use cloud computing without realizing it: Gmail, YouTube, Pandora, Facebook, Flickr, LinkedIn, Netflix. All these are cloud-based services. You do not need any software other than an up-to-date Internet browser to use them, and the data you generate is not stored on your local computer. It is stored in the cloud.

Another easy-to-understand example is word processing software. If you want to use Microsoft Word, you have to buy the software and install it on your computer. When you save a document, you save it to your local hard drive or maybe a firm-owned server. It may be difficult to get to from any other computer. When the software needs updating, you have to get and install the update. If you want to use cloud-based word processing software, you don't need to install anything. Just point your web browser to the address and start a document. When you save it, it is saved in the cloud and will be accessible from any device that can browse the internet.

In addition to instant updates and limitless mobility, cloud computing lets you quickly use as much or as little computing power and data storage as you need. Rather than having to

buy and set up new servers, you just buy more space from a cloud service provider. Or use less, if your needs diminish. It's faster and less expensive.[1]

Now we see law firm management software beginning to shift to the cloud.[2] As with other cloud computing software, this means increased mobility, greater connectivity, easy updates and expansion, and presumably lower IT costs. As we move our firms' data and documents to the cloud, what risks do we need to anticipate? What concerns regarding privacy and confidentiality do we need to consider and address beforehand?

First, let's look at what laws regarding privacy currently exist and what might be in the pipeline.

CURRENT AND UPCOMING ONLINE PRIVACY LAWS AND THEIR EFFECT ON LEGAL PRACTICE

Privacy laws generally incorporate a number of principles based on concerns that we have about our personal information.

- **Notice:** Individual should receive notice about the information being collected and its intended uses.
- **Choice:** Individuals should have a choice about the collection and use of their information.
- **Access & Correction:** Individuals should be able to access the information held about them and correct any errors.
- **Onward Transfer Limitations:** Individuals should be able to set limits on the sharing of the data.
- **Integrity:** Data should be protected against corruption and be relevant to the purpose for which it was collected.
- **Security & Confidentiality:** Data should be protected against intentional or accidental unauthorized disclosure, misuse, unauthorized access, or tampering.
- **Accountability/Enforcement:** Businesses that collect or store data should provide enforcement mechanisms to see that these principles are upheld and be held accountable for breaches of these principles. [3]

In the United States, we currently have a number of federal privacy laws, some of which are more or less relevant to running a practice depending on the kind of work you do. These include:

- Dodd-Frank Act[4] and the Bureau of Consumer Financial Protection;[5]

---

[1] For more information on cloud computing, see Nicole Black, CLOUD COMPUTING FOR LAWYERS (2012).
[2] Cloud-based law firm management software, like cloud-based email or word processing, is a type of cloud computing called SaaS or Software as a Service. You may also run across PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). PaaS offers cloud-based software development programs, and IaaS offers access to virtual hardware/storage.
[3] Andrew B. Serwin et al., PRIVACY, SECURITY AND INFORMATION MANAGEMENT: AN OVERVIEW 10-11 (2011).
[4] 12 U.S.C. § 5301 *et seq*.
[5] 12 U.S.C. § 5491 *et seq*.

- Electronic Communications Privacy Act, which covers interception review of both electronic and wire communications;[6]
- Gramm-Leach-Bliley Act, which governs nonpublic personal information held by financial institutions; [7]
- HIPAA, which governs health information;[8]
- HITECH Act, which imposes obligations in addition to HIPAA regarding health information;[9]
- Computer Fraud and Abuse Act, which provides criminal and civil remedies when system has been hacked or info has otherwise been stolen/misused;
- CAN-SPAM, which controls email marketing;[10]
- Right to Financial Privacy Act;[11]
- Fair Credit Reporting Act;[12]
- Fair and Accurate Credit Transactions Act of 2003;[13]
- Communications Decency Act;[14]
- Digital Millennium Copyright Act;[15]
- COPPA (Children's Online Privacy Protection Act);[16]

Notably, the Federal Trade Commission has tried to argue that law firms should be included in the definition of "financial institution" and therefore be subject to the Gramm-Leach-Bliley Act or GLBA. The GLBA protects the privacy of individuals' nonpublic personal information (NPI) held by financial institutions. It has been held that law firms are not included in this definition and are not subject to the GLBA.[17]

Nonetheless, law firms may still be expected to comply with the spirit of the GLBA. In *New York State Bar Ass'n v. F.T.C.*,[18] the ABA argued that law firms' obligations under the Model Rules of Professional Conduct were essentially the same as those of the GLBA.[19] The GLBA attempts to ensure security and confidentiality of NPI, protect against anticipated threats or hazards that might breach security of this data, and protect against unauthorized access or use. Financial institutions must implement a comprehensive security plan that covers (1) identification and assessment of risks; (2) development of written policies and procedures to manage these risks; (3) execution and testing of the plan; and (4) adjustments according to outcomes.

---

[6] 18 U.S.C. §§ 2510–22, 2701–12.
[7] 15 U.S.C. §§ 6801–09.
[8] 42 U.S.C. §§ 1320d–1320d-8.
[9] 42 U.S.C. § 300kk.
[10] 15 U.S.C. §§ 7701 *et seq.*
[11] 15 U.S.C. §§ 3401 *et seq.*
[12] 15 U.S.C. § 1681(a)–(b).
[13] 15 U.S.C. §§ 1681 *et seq*.
[14] 47 U.S.C. § 231.
[15] 17 U.S.C. § 512.
[16] 15 U.S.C. § 6501 *et seq*.
[17] See, e.g., *Am. Bar Ass'n v. F.T.C.*, 430 F.3d 457 (D.C. Cir. 2005).
[18] *New York State Bar Ass'n v. F.T.C.*, 276 F. Supp. 2d 110 (D.D.C. 2003).
[19] See *Privacy in Focus: Court Rules that Lawyers Are not Subject to Gramm-Leach-Bliley Act*, May 2004, http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=4&id=2657 (last visited Oct. 30, 2012).

More recently, a number of information privacy bills introduced in the 112th Congress most of them relating to identity theft and notification of security breaches. None became law, but it is an indication of what is on the Congressional radar terms of future privacy laws.

With law practices taking on greater global reach all the time, it is important to note that EU laws regarding data collection and protection are much more stringent than law in the U.S. The data protection directives of the EU grant greater protection to end-user data. U.S. companies that handle data regarding EU citizens or even store data on computers located in the EU must comply or they may find their data unavailable to them.

We also have to be aware of state laws. Virtually all states now require notification in the event of a data security breach. Many also have laws governing the disposal of personal information. Some also impose minimum security standards, privacy notices, and protection of Social Security numbers.

In all of this discussion, it is necessary to ask what information must be protected. The information covered by these many laws is not the same as the information considered confidential in the context of the attorney-client relationship, though there may be considerable overlap. Although the definitions of protected information vary across the laws mentioned above, the FTC has used a broad definition in its enforcement actions that is particularly useful in guiding law firms.[20] For example, in the consent decree in an enforcement action against Dave and Buster's Inc., personal information was defined as:

> individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license number; (g) a credit card or debit card account number; (h) a persistent identifier, such as a customer number held in "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information that is combined with any of (a) through (h) above.[21]

Every day, law firms handle this kind of information about their clients, opposing parties, expert witnesses, employees, and other individuals. Not only must law firms abide by the laws regulating this information, but as the ABA noted in its argument in *New York State Bar Ass'n v. F.T.C.*, lawyers also have an ethical duty to protect certain data as well.

ABA ETHICS GUIDELINES FOR ATTORNEY USE OF THE INTERNET

[20] Lisa J. Sotto et al., *Law Firms Face Risks in Handling Personal Information*, http://www.redteamusa.com/PDF/Lawyer%20info/LawFirmsFaceRisksHandlingPersonalInformation%20%28HuntonWilliams%29.pdf (last visited Oct. 31, 2012).

[21] Agreement Containing Consent Order, *In re Dave and Buster's Inc.*, No. 0823153 (F.T.C. March 25, 2010) (available at http://www.ftc.gov/os/caselist/0823153/100325davebustersagree.pdf).

In August 2012, the ABA House of Delegates voted to amend several of the Model Rules of Professional Conduct to reflect changes in technology since 2002. The amendments take into account changes in legal practice such as cloud computing, social media, global outsourcing, and frequent relocation. These amendments had been studied at length before being recommended by the Commission on Ethics 20/20 and are only the first set of recommendations the Commission on Ethics 20/20 expects to present to the House of Delegates. Further recommendations are expected in 2013.

Which rules did these amendments affect?

- Rule 1.0 Terminology (n), Comment 9.
- Rule 1.1 Competence, Comments 6-8.
- Rule 1.4 Communication, Comment 4.
- Rule 1.6 Confidentiality of Information (b)(7) & (c), Comments 13, 14, 18, 19 plus others renumbered.
- Rule 1.17 Sale of Law Practice, Comment 7.
- Rule 1.18 Duties to Prospective Client (a), (b), Comments 1-5.
- Rule 4.4 Respect for Rights of Third Persons (b), Comments 2-3.
- Rule 5.3 Responsibilities Regarding Nonlawyer Assistants, Comments 1-4.
- Rule 5.5 Unauthorized Practice of Law; Multijurisdictional Practice of Law (d), Comments 1, 4, 18, 21.
- Rule 7.1 Communications Concerning a Lawyer's Services, Comment 3.
- Rule 7.2 Advertising, Comments 1-7.
- Rule 7.3 Solicitation of Clients (note new name!) (a)-(c), Comments 1-9.
- New Rule: Practice Pending Admission

What did the changes do?

Technology and Confidentiality

- Rule 1.6: Clarifies that a lawyer has a duty to take reasonable measures to protect confidential client information from "inadvertent or unauthorized disclosure and unauthorized access, regardless of the medium used." The Comments now specify certain factors that a lawyer must consider to be sure their efforts to protect confidential information are reasonable. It does not, however, impose any kind of strict liability for inadvertent disclosures.
- Rule 4.4: Adds "electronically stored information" to that which will trigger the notice requirements that apply when a lawyer receives information relating to representation that are sent inadvertently.
    - Further clarification of "inadvertently sent" may be coming.
- Rule 1.0: Expands the definition of "writing" beyond email to include all "electronic information." The Comment on the term "screened" now clarifies that restrictions on sharing information within a firm apply to both tangible and electronic information.
- Rule 1.1: Requires lawyers to keep up to date in their understanding of the uses, benefits, and risks of technology as it relates to client confidentiality.

- Rule 1.4: Changes comment [4] to require prompt responses to client communications rather than just telephone calls.

Technology and Client Development

- Rule 1.18: Changes the word "discusses" to "consults" and "learned information from" in an attempt to clarify that new online communications can allow an attorney-prospective client relationship to exist before a traditional "discussion" takes place, triggering the need to protect any confidential information. The changes to the comments give more guidance as to when a consultation has occurred.
- Rule 7.2: Internet-based client development tools challenge the boundaries of the prohibition against paying for recommendations. The changes to this rule attempt to clarify that a lawyer can use online client development tools (pay-per-lead or pay-per-click) as long as the tools do not give the impression that the lawyer's professional qualities are being endorsed, that the inquirer's legal issues are being analyzed, or that the lawyer is being listed for no charge.
- Rule 7.3: Clarifies that a "solicitation" is directed toward a specific person and is reasonably understood to be an offer of legal services. Lawyers can use web browser banner ads, a website, a blog, and email (because it is no real-time). They can also respond to requests for information and have their "communications" returned to searchers in automatically-generated Internet searches.

Outsourcing

- Rule 1.1: New comments identify what a lawyer must consider when contracting with lawyers in another firm to assist with the representation of a client: circumstances, experience, education, reputation, nature of the services, and ethical requirements and protections. Changes to comments also stress need for lawyers to keep abreast of advances in technology and how they affect the practice of law and law firm management.
- Rule 5.3: Lawyers must make reasonable efforts to ensure that non-lawyers outside the firm provide their services is such a way as to comport with the ethical requirements placed on the lawyer. This is perhaps going to arise most often with the protection of client information. Also, if the client directs the attorney to use a particular non-lawyer service provided, the attorney must consult with the client as to how monitoring responsibilities are to be shared.
- Rule 5.5: Comment 1 clarifies that a lawyer cannot use the assistance of outside firms or other service providers in such a way that the other firms/providers would be engaging in the unauthorized practice of law.

Admission to the Bar

- Practice Pending Admission: This is a new rule that allows a relocating attorney to practice in a new jurisdiction for up to 365 days while applying for admission in that jurisdiction.

- Admission by Motion: For admission by motion the required time spent in practice is reduced to three years out of the last five, but this three years cannot include the 365 days of practice pending admission.

Detection of Conflicts

- Rule 1.6: Recognizes the increased employment mobility of attorneys. Allows the exchange of certain categories of confidential information (that which does not compromise the attorney-client relationship or otherwise prejudice the client) when a firm is exploring hiring an attorney from another firm or when two firms are merging:
    - Only after substantive discussions have begun;
    - Only to the extent reasonably necessary; and
    - Information would normally include only names of people/entities involved, a brief summary of the general issues in the representation, and whether the matter has been concluded.
- Rule 1.17: Similar change to that in 1.6.

ETHICS OF CLOUD COMPUTING

Cloud computing raises the issue of data security as well as data privacy, though it can be difficult to distinguish between the two and they often overlap. Principles that arise when we talk about data security include the following:

- **Confidentiality:** protection against unauthorized disclosure, either intentional or accidental;
- **Integrity:** protection against corruption, tampering, alteration;
- **Availability:** prompt and reliable access;
- **Authentication:** assurance that a person/organization/device is who/what it claims;
- **Authorization:** effective administration of security;
- **Access Control:** ability to restrict and control access;
- **Accountability:** identification of person/organization who is responsible for security;
- **Assurance:** confidence in the system;
- **Nonrepudiation:** ability to track and prove use of the system to counter claims that data was not used.[22]

Data security is of particular concern in cloud computing because the data leaves the control of the attorney and rests in the hands of a third party vendor. We can see this reflected in the changes to the ABA Rules 1.6 and 5.3 discussed above. Essentially, these rules state that lawyers must keep abreast of technological advances and ensure that they and those with whom they contract for services safeguard the confidentiality of personal data.

[22] Kimberly Keifer et al., INFORMATION SECURITY: A LEGAL, BUSINESS, AND TECHNICAL HANDBOOK 6 (2004).

Thus far, every state ethics board that has considered cloud computing (or technology that poses similar issues)[23] has found that it is acceptable for law firms as long as the law firm exercises reasonable care in the selection and use of cloud computing vendors. [24]

To exercise reasonable care, a lawyer should consider particular issues relevant to data security in cloud computing when working with a vendor:

1. unauthorized access to confidential client information by a vendor's employees (or sub-contractors) or by outside parties (e.g., hackers) via the Internet;
2. the storage of information on servers in countries with fewer legal protections for electronically stored information;
3. the storage of information on servers in countries with greater legal protections for electronically stored information, resulting in your data being "held hostage";
4. a vendor's failure to back up data adequately;
5. policies regarding ownership of stored data;
6. the ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business;
7. the provider's procedures for responding to (or when appropriate, resisting) government requests for access to information;
8. policies for notifying customers of security breaches;
9. policies for data destruction when a lawyer no longer wants the relevant data available or transferring the data if a client switches law firms;
10. sufficient data encryption; and
11. the extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information.

USING THE METADATA OPPOSING SIDE ACCIDENTALLY SHARED THROUGH ELECTRONIC COMMUNICATION

What is metadata?

When you create a document, the software keeps track of certain information about the document itself:

- Who created it and when
- Who edited it and when
- Your company or organization name
- The name of your computer
- The name of the network server or hard disk where you saved the document
- Other file properties and summary information

[23] These states include Alabama, Arizona, California, Iowa, Maine, Massachusetts, New Jersey, New York, Nevada, North Carolina, Oregon, Pennsylvania, and Vermont.

[24] See *Cloud Ethics Opinions Around the U.S.*, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Oct. 31, 2012).

- Non-visible portions of embedded OLE objects
- The names of previous document authors
- Document revisions
- Document versions
- Template information
- Hidden text or cells
- Personalized views
- Comments

A distinction can be made between three kinds of metadata:

1. Substantive metadata is application-based and may contain modifications, edits, comments, etc., that were not necessarily intended for adversaries to see.
2. System-based metadata includes information automatically captured by the computer system, such as author, date, time of creation, and date of modification.
3. Embedded metadata consists of text, numbers, and content that is directly input but not necessarily visible on output, such as spreadsheet formulas or hyperlinks.[25]

Metadata gives rise to several major discovery issues: what metadata are you obligated to produce? What precautions should you take against inadvertent disclosure of confidential metadata? What do you do if you are on the receiving end of metadata that was likely shared inadvertently?

It is generally accepted – and has been for some years – that metadata is an integral part of an electronic record and must be produced. "If you remove it, you are altering the file, changing the evidence. You might as well rip off the cover of a paperback book, tear out the table of contents and the index, and then rip off each and every page number in a book – all metadata – and then claim you have not altered the book. Of course you have. It is indisputable. The same applies to metadata in computer files, although not all metadata. All metadata are not created equal."[26]

In a 2011 decision,[27] Judge Scheindlin of the Southern District of New York stated that the following minimum fields of metadata should be included in any production of electronically stored information:

- **Identifier**: A unique production identifier ("UPI") of the item.
- **File Name**: The original name of the item or file when collected from the source custodian or system.
- **Custodian**: The name of the custodian or source system from which the item was collected.
- **Source Device**: The device from which the item was collected.

---

[25] See *Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dept. of Homeland Sec*., 255 F.R.D. 350, 354-55 (S.D.N.Y. 2008).
[26] Ralph Losey, *New Opinion by Judge Scheindlin on FOIA, Metadata and Cooperation,* http://e-discoveryteam.com/2011/02/07/new-opinion-by-judge-scheindlin-on-foia-metadata-and-cooperation/ (last visited Oct. 23, 2012).
[27] *National Day Laborer Organizing Network v. United States Immigration and Customs Enforcement Agency* , 10 Civ. 3488, (S.D.N.Y., Feb. 7, 2011) (available at http://commonscold.typepad.com/files/nationaldaylabor.pdf).

- **Source Path:** The file path from the location from which the item was collected.
- **Production Path**: The file path to the item produced from the production media.
- **Modified Date**: The last modified date of the item when collected from the source custodian or system.
- **Modified Time**: The last modified time of the item when collected from the source custodian or system.
- **Time Offset Value**: The universal time offset of the item's modified date and time based on the source system's time zone and daylight savings time settings.[28]

Judge Scheindlin went on to require production of the following additional metadata fields for all email messages:

- **To**: Addressee(s) of the message.
- **From**: The e-mail address of the person sending the message.
- **CC:** Person(s) copied on the message.
- **BCC**: Person(s) blind copied on the message.
- **Date Sent**: Date the message was sent.
- **Time Sent**: Time the message was sent.
- **Subject**: Subject line of the message.
- **Date Received**: Date the message was received.
- **Time Received**: Time the message was received.
- **Attachments:** Identifying numbers for all attachments.

Judge Scheindlin's standards give us a good sense of what can be required in terms of production – enough metadata that the electronically stored information can be understood and organized. But what metadata needs to be protected from disclosure? Attorneys also have an ethical obligation to protect confidential client information, including metadata. It is generally accepted that an attorney must take reasonable measures to "scrub" confidential metadata before production. In an opinion released in January of 2010, the North Carolina State Bar Ethics Committee opined that what is "reasonable" can vary with the sensitivity of the data, the potential adverse consequences, and any specific instructions from the client.[29] In its own opinions, Arizona's Ethics Committee has expanded on this idea of "reasonable" to include "whether further disclosure is restricted by statute, protective order, or confidentiality agreement."[30]

What if a lawyer receives metadata that was inadvertently produced? Under the amendments to Model Rule 4.4, a lawyer is clearly required to notify opposing counsel of confidential metadata believed to be inadvertently disclosed. Most state bar ethics opinions

---

[28] *Id*.
[29] 2009 Formal Ethics Opinion 1, http://tinyurl.com/ca7od29 (last visited Oct. 31, 2012).
[30] Michael Kozubek, *Metadata raises legal risks*, INSIDECOUNSEL (Aug. 2011) (available at http://www.insidecounsel.com/2011/08/01/metadata-raises-legal-risks?page=2) (last visited Oct. 31, 2012).

already agree with this clarification, but some do not. Maryland, for example, has issued an opinion that does not require notification but suggests consulting with the client as to the pros and cons of notification. Presumably, unless the Maryland Supreme Court adopts the amendments proposed in the Model Rules, this would still be the prevailing opinion in that state.[31]

Even if an attorney is obligated to notify opposing counsel of inadvertently disclosed confidential metadata, can the attorney "mine" the data for information? According to a 2006 ABA opinion and a few states, the answer is yes. Several other states clearly restrict the mining of confidential information thought to be inadvertently disclosed. A few draw the line between confidential data that is known to be inadvertently disclosed and confidential data that is merely suspected to have been inadvertently disclosed.[32]

PITFALLS OF INTERACTIVE WEBSITES: WHEN DOES THE ATTORNEY-CLIENT RELATIONSHIP BEGIN?

The explosion of digital technology poses other questions for the legal profession as well. In recent years, lawyers have made use of the internet to advertise their services and attract clients. Such websites can work in a number of different ways, but some of them involve communication between a lawyer and an inquirer. This leads to the question of confidentiality and the start of the attorney-client relationship.

The amendments to Model Rule 1.18 changed the word "discusses" to "consults" so that any person who "consults with a lawyer about the possibility of forming a client lawyer relationship . . . is a prospective client." The new language in Comment 2 explains that a consultation is likely to have occurred if a person submits information to a lawyer in response to a request or invitation – communicated through any advertising medium – to submit information about a potential representation without adequate warnings as to limits on the lawyer's obligations.[33] The comment goes on to clarify that a consultation does not occur if a person contacts a lawyer with information simply in response to advertising that describes the lawyer's education, areas of practice, and contact information.[34]

The upshot of this new language is that interactive websites are likely to lead to consultations because, by definition, such websites invite users to communicate their questions to an attorney. Although the ABA does say that it is a determination that will depend on the circumstances, anything encouraging communication beyond contact information may pave the way to a consultation. That said, there is nothing unethical about having a consultation as long as the attorney takes appropriate steps to protect confidential information.

Another ethical quandary that arises with internet advertising is the use of pay-per-click ads or pay-per-lead services. According to long-standing ethical restraints, a lawyer may not pay a third party for recommending his or her services to another. Does using an Internet advertising

[31] *Id.*
[32] *Id.*
[33] Model Rules of Professional Conduct, Rule 1.18 cmt. [2] (2012).
[34] *Id.*

services where the attorney pays a third party every time someone clicks on the attorney's ad violate this restraint?

The amendments to Model Rule 1.7 are intended to address this issue. The new language clarifies that a recommendation occurs when a third party vouches for or endorses a lawyer based on professional capabilities, character, competence, etc. Pay-per-click ads are acceptable advertising. Pay-per-lead services are as well as long as it is clear to the end user that (1) the service is not actually recommending the lawyer, (2) the service has not evaluated the end user's legal issues; and (3) that the service is being paid to generate the lead. [35]

WHAT CAN ATTORNEYS SAY IN BLOGS AND OTHER ONLINE FORUMS?

Blogs are an exciting and easy way for attorneys to communicate their thoughts, experience, and expertise to the world at large. They can be effective marketing tools or simply outlets for creative intellectual work. Nonetheless, blogs – or blawgs, as blogs by lawyers are often called – come with their own set of ethical concerns.

Blawgs, along with other online forums such as tweets, newsletters, and even bios on firm websites, can constitute lawyer advertising. Lawyers need to make sure the information they state about themselves doesn't violate their ethical obligations. There is, of course, the relatively obvious prohibition against false or misleading representation. Any attorney should realize that his or her blog needs to be truthful and also carry appropriate disclaimers regarding legal advice and expectations.[36]

Client confidentiality also comes into play when writing for a blog, posting a status update, or updating a bio on a law firm website. Some states protect only a client's "secrets and confidences" while most follow the ABA's lead in protecting all "information relating to the representation of the client."[37] In the few states that protect only "secrets and confidences," an attorney can blog or tweet about his or her activities regarding the client as long the information is publically available. In most states, however, even this would be unethical because confidentiality is something only the client can waive. This is easy to overlook when we want to blog about our latest breakthrough in a difficult negotiation. Such information can only be used if the client gives consent.[38] An assistant public defender in Illinois serves as an example of the consequences of blogging about cases. A 19-year veteran of the public defender's office was fired and charged with ethical violations for revealing confidential client information when she blogged about the cases on which she worked.[39]

Blawgs also raise the issue of confidentiality in terms of the relationship with a potential client. As discussed above, it can be difficult to discern when the attorney-client relationship begins with digital media. The conversational tone of many blawgs and the ability to engage in

[35] Model Rules of Professional Conduct, Rule 7.2 cmt. [5] (2012).
[36] Model Rules of Professional Conduct, Rule 7.1 (2012).
[37] Model Rules of Professional Conduct Rule 1.6 (2012).
[38] William Hornsby. *Can I Say That? Part One,* Aug. 3, 2011, http://www.attorneyatwork.com/can-i-say-that-part-one/ (last visited Oct. 31, 2012).
[39] See Steven Seidenberg, *Seduced: For Lawyers, the Appeal of Social Media is Obvious. It's Also Dangerous,* ABA J., at 48 (Feb. 2011).

comments can be confusing for readers/users who are seeking legal information and advice. Suppose a woman seeking a divorce reads a blawg by a divorce lawyer, is impressed with what she reads, and then comments on the blawg entry with some detail about her situation and a question. Does the lawyer need to treat this as confidential information of a prospective client? What if the lawyer happens to already be representing the husband?[40] How should the lawyer respond?

The upshot of this example is that blawgers or lawyers who post in other online forums (newsletters, firm websites, etc.) need to be extremely careful about allowing comments and/or soliciting contacts and information. Disclaimers as to legal advice and the relationship established between the lawyer and the reader/user need to be explicitly clear. In the example above where the woman was seeking divorce, the California Bar opined that the website's disclaimer, which read, "I agree that I am not forming an attorney-client relationship by submitting this question. I also understand that I am not forming a confidential relationship," was enough to prevent an attorney-client relationship but not enough to defeat a user's expectation of confidentiality. As a result, the firm could be disqualified from representing the husband.[41]

Blawgers have also run into trouble for criticizing judges, a violation of rule 8.2.[42] In an oft-reported example, an attorney was angry that a Florida judge gave only week to prepare for trial. When working through normal administrative grievance channels did nothing to resolve this ongoing problem, the attorney wrote a blawg exposé in which he called the judge an "'evil, unfair witch,' 'seemingly mentally ill,' and 'clearly unfit for her position and knows not what it means to be a neutral arbiter.'"[43] The Florida Bar found him to be in violation of five rules of ethics including the prohibitions against making false or reckless statements about the integrity of a judge and engaging in conduct that is prejudicial to the administration of justice.[44]

Because blawgs can be authored by more than one person, lawyers who run a blawg need to be aware of their ethical duties under rules 5.1 and 5.3, requiring attorneys to make reasonable efforts to assure that other lawyers and non-lawyers in the firm conform to the rules of ethics. It can be hard to know what "reasonable efforts" entails, but written policies regarding blawg entries and review of all entries before publication have been suggested.[45]

Finally, lawyers who use a blawg to argue a certain position on an issue may also run the risk of backing themselves into a corner if they end up representing a client who requires that a different view be taken. As Judy Cornett points out in her 2009 article on the ethics of lawyer blogging,

> [i]f a blawger whose reputation is entwined with her blawg needs to take a contrary position in order to advance a client's interests, she may be 'materially limited' from doing so because of that reputational interest. …It is not hard to imagine that a losing client might point to blawg posts

---

[40] See Judy M. Cornett, *The Ethics of Blawging: A Genre Analysis*, 41 LOY. U. CHI. L.J. 221 (2009) (citing Cal. Ethics Op. 2005-168).
[41] *Id.*
[42] Seidenberg, *supra* note 39, at 50.
[43] *Id.*
[44] *Id.*
[45] Cornett, *supra* note 40, at 237-38.

on a given legal issue as evidence that his attorney had a personal conflict of interest in advocating the other side of that issue.[46]

Cornett goes on to offer the following practical advice regarding blawgs:

1. Be responsible for your own blawg.
2. Decide whether your blawg is marketing tool. If it is, comply with the ethical restrictions on advertising. If it is not, do not engage in any self-promotion and tread very carefully.
3. Be wary of interacting with those who comment. If you allow comments, consider moderating them before allowing them to be posted.
4. Use explicitly clear and obvious disclaimers.
5. Review all blawg material carefully and frequently.[47]

SEPARATING PERSONAL AND PROFESSIONAL IDENTITIES ONLINE

The online world is seductive in its ability to let us speak our minds with little effort and often little thoughts. Yet attorneys have ethical and legal obligations that require us to think before we speak and take stock of appearances. These responsibilities play out in a number of ways when it comes to the criss-crossing of personal and professional lives online.

It seems a reasonable rule of thumb to keep personal and professional realms separate online. Take "friending" someone on Facebook as an example. A judge in North Carolina was Facebook "friends" with a local attorney who was appearing before him in a case. The two men went so far as to exchange comments about the proceeding on Facebook. This was deemed an ethical violation because of the appearance that the attorney might have improper influence with the judge.[48]

A few states disagree that online "friend"-ships between judges and attorneys are ethical troublesome. Ethics committees in Kentucky, New York, and South Carolina have all stated that there is nothing inherently unethical about social media links between judges and attorneys, though judges are cautioned regarding "close social relationships" that need to be disclosed to opposing counsel or prompt the judge to recuse him- or herself.[49]

In another Facebook incident, an attorney in Texas asked the judge for a continuance because of a death in the family. There was a funeral, but the judge checked the lawyer's Facebook page and noted that the week was largely spent drinking and partying. When the lawyer requested a second continuance, the judge denied the request.[50]

---

[46] Id., at 259-60 (referring to ethical limits imposed Model Rule 1.7).
[47] *Id.*, at 260-61.
[48] Seidenberg, *supra* note 39, at 50.
[49] *Id.*, at 52. See also Daniel Smith, *When Everyone is the Judge's Pal: Facebook Friendship and the Appearance of Impropriety Standard*, 3 J. OF L., TECH., & INTERNET 1 (2012).
[50] John Schwartz, *A Legal Battle: Online Attitude vs. Rules of the Bar*, N.Y. Times (Sept. 12, 2009) (available at http://www.nytimes.com/2009/09/13/us/13lawyers.html).

Facebook and other social media have also cropped up in investigations. Can an attorney send a "friend" request to a represented party? That would violate Model Rule 4.2, though reading a blog post by a represented party would not.[51] What about an unrepresented witness for the opposing side? The New York City Bar Association says this is okay and that the attorney does not have to reveal the motive behind the friend request, but the Philadelphia Bar says she does.[52]

This last question raises the specter of anonymity online. Lawyers, like anyone else, can create a fake and anonymous online identity, and some do. It is worth noting that under the Federal Rules of Civil Procedure, anonymity before a tribunal is prohibited. In addition, Model Rule 8.4(c) prohibits engaging in "conduct involving dishonesty, fraud, deceit or misrepresentation." Arguably, the Internet is not a tribunal and it is not deceitful to be anonymous, but this argument skates the edge of our obligations as attorneys. Perhaps the better guiding principle should be: if you do not want your name associated with the statements, you should not be making the statements online.

Furthermore, Kevin O'Keefe, who writes Real Lawyers Have Blogs, urges lawyers to use their real identities not just because it keeps us honest but because it helps us build valuable reputations.[53] It is effective marketing to put your name on the accurate and insightful information you have to share.

The upshot of this discussion is that lawyers need to be mindful and careful about mingling their personal and professional identities online. When the two intermingle, ethical problems can easily arise. One common approach is to use one social media outlet professionally (e.g. LinkedIn) and another for personal life (e.g. Facebook), though this does not remove the need to be careful about what you post in either outlet or anywhere else. As we all know, the Internet has radically altered our views on privacy and communication, and we are scrambling keep up ethically. As the ABA Commission on Ethics 20/20 said in its Introduction and Overview of the proposed rule amendments, the goal of the ethical rules is to "protect[] the public; preserv[e] the core professional values of the American legal profession; and maintain[] a strong, independent, and self-regulated profession." This self-regulation can be particularly challenging in the face of constantly shifting means of communication, but in the end it is what we all must do.

---

[51] Oregon State Bar Opinion No. 2005-164 (Aug. 2005).
[52] Seidenberg, *supra* note 39, at 51-52.
[53] See Kevin O'Keefe, *Fallacy of lawyers using multiple identities in social media and networking*, Real Lawyers Write Blogs, http://kevin.lexblog.com/2011/03/10/fallacy-of-lawyers-using-multiple-identities-in-social-media-and-networking/ (last visited Nov. 1, 2012).