Social Media and its Impact on the Legal Process

Robert A. Heverly
Associate Professor
Albany Law School

New York State Magistrate's Association
and Magistrate's Court Clerks Conference
Annual Conference
Monday, September 28, 2015
Sheraton, Niagara Falls, NY

| rheve@albanylaw.edu | http://robert.heverly.org | 518 445-2379 |

Robert A. Heverly is an Associate Professor of Law at Albany Law School of Union University. He has taught as a visiting professor at Michigan State University College of Law, taught in and directed a Masters in Law Program at the University of East Anglia's Norwich Law School in the UK, has taught in Trier, Germany as a Guest Professor of the Common Law, and regularly teaches Internet Law as part of the George Washington University School of Law's Munich Intellectual Property Summer Program.

Professor Heverly earned his LL.M. from Yale Law School, after which he undertook a Resident Fellowship with the Information Society Project at Yale Law School, where he retains an affiliation as a Faculty Fellow. He received dual Bachelor of Arts degrees (Broadcasting & Mass Communications Studies and Psychology) from the State University of New York College at Oswego (with honors), and a Juris Doctor (with honors) from Albany Law School of Union University. Prof. Heverly is currently the Chair of the Internet and Computer Law Section of the American Association of Law Schools.

Professor Heverly's research interests include intellectual property, technology and society (especially the Internet, computers, networks, and information law), media law, property, and globalization. He regularly teaches continuing legal education courses on legal ethics and social media & online activity. He has taught Torts, Property Law, Art and Entertainment Law, Cyber/Internet Law, Copyright Law, International and Comparative Intellectual Property Law, and related courses. He has published articles and book chapters in the Berkeley Technology Law Journal, the Georgetown Journal of International Law, and MIT Press, among others, and recently spoke at the Drones and Aerial Robotics Conference (DARC) sponsored by NYU's Engleberg Center on Innovation Law and Policy.

Contents

This page intentionally blank.

The Internet, mobile telephony, and the apparently constant connectedness of business professionals and their clients and colleagues raise a variety of issues in the modern professional world. Of these, new technologies often raise many issues, often simply because we are unaware of the technology's true impact on our lives and our practice. These materials will look at how connectedness in many of its forms implicates judicial, procedural, and ethical concerns.

I. Introduction: The Internet Changes Nothing, the Internet Changes Everything

The Internet is essentially a series of inter-connected computers. At each end of any particular connection established over the Internet are computers, and in between are all the networking elements that allow the Internet to function. Networking works by providing standardized ways to transmit information from one location to another, and involves a transmission medium (such as fiber optic cable) and routers that know where the information needs to go. The "under the hood" elements are not particularly important for us here, though some of the workings of the network itself are relevant to inquiries regarding things like cloud computing and E-mail usage, and where that is the case we will delve lightly into them.

In the opening days of the Internet there was a scholarly debate between Judge Frank Easterbrook and other scholars (most notably Larry Lessig) as to whether there should be a legal field known as "Cyberspace Law." While the debate took turns not relevant to us here, one advantage of its having taken place is that it helped develop the analytical tools we need to ask whether the Internet changes anything when it comes to legal relations among people. In some cases, the Internet changes nothing. The doctrinal analysis we undertake is "the same" as it was before the Internet, and the Internet's involvement in the scenario is at best a red herring, and at worst a fatal distraction. In other cases, the Internet does change something, either by amplifying the effects of actions that existed in the past, by changing how those actions are perceived, or by making new aspects of them salient to our legal analysis.

The Internet is sometimes called "The Big Equalizer;" it allows everyone who wants to publish to publish whatever they would like. A variety of ways to publish are available, and in each case they offer various advantages and disadvantages. Building your own Web site takes time, some design sense, and an ability to understand how other people will use your site. Websites are also often time-consuming to update manually. This has lead to a plethora of online options for people to not only publish entire websites, but also options to publish in more limited ways, or to more limited groups of people. These include blogging platforms such as Wordpress and Blogger (the latter now owned by Google) that allow you to publish rather quickly and without much knowledge of how the Web works. These sites are indexed by the

search engines and all the maintenance is done by the host site, streamlining the online presence problem.

Social networking sites play a different and larger role, but include publishing abilities within their structures. These sites, such as myspace and Facebook, allow much more than publishing, but publishing – whether to the world or to a group of "friends" that can be upwards of 1,000 or more people – is a key ingredient to what the sites hope to accomplish. Add to these Twitter, a "micro-publishing" site that allows users to post short messages of up to 140 characters and in which people can "follow" and "be followed" by other Twitter users, and you have but a few of the ways in which content can be added by Internet users to the Web.

Each of these methods of online exchange contains pitfalls that must be considered by those who take them up. One woman lost her position in a teaching school because she posted a picture on Facebook of herself, holding a cup of what appeared to be beer. Her school kicked her out of the program and she lost her opportunity to finish the program and become a school teacher (she has rather infamously become known as the "drunken pirate" as that is what she captioned the image). Others have, for example, been "caught" cheating on disability claims, posting how active they have been while collecting disability benefits.

The potential pitfalls of both publishing online and of connecting online are multiplied by their interaction with the Rules of Professional Conduct. The complexity of the ethical analysis increases when we talk about using online resources in the practice of law itself (ie, as a component of practice, such as in seeking information about other parties, connecting with the judiciary, or soliciting business online), as opposed to more straightforwardly engaging in online speech.

II. Social Media and the Internet: The Technological Framework

In addition to the "regular" Internet uses with which most of us are familiar – sending E-mail and browsing the Web – recent years have brought us a host of new ways to interact and work over the Internet. These technologies and the ways they are implemented change over time. Learning today about MySpace.com, a web meeting place that was popular in the late 2000s, peaking in popularity from 2005 to 2008, may not be useful directly today, but the same kinds of issues raised by MySpace may arise again in the context of another technology. What is the current "fad" tends to get lots of attention, both in the popular press and in the courts. As the introductory discussion shows, however, the technology focused approach is often the wrong approach. A better approach involves learning about a technology, determining how it works,

who uses it, and how it is used, and then making appropriate determinations based on the elements of the analysis that become more or less important given the technological context in which the issue arose.

To spend significant time making rules for Facebook, or Google, or E-mail, or texts, is inefficient both in terms of resources and in terms of development of the common law. There may be times that one technology needs to be treated differently than another, but it will not be because one is called Facebook and another is called E-mail. It may be because the written content of an E-mail, when functioning properly, is largely under the control of the sender, while what appears on a person's Facebook page is an amalgamation of the input of others, advertisements, and choices made by Facebook itself.

The steps to addressing any social media question are to: 1) Determine who plays what role in the content or process that is relevant to the case; and, 2) Determine how users actually use the system (that is, what do they do with the technology). With these two questions in hand, a court is well placed to decide whether and to what extent social media should be a focus in the decision or is rather a red herring, distracting the court and the attorneys from issues more directly relevant to the case. As an aid to understanding the basics of the technologies, the following short descriptions of some of the most prominent social media technologies in use today serve as an introduction to these social media technologies themselves.

A. Facebook

One of the most prominent social media networks, Facebook allows its members to post announcements, photographs, videos, links to other sites, and related materials. Facebook members can become "friends" with other Facebook members, at which point the members can interact more closely, for example, by reading what the other has posted or seeing details about the friend's work, family or hometown. To become a friend, one member sends a friend request to another, and if the second member accepts the request, they are then "friends" for Facebook purposes. Facebook friends may be people the member knows in real life, such as family members, current or past classmates, colleagues, and others, but Facebook does not control "friending" and some people have thousands of friends on Facebook, essentially accepting all friend requests that come their way. Additionally, businesses and prominent or famous individuals may have business pages that members can "like" to receive posts from the liked page. Facebook obtains financial support for the site from targeted advertisements shown to the members, as well as from related commercial agreements. Users have some control over how much of their information is available to non-friends and to non-Facebook members (for example, through search engines).

B. LinkedIn

LinkedIn is often referred to as a professional or business person's Facebook. LinkedIn encourages people to "connect" (the LinkedIn word for what is a "friend" on Facebook) only with people they know or have been introduced to, and the content on LinkedIn is decidedly more professional and serious. Unlike Facebook, LinkedIn offers a premium membership which provides greater access to other users' information.

C. Twitter

Twitter is a "micro-blogging" platform. Users use Twitter to post links, short bursts of information, and images. Twitter's "Tweets" are limited to 140 characters (including spaces). Users can "follow" another person's Twitter feed, and then see the things that person is tweeting. Direct interaction among members is possible using direct messaging, but the majority of twitter users interact simply by directing messages at each other. Twitter is the main impetus behind "hash tags" – short lines of text following the "hash" symbol (#). A Twitter user can search for a hash tag to see what others are identifying as being related to that topic. Twitter feeds can be private, allowing only those approved by the Twitter user to see the tweets.

D. Google Plus (Google+)

Google+ is Google's foray into the Facebook/LinkedIn style of social network. Users form "circles" and share information, posts and links. As with Facebook, users have some controls over who can see and access their information.

E. Other Sites and Technologies

There are a variety of other social media and sharing sites on the Internet. Instagram and Flickr are focused primarily on image sharing. Snapchat was designed as a way to send secure images that "self-destruct" shortly after they are viewed, and Delicio.us and Digg allow users to share web content with others. Pinterest allows users to share web content by "pinning" it to pages on the Pinterest site, and sites such as Reddit allow users to share links, jokes, images and more anonymously (Reddit has a culture of prohibiting "doxing" – or identifying users in real life).

In addition to these technologies, all of which allow some interaction among users (thus qualifying as social media), more Internet-based technologies exist, such as blogging platforms that allow for the posting of stories, links or images (and more), E-mail, and even "plain, old" web pages. All of these may raise the same kinds of questions and concerns raised by social media. When we add in smartphone "apps" (short for applications that run either the Windows operating system, Android, or Apple's iOS operating system), many of which exist for the social media networks described above, the issues can expand quite quickly. In any case, however, be clear as to which technology is at issue, and in what way, and determination of the who and the how from our questions above becomes easier.

III. Internet Law and Law for the Internet

A. Introduction

When we think through whether the Internet matters when we are asked to answer legal questions, one place to start is to ask whether there are "Internet specific" statutes relevant to the question raised. If there are, we know that – at least from a statutory standpoint – the Internet matters. In this section we will address questions that are likely to arise in generalized legal practice, that is, in practices that are not focused on technology, communications or the Internet. Within this area we will look at two examples where there are specific federal statutes on point, and at another area where the Internet has asserted it importance in practice.

B. The Internet and User Content—Part I: 47 U.S.C. §230

One area of Cyberspace Law that any general practitioner might run into involves the potential liability of online hosts (and other service providers) for civil wrongs carried out by service users. If a Facebook user posts a defamatory statement on his or her wall, is Facebook liable for "publishing" the post, at the time it is posted, after Facebook gains knowledge of it, or after Facebook is informed it is defamatory?

Two early cases dealt with a similar issue and reached different results on slightly different facts. In the first, the Southern District of New York held that online service providers were distributors, not speakers, for defamation law purposes, analogizing an online service provider

to a newspaper stand rather than a publisher or republisher of a statement.[1] As distributors are only liable for defamation if they have the requisite knowledge – that they knew or should have known – of the defamation – the court thus held that the defendant was a distributor and not liable for the complained defamation.

In a subsequent case, a New York State court held that an online service provider could be liable as a speaker, specifically as a republisher, if it did more than simply distribute the defamation.[2] In the second case, the online service provider used volunteer moderators to remove or edit posts that were objectionable (selling itself as "family friendly" due in part to this feature). Given the apparent incongruity in granting distributor status to service providers who take no action to counter the edginess of Internet communications, while imposing a more onerous burden on those who made that ostensibly worthwhile effort, Congress enacted (as part of the Communications Decency Act) 47 U.S.C. §230, limiting liability for providers for content provided by others. The statute provides, in part, as follows:

> **(c) Protection for "Good Samaritan" blocking and screening of offensive material**
>
> *(1) Treatment of publisher or speaker*
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> *(2) Civil liability*
> No provider or user of an interactive computer service shall be held liable on account of—
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

While set out in terms of providing protection for service providers who block or screen offensive material, that language is not operative in the statute, and the courts have dismissed it. That is, the statute instead precludes treating online service providers as publishers in all circumstances where the defamatory content is or was provided by another. This interpretation has significantly expanded the scope of the provision and subjected it to significant criticism. For example, even where a service provider was made aware of defamatory material that was

[1] *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

[2] *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y.Sup.), 1995 N.Y. Misc. LEXIS 229 63 USLW 2765, 23 Media L. Rep. 1794 (N.Y. Sup. Ct., Nassau County, 1995).

causing current harm and promised to take action to remove the material but failed to do so, §230 immunized the service provider from liability for content provided by another.[3]

Subsequent cases applied the bar against liability to an online service provider that paid for content from a third party (holding the service provider immune from liability for content provided by the paid provider),[4] as well as an allegation that an online service provider failed to maintain a safe online environment for its users (the court instead holding that the claim sought to hold the provider liable for the speech two users engage in while using the site).[5] One exception seemed to be found where a provider required a user to provide content that was illegal (in this case a violation of the Fair Housing Act) as a condition of posting on the site. [6] There a court found the provider to be engaged in joint provision of the content, and thus potentially liable. The result, however, was thrown into uncertainty by a later holding of the same court that held that the underlying activity that formed the basis for the earlier holding was in fact not illegal.[7]

The lesson to take away in this area of law is that when "bad things" happen online, often the primary perpetrator is either anonymous/hidden or judgment proof. In these cases, it is tempting to go after the online service provider. But as *Zeran* and its progeny teach us, even where an online service provider has been given notice of content that in some way injures the legal rights of a client (outside of the intellectual property area, which we will discuss next), the provider will not be liable for the damages caused by the content.

Lawyers sometimes meet word of this near absolute ban on service provider liability with a sense of incredulity: how can it be that an online service provider that has knowledge of damaging content can ignore that content and not be held liable? The answer is one of the standards of the legal lexicon: because the courts have said so. 47 U.S.C. §230 is thus a bar to many types of actions that might be brought outside of the Internet context, and ignoring it means risking dismissal of the case on motion early on in the proceedings. Note that this provision is relevant to any size business that allows third party generated content – which

[3] *Zeran v. America Online, Inc.*, 129 F. 3d 327 (4th Cir., 1997).

[4] *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.C. Cir., 1998).

[5] *Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843 (W.D. Tex. 2007).

[6] *Fair Housing Council of San Fernando Valley v. Roommate.com, LLC,* 521 F.3d 1157 (9th Cir. 2008).

[7] *Fair Housing Council of San Fernando Valley v. Roommate.com, LLC,* 666 F.3d 1216 (9th Cir. 2012).

includes user comments and ratings – on its site. As such, it may serve you well when defending businesses with an online presence from civil liability.

C. The Internet and User Content—Part II: 17 U.S.C. §512

In addition to the bar provided by 47 U.S.C. §230, a second federal statute provides a safe harbor for website owners and operators whose sites contain content provided by third parties (section 230 does not apply to Intellectual Property[8]). While some provisions of this statute are more relevant to those engaged more deeply in Cyberspace Law issues, the safe harbor provides immunity to copyright infringement claims to all online service providers under the defined circumstances. Because the provisions ostensibly protect all kinds of businesses, it is worthwhile to ensure that clients that have an online presence take the minimal steps necessary to gain the protection of the statute. Where a business or site is engaged in the "user generated content" business, further study of 17 U.S.C. §512 is required.

Subdivision (c) of 17 U.S.C. provides as follows:

> **(c) Information Residing on Systems or Networks at Direction of Users.—**
> (1) In general. — A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider -
>
> (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.
>
> (2) Designated agent. — The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:
>
> (A) the name, address, phone number, and electronic mail address of the agent.
> (B) other contact information which the Register of Copyrights may deem appropriate.
>
> The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

[8] 47 U.S.C. §230(e)(2).

Unlike 47 U.S.C. §230, 17 U.S.C. §512 does not automatically apply to online service providers. Instead, the provider must follow the process set out both to obtain protection and to keep it. Registering an agent for copyright purposes and responding to notice and takedown requests are essential elements of §512's structure. While there is more here, and while details of what constitutes notice remain in flux, the basic requirement of registering and having appropriate policies in place is a simple step that every business with an online presence can take to minimize potential liability from the actions of third parties who can post content to a website.

D. Jurisdiction and the Internet

The final area to touch on that may confront non-technology practitioners is that old law school standby, personal jurisdiction. One of the early trends in Cyberspace Law cases was to treat the Internet as "different" and to fashion tests that focused on elements of online interaction that seemed unique in comparison to offline transactions. In *Zippo Manufacturing Co.*,[9] the court fashioned a "sliding scale" by which jurisdictional claims could be measured. According to the Court:

> [T]he likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction if proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. (citations omitted)

[9] *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).

While the sliding scale has some appeal, more recent cases have placed it, if using it all, in the context of the overall test for personal jurisdiction (that is, the well-known *International Shoe* test requiring minimum contacts, a claim arising out of those contacts, and reasonableness in the exercise of jurisdiction). While *Zippo* can be read as establishing an independent test for jurisdiction, it can also be read as applying primarily to the minimum contacts element of the test, and this is how it has been applied in recent cases. That is, it can inform the "minimum contacts" inquiry, but does not determine it. Thus, a "standard" jurisdiction inquiry should be performed in Internet involved cases, with the caveat that the sliding scale may prove useful in cases with facts tied up in Internet transactions.

E. Access to Electronic Communications

Federal law, in a complicated and confusing patchwork quilt of laws, protects both the transmission and storage of electronic communications. Prof. James Grimmelmann describes it as follows:

> *A variety of federal and state statutes also regulate the use and disclosure of information stored in computers or transmitted on networks. This section examines the two principal federal statutes on point: the Stored Communications Act (the SCA, codified at 18 U.S.C. §§ 2701–2712) and the Wiretap Act (codified at 18 U.S.C. §§ 2510–2522). The SCA is also commonly referred to by its other name, Title II of the Electronic Communications Privacy Act, or ECPA. These statutes have two interlocking roles:*
>
> - *To protect individuals from having their private communications seen by otherprivate parties.*
> - *To regulate the process by which the government acquires private communications during investigations.*
>
> *Unfortunately for statutory clarity, these two roles are utterly intermingled in the SCA and Wiretap Act. They both take the form of a general prohibition on unauthorized access, together with exceptions for private and governmental access under certain circumstances.*
>
> *Figuring out what law applies to a given situation is often a matter of extensive back-and-forth cross-referencing. [When considering the statutes], keep in mind the private/governmental distinction and, also, whether the communications are being intercepted while in transit ("prospectively"), or retrieved after the fact ("retrospectively").*[10]

We must add to this uncertainty restrictions on access to electronic communications under the Fourth Amendment to the Constitution (and perhaps the Fifth, as well). Unfortunately, a full review of these statutes and requirements would require materials (and a lecture) of their own. We must make due instead with the understanding that these concerns are relevant to court

[10] James Grimmelmann, INTERNET LAW: CASES AND PROBLEMS, p. 210 (Semaphore Press, 2013).

orders related to electronic evidence, and we must consider them thoroughly when making such orders. By way of example, one of the best known cases in this area is *Romano v. Steelcase, Inc.*.[11] In *Romano*, the Court granted a party's request to an opposing party's Facebook pages and accounts (both current and deleted), noting that a Facebook member does not have a privacy interest that would preclude such access given Facebook's terms of service and warnings, which make clear that information posted to Facebook may not be private even when a user chooses private settings. The federal statutory prohibitions on Internet service providers disclosing information by requiring the party to consent to the disclosure and provide the information.

IV. Computers, the Internet, and the Courts

Judges are called upon more and more to make decisions about discovery and admissibility of evidence from Internet and other communications sources. Many of these decisions so far have been based on a particular technology, such as E-mail, social networks such as Facebook, twitter, or even text messages via cell phones. The issues, however, are likely to be similar across the various technologies. In addition, even where we talk about a particular technology, the issues will change based on how and what within that technology we are talking about. For example, making the bare claim that "service of process via E-mail is appropriate" misses the point. Some technologies may raise one issue more strongly, while another may raise other issues, but on the whole the framework of analysis should be – and is – likely to remain consistent across technologies. This means that as we proceed, a decision regarding admissibility of E-mail may provide strong arguments as to why (or why not) a "tweet" might be admissible in a later case, but may not be particularly helpful when it comes to discussing a later case involving E-mail. Each inquiry should focus on what is being sought or offered and how it came into existence, but not the general type of technology being considered.

A. Social Media Discovery

Litigants' social media accounts often contain information that is relevant to the litigation. Accessing that information is seen as important to presenting a solid case, and being aware of one's own client's social media use is an ethical responsibility. Access to social media content that is available to the general public requires no intervention; a party may simply view the available web pages (though at times these pages may provide insights that justify further

[11] *Romano v. Steelcase,* 30 Misc. 3d 426 (Sup. Ct. Suffolk County 2010)

inquiries into private areas of a litigant's social media involvement). If, however, a party wishes to access areas of another party's private social media content, a court may be called upon to provide assistance to the party seeking disclosure.

When this occurs, the party whose content is sought may assert privacy rights to attempt to block the other party's access. As noted above, in *Romano*[12], the defendant sought access to the Plaintiff's restricted and even deleted pages on Facebook. The plaintiff sought to block access, asserting privacy concerns, but the Suffolk County Supreme Court rejected these claims, noting that even Facebook says that information kept on its service should not be considered private. The Court also avoided the implications of the Stored Communications Act and the Electronic Communications Privacy Act by not requiring the providers to provide the information pursuant to a subpoena, but rather by requiring its production by the plaintiff.

Other cases have likewise held social media content that is alleged to be relevant to ongoing litigation is discoverable. The information sought, however, should be relevant, and the party seeking it should be doing more than going on a fishing expedition.[13] Instead, a basis for believing relevant information is available in the party's private content should be stated. Where there is only a broad request based on an unspecified belief that the social media page holds relevant information, the request has been denied. [14] There may also be circumstances under which it is appropriate to order in camera reviews of social media content, either by the court[15] or by a specially appointed master or referree.[16]

These examples show that past precedents and procedures often work sufficiently to address modern concerns. It was relatively unimportant that the cases noted above primarily concerned Facebook. Instead, once a showing was made that relevant information was either in the possession of or accessible to the opposing party, the court ordered that it be turned over. As

[12] *Romano v. Steelcase,* 30 Misc. 3d 426 (Sup. Ct. Suffolk County 2010).

[13] *See, e.g., McCann v. Harleysville Ins. Co.*, 78 A.D.3d 1524 (4th Dept. 2010); *Kregg v. Maldonado*, 98 A.D.3d 1289 (4th Dept. 2012).

[14] *See, e.g., Winchell v. Lopiccolo*, 38 Misc. 3d 458 (Sup. Ct. Orange Co. 2012).

[15] *See*, *Patterson v. Turner Constr. Co.*, 88. A.D.3d 617 (1st Dept. 2011)(remand requiring further in camera review to determine which portions of plaintiff's Facebook content was relevant to the litigation); *see also*, *Imanverdi v. Popovici*, 109 A.D.3d 1179 (4th Dept. 2013)("Contrary to plaintiffs' contention, Supreme Court properly exercised its discretion in modifying its prior order to compel discovery by directing plaintiff Atash Imanverdi to produce her Facebook page for in camera review).

[16] *Bianco v. North Fork Bank Corp.*, 2012 N.Y. Slip Op. 32611 (Sup. Ct. NY County 2012).

with company books, industrial logs, and even personal journals, the judicial process requires granting such access as is necessary and appropriate to opposing parties so as to allow them to appropriately pursue or defend the legal action.

A final note on discovery: spoliation is a potentially significant concern when it comes to social media (and other electronic) content. The "delete" button is very tempting for litigants, and counseling clients to use it is very tempting to litigation counsel. This must, of course, be avoided, as it violates procedural and ethical rules. Where it occurs, significant sanctions have been held to be appropriate.[17] Note also that delete does not always mean delete. Facebook and other resources may have backup files of deleted content and may even simply not delete content that the user removes from public or private view. If that deleted information is not accessible to the party who created it, however, or if the information was not party created at all – such as access logs or timestamp information – the cooperation of the social media site will be necessary, as the federal laws noted above likely preclude enforcement of a state subpoena or discovery order against such a provider.

B. Social Media Evidence

1. A General Framework

In relation to evidentiary decisions, authentication and hearsay form the core doctrines for the issues that surround social media evidence in the courts and provide the framework within which individual requests should be considered. In considering how to authenticate or treat social media content for hearsay purposes, it is again best not to focus too closely on the name or type of the social media in question. It is unlikely to matter, for authentication purposes, for example, whether a post offered as the defendant's was posted on Facebook or on Twitter or, for that matter, was sent by E-mail. It must still be shown to have its origin with the defendant. If it is offered for its content, and that content originated with a declarant, it must meet the requirements of hearsay doctrine. Content offered from automated systems that relates to the operation of those systems lacks a declarant, however, and thus is subject only to authentication, not hearsay, analysis. The key is to pay attention to who took the actions relevant to the information sought, not the name or type of technology they used to do so.

[17] *See, Allied Concrete Co. v. Lester,* 736 SE 2d 699 (Va. 2013); *Gatto v. United Airlines, Inc.*, 10-cv-1090 (D.N.J. 2013).

2. Authentication Issues

Authentication requires that evidence be shown to be what it is represented to be. Authentication may relate to the content of the message, or it may relate to the operation of the system that generated the content. If referring, for example, to a delivery report for a Facebook message, it is the operation of the Facebook messaging system that is in question. If referring to information found in a post or message sent via Facebook's services, then it is the content of the message that is in question. The two types of authentication raise separate questions.

For example, when allowing into evidence a printout of a page from a Russian social networking website that was referred to as the Russian Facebook, the Federal District Court was held on appeal to have erred. This was not because the page was a social media site, or even that it was a Russian site, but rather because the prosecutors in the case failed to fully authenticate the website represented in the printout as belonging to the defendant.[18] The case provides a template for dealing with authentication issues of this type. Beginning with authentication in general:

> *For instance, we have said that a document can be authenticated by "distinctive characteristics of the document itself, such as its '[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances.' " Maldonado–Rivera, 922 F.2d at 957 (alteration in original) (quoting Fed.R.Evid. 901(b)(4) (pre–2011 amendments)); see also Sliker, 751 F.2d at 488 (contents of alleged bank records, in conjunction with their seizure at purported bank office, provided sufficient proof of their connection to allegedly sham bank). Or, where the evidence in question is a recorded call, we have said that "[w]hile a mere assertion of identity by a person talking on the telephone is not in itself sufficient to authenticate that person's identity, some additional evidence, which need not fall into any set pattern, may provide the necessary foundation." Dhinsa, 243 F.3d at 658–59 (brackets and internal quotation marks omitted); see also Sliker, 751 F.2d at 499 (voice on tape recording was sufficiently authenticated as defendant's based on comparison of taped voice with defendant's trial testimony). And in a case where credit card receipts purportedly signed by the defendant would have tended to support his alibi defense, we ruled that the defendant's copies had been sufficiently authenticated, despite some question as to when these copies had been signed, where the defendant offered testimony from store managers as to how the receipts were produced, testimony from the defendant's wife (a joint holder of the credit card) that she had not made the purchases in question, and testimony from a handwriting expert that the defendant's signature was genuine. United States v. Tin Yat Chin, 371 F.3d 31, 35–38 (2d Cir.2004)*[19]

In analyzing the admissibility of the website content, the court continued:

> *The government did not provide a sufficient basis on which to conclude that the proffered printout was what the government claimed it to be—Zhyltsou's profile page—and there was thus insufficient evidence to authenticate the VK page and to permit its consideration by the jury.*

[18] United States v. Vayner, 769 F.3d 125 (2d Cir. 2014).

[19] *Id.* at 130-131.

In the district court, the government initially advanced the argument that it offered the evidence simply as a web page that existed on the Internet at the time of trial, not as evidence of Zhyltsou's own statements. The prosecution first represented to the district court that it was presenting the VK page only as "what [Special Agent Cline] is observing today on the Internet, just today," J.A. 26, conceded that "the agent does not know who created it," and averred that Special Agent Cline would testify only that "he saw [the VK page] and this is what it says," J.A. 30. Consistent with these representations, Special Agent Cline testified only that the page containing information related to Zhyltsou was presently accessible on the Internet and provided no extrinsic information showing that Zhyltsou was the page's author or otherwise tying the page to Zhyltsou.

At other times, however, the government repeatedly made a contrary argument to both the trial court and the jury, and insisted that the page belonged to and was authored by Zhyltsou.7 Nor is this surprising. The VK profile page was helpful to the government's case only if it belonged to Zhyltsou—if it was his profile page, created by him or someone acting on his behalf—and thus tended to establish that Zhyltsou used the moniker "Azmadeuz" on Skype and was likely also to have used it for the Gmail address from which the forged birth certificate was sent, just as Timku claimed. Moreover, the district court overruled Zhyltsou's hearsay objection and admitted a printout of the profile page, which stated that "Zhiltsov's" Skype username was "Azmadeuz," because it found that the page was created by Zhyltsou, and the statement therefore constituted a party admission. See J.A. 23 (The Court: "This is a statement made by your client. This is his Facebook record."); J.A. 29–30 (describing the government's plan to establish that the Gmail address was Zhyltsou's "by what [the court] regard[ed] to be perfectly legitimate admissible evidence of what it is, the assumption is quite clear that what appears on the Facebook page is information which was provided by" Zhyltsou); J.A. 32 (The Court: "It's his Facebook page. The information on there, I think it's fair to assume, is information which was provided by him."); see also Fed.R.Evid. 801(d)(2)(A) (defining an opposing party's statement as non-hearsay).

As noted above, Rule 901 requires "evidence sufficient to support a finding that the item is what the proponent claims it is." It is uncontroverted that information about Zhyltsou appeared on the VK page: his name, photograph, and some details about his life consistent with Timku's testimony about him. But there was no evidence that Zhyltsou himself had created the page or was responsible for its contents. Had the government sought to introduce, for instance, a flyer found on the street that contained Zhyltsou's Skype address and was purportedly written or authorized by him, the district court surely would have required some evidence that the flyer did, in fact, emanate from Zhyltsou. Otherwise, how could the statements in the flyer be attributed to him? Cf. Dhinsa, 243 F.3d at 658–59 ("[A] mere assertion of identity by a person talking on the telephone is not in itself sufficient to authenticate that person's identity...."). And contrary to the government's argument, the mere fact that a page with Zhyltsou's name and photograph happened to exist on the Internet at the time of Special Agent Cline's testimony does not permit a reasonable conclusion that this page was created by the defendant or on his behalf.

It is true that the contents or "distinctive characteristics" of a document can sometimes alone provide circumstantial evidence sufficient for authentication. Fed. R. Evid. 901(b)(4). For example, a writing may be authenticated by evidence "that the contents of the writing were not a matter of common knowledge." Maldonado–Rivera, 922 F.2d at 957 (brackets and internal quotation marks omitted). Here, however, all the information contained on the VK page allegedly tying the page to Zhyltsou was also known by Timku and likely others, some of whom may have had reasons to create a profile page falsely attributed to the defendant. Other than the page itself, moreover, no evidence in the record suggested that Zhyltsou even had a VK profile page, much less that the page in question was that page. Nor was there any evidence that

> *identity verification is necessary to create such a page with VK, which might also have helped render more than speculative the conclusion that the page in question belonged to Zhyltsou.*[20]

What occurred in Vayner was an attempt by the prosecution to introduce the social media page and attribute that page to the defendant. The prosecution did this not just by using his photograph and related personal information appearing on the page, but by trying to buttress this information with testimony of someone who knew the defendant and whose story matched with what appeared on the page. The Second Circuit rejected this approach, and most likely rightfully. While authenticating a document by its contents is at times acceptable, it takes more than just a consistency between the content and the person alleged to be responsible for it. Where the allegedly distinctive characteristics are not sufficiently distinctive, however, because for example others have knowledge sufficient to create the content, authentication fails and the evidence should not be admitted.

Alternative questions are raised when evidence results from the operation of a technological process. In these cases, the reliability of the process itself is at issue, and must be established by someone with sufficient knowledge of the system so as to be able to testify as to its operation and dependability.

3. Hearsay

As with authentication, it is easy to quickly become focused on a specific technology when considering hearsay questions. A better path is to consider the how the statement came into being and what it is being offered to show. If it was the result of a technological process that occurred without direct human intervention, there is no declarant, and authentication is the primary barrier to admissibility. Where content is offered as allegedly originating with a declarant, hearsay considerations may come to the forefront. The hearsay considerations, however, are not substantially different from those raised with other kinds of evidence, and the relevant hearsay exceptions apply.

Not getting distracted by the technology will help when applying the hearsay exceptions, however. For example, not all E-mail sent from a work computer will qualify as a business record. Where sent for personal reasons, the business record exception is inapposite. This is true for the same reasons that would hold if an employee sent personal letters from work, even if the employee kept a file with the letters in his work filing cabinet, because it was not a record kept in the ordinary course of business.

[20] *Id.* at 131-132.

4. Anonymity

Anonymous speech is constitutionally protected.[21] The Constitutional protection extends to the Internet.[22] The Internet, and social media in particular, provide significant opportunities for anonymous speech. Under what circumstances should a court order an anonymous – or a pseudonymous – speaker to be identified using the legal process? The Federal District Court for the District of Connecticut answered that question using the following balancing analysis:

1) Whether "the plaintiff has undertaken efforts to notify the anonymous posters that they are the subject of a subpoena and withheld action to afford the fictitiously named defendants a reasonable opportunity to file and serve opposition to the application;"

2) Whether the plaintiff has identified a cause of action arising from the online speech;

3) Whether the anonymous person had an expectation of privacy at the time of posting; and,

4) Whether the plaintiff has made an "adequate showing" as to the cause of action against the poster.[23]

Using this analysis, a court can try to ensure that the Internet's promise as a robust forum for discourse and deliberation does not unnecessarily restrict access to the courts for those who have suffered legal wrongs via the Internet.

C. Service of Legal Process via the Internet

Due process permits service of process via alternative means so long as the means is "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections."[24] Various courts have permitted service of process via the Internet, including specific decisions permitting service by E-mail and through Facebook.[25]

---

[21] *Buckley v. American Constitutional Law Found.*, 525 U.S. 182, 199-200 (1999).

[22] *Reno v. ACLU*, 521 U.S. 844, 870-871 (1997).

[23] *Doe I v. Individuals*, Civil Action No. 3:07 CV 909 (CFD) (D. Ct. 2008).

[24] *Mullane v. Central Hanover Bank & Trust*, 339 U.S. 306, 314 (1950)(citations omitted).

[25] *See, Rio Properties, Inc. v. Rio International Interlink,* 284 F.3d 1007 (9th Cir. 2002); *Popular Enterprises, LLC v. Webcom Media Group, Inc.*, 225 F.R.D. 560 (E. D. Tenn. 2004); *Williams v. Advertising Sex LLC*, et al., 2005 U.S.

The issues that arise in these cases provide another good example of the point made at the start of these materials: sometimes the Internet matters, sometimes it does not. In determining whether to allow alternative service of process via some Internet based method, courts should generally ask two questions (after the appropriateness of alternative service is generally established by the moving party):

1) Do the defendants have the technological sophistication necessary to receive important documents in the manner requested? And,

2) Is the particular method chosen shown by the moving party to be a reliable one for reaching these particular defendants.

This second point should be further broken into two inquiries:

a) Does the address, identity, location or Internet facility unquestionably belong to the defendant? And,

b) Is it reasonable to believe that there are likely to be technological impediments to receipt of the process given the method chosen?

While courts confronted with this issue to date have often engaged in the inquiry spawned by questions 1 and 2 above, they have often not taken into account part b of the second part of the inquiry. Once the appropriateness of alternative methods of service are established, the courts ask whether the defendant is an Internet user of the type who is able to receive important communications via the Internet method in question. They may then ask whether the particular address or resource used belongs to the defendants, requiring plaintiffs to show that the address is "reliable," but courts to date have not shown an awareness of the many ways in which E-mail and other online communications can become lost or waylaid. For example, an automated spam filter may prevent service from reaching a defendant, although it will appear as though the message was delivered to the relevant account. A simple misspelling of the address may also result in lost service, and because a significant online spam[26] problem has caused mail servers not to notify the sender that the message was not delivered. In addition, there is no foolproof method to ensure delivery through delivery confirmation via Internet, even this method will not suffice to ensure delivery. In such cases, E-mail or social media service may be appropriate, but additional methods – such as publication – may be necessary to ensure the defendant's due process rights are protected.

District LEXIS 25670 (N.D. W. Va. Oct. 26, 2005); *FTC v. PCCare247 Inc.*, 2013 WL 841037 (S.D.N.Y. 2013); *but see, contra*, *Ehrenfeld v. Bin Mufouz*, 2005 WL 696769 (S.D.N.Y. 2005).

[26] Spam is the Internet name for unsolicited commercial advertisements which often arrive unrequested via E-mail.

V. Online Speech, Legal and Otherwise: Publishing Online, Blogging, Facebook, Twitter and More

There are a variety of ways to publish online. One is simply to develop a Web page. This was the earliest of the ways in which people published online, but it required (and to a certain degree still requires) skills in web page coding (known as HTML, now in its fifth iteration), and it can be labor and time intensive. In place of developing a Web page or site, a variety of opportunities for easier online publishing exist, including blogging platforms such as Blogger[27] and Typepad.[28] A ready-made blogging platform allows the user to choose a design for their page, choose various elements of the page, and integrate them into the final blog – a blog being little more than a web page that allows for interactive publishing, including comments and links from other blogs that reference a post. Many lawyers blog, and there are a great many law related blogs to choose from.[29]

In addition to blogging, lawyers may publish through social networking platforms such as Facebook,[30] Google+,[31]LinkedIn,[32] and Twitter.[33] These platforms enable publishing in different ways, oftentimes integrated with tools to connect the user to friends, acquaintances, and perhaps even strangers.[34] Twitter, for example, requires posts to be short: no longer than 140 characters. Facebook allows users to "friend" each other and to control the extent to which their information and posts are shared with others, but a large part of the Facebook experience involves a user posting information as a "status update." This information is then automatically placed into the user's friend's wall, where they can scroll their friends' updates and see what they have been up to. LinkedIn uses a similar newsfeed model, though LinkedIn is more focused on professional information and less on personal updates.

[27] http://www.blogger.com/

[28] http://www.typepad.com/

[29] Legal or "Law Blogs" are sometimes referred to as Blawgs. For a thorough and up to date list, s*ee*, Blawg Directory, ABA Journal (with ability to search by category, region, and author type): http://www.abajournal.com/blawgs/

[30] http://www.facebook.com/

[31] http://plus.google.com/

[32] http://www.linkedin.com/

[33] http://www.twitter.com/

[34] MySpace is another social networking site, but it is not often used by lawyers.

With all of these (and even more) outlets for online expression, it is not surprising that lawyers have been crossing the line when it comes to information posted online.

A. Identifying clients online

Illinois Assistant Public Defender Kristine Peshek was suspended from the practice of law in the spring of 2010 for content she posted on her blog, which was entitled, "The Bardd Before the Bar—Irreverant Adventures in Life, Law, and Indigent Defense." Her blog included stories of her defense activities, but she included clients in her posts, using either names or jail numbers that would have allowed them to be identified. She also admitted that one of her clients had lied to a court and she had not brought the lie to the Court's attention. Finally, she referred to one judge as an a**hole, and another as "clueless." She lost her job and was suspended from the practice of law for 60 days.

B. Florida lawyer disciplined for calling a judge names on a blog

Sean Conway was upset with Judge Cheryl Aleman for using procedural rules he thought deprived his clients of the right to a speedy trial. After filing complaints with the judicial watchdog agency without any observable results, he posted about his experiences on his blog.[35] Included in his posting were the following quotations:

> Recently, in an attempt to make defendants waive their rights to a speedy trial, Judge Cheryl Aleman has decided to set trials about 1-2 weeks after arraignment, hoping that defendants will move for a continuance, thereby waiving their right to a natural speedy trial.
>
> Today, Oct. 30th, I along with several other attorneys, had to endure her ugly, condescending attitude . . . Every atty tried their best to bring reason to that ctroom, but, as anyone who has been in there knows, she is clearly unfit for her position and knows not what it means to be a neutral arbiter.
>
> * * *
>
> As my case was on recall for 2 hours, I watched this seemingly mentally ill judge condescend each previous attorney.
>
> * * *

[35] http://jaablog.jaablaw.com/2006/10/30/judge-alemans-new-illegal-oneweek-to-prepare-policy.aspx

ME: "Judge (not your honor b/c there's nothing honorable about that malcontent) ... there seems to be a mistake in this case."

EVIL, UNFAIR WITCH ("hereinafter "EUW"): "and what is that?"

The Florida Bar found that Conway's post violated five ethics rules. Included were alleged violations of Florida Rules 4-8.2(a) ("A lawyer shall not knowingly make a false statement of fact concerning the qualifications, conduct or integrity of a judge" – New York's rule is the same, N.Y. R. Prof'l. Conduct 8.2(a)) and 4-8.4(d) ("A lawyer or law firm shall not . . . engage in conduct that is prejudicial to the administration of justice"). Conway initially defended himself on free speech grounds, but after the Florida Supreme Court rejected his argument, he eventually agreed to a public reprimand and a fine.

C. Admission Denied for Online Crime

Other online troubles can arise when people do things online that they may have never tried offline for fear of getting caught. In one case, a recent law school graduate waiting to take the bar exam was arrested for sexual solicitation of an underage girl online. He was unable to take the bar, but after completing a diversion program, the charges were dropped. He then applied to take the bar and was allowed, subsequently passing, but was then denied admission to practice. The Supreme Court of Louisiana stated:

> "[I]t is ordered that the petition for admission to the bar of Louisiana filed by petitioner, Philip R. Pilie, be and hereby is denied. It is further ordered that no applications for admission shall be accepted from petitioner in the future."[36]

D. Texas lawyer gets in trouble for asking for continuance for funeral then partying

In another case a Texas lawyer asked a judge for a continuance so that she could attend a funeral. She seemed to have forgotten, however, that she and the judge were "Facebook friends." While she really was attending a funeral, she also posted many times about going to parties, drinking, and generally having a good time. When she returned, she asked the judge for another continuance, which the judge denied.

[36] In re: Philip R. Pilie, On Application For Admission To The Bar, NO. 12-OB-1846, Louisiana Supreme Court (2012). *See also*, In re Kenneth Alan Goldman, Commission No. 201PR00028 (August 2012) (regarding internet solicitation and chatting with minors).

E. Posting False Negative Review Earns Reprimand

In a case in Minnesota, an attorney was publicly reprimanded (and paid costs) for "falsely posing as a former client of opposing counsel and posting a negative review about opposing counsel on a website."[37]

F. Responding to Negative Online Review with Confidential Information Earns Rejection of Reprimand

The Georgia Supreme Court rejected a voluntary reprimand for an attorney who disclosed client confidences online. The client posted negative reviews of the attorney online after dismissing her, and the attorney responded by disclosing details concerning the case. The Georgia Supreme Court noted that "a lawyer maintain confidentiality of information relating to the representation is a fundamental principle in the client-lawyer relationship" and rejected the reprimand as an appropriate sanction.[38]

G. Posting Fake Dating Ad for College Acquaintance Yields Suspension

A New York attorney who created a fake lesbian dating profile for a woman he knew in college years before was suspended by the Appellate Division, Second Department. According to the Court, "respondent's conduct was highly inappropriate and adversely reflects on the legal profession."[39]

H. Hiring a Secretary via Craigslist Is Fine; Asking for Sex as Part of the Job is not

A Chicago attorney was suspended from practice after he ran this Craigslist Ad advertising a vacant secretarial position with his firm:

> Loop law firm looking to hire an energetic woman for their open secretary/legal assistant position. Duties will include general secretarial work, some paralegal work and additional duties for two lawyers in the firm. No experience required, training will be provided. Generous annual salary and benefits will be provided, including medical,

[37] In re Petition for Disciplinary Action against Allison Wiles Maxim Carlson, a Minnesota Attorney, Registration No. 353784, MN Supreme Court, July 11, 2013, http://mn.gov/lawlib/archive/supct/1307/ORA131091-071113.pdf (PDF)

[38] *In re Skinner*, 292 Ga. 640, 740 S.E.2d 171 (2013)(note that the court was also clearly unhappy that details of the case, such as the actual items disclosed, were not part of the record in the case).

[39] *In re O'Hare*, App. Div. 2nd Dept. (July 11, 2013), http://www.nycourts.gov/reporter/3dseries/2013/2013_05320.htm

> dental, life, disability, 401(k) etc. If interested, please send current resume and a few pictures along with a description of your physical features, including measurements. We look forward to meeting you.

This ad isn't what led to the suspension, however. It was the follow-up E-mail that went to those who expressed an interest in the position:

> [I]n addition to the legal work, you would be required to have sexual interaction with me and my partner, sometimes together sometimes separate. This part of the job would require sexy dressing and flirtatious interaction with me and my partner, as well as sexual interaction. You will have to be comfortable doing this with us.

In addition, Chowhan indicated to applicants that they would have to "perform" during the interview, and initially denied that he had sent the E-mail (claiming he had been hacked).[40]

I. Judges can get in trouble, too

There are a number of judges who have run into problems with their online interactions in recent years. One is Ninth Circuit Chief Judge Alex Kozinski, known for his decisions in Cyberlaw cases. Judge Kozinski maintained a web page on a private server and on which he shared what he thought was humorous material, but which content was also at times risqué or sexually oriented. Unfortunately for the judge, who thought the web page was private, the webpage was publicly available.[41] An external ethics investigation (conducted by the Judicial Conduct panel for the Third Circuit) called Kozinski's actions "imprudent" but concluded without any further action following the judge's acceptance of responsibility and corrective actions following disclosure of the site.[42]

Chief Judge Cebull of the Montana Federal District Court also ran into trouble, but in a different way. Earlier this year he sent out an E-mail that contained a racist joke about President Obama's mother (and, by implication, the president himself).[43] After Judge Cebull sent the

---

[40] Lizzie Schiffman, Samir Chowhan, Illinois Attorney, Suspended Over Ad For Secretary Job With 'Sexual Aspect' [http://www.huffingtonpost.com/2011/12/02/samir-zia-chowhan-illinoi_n_1127022.html]

[41] 9th Circuit's chief judge posted sexually explicit matter on his website, L.A. Times, June 11, 2008, http://www.latimes.com/news/local/la-me-kozinski12-2008jun12,0,6220192.story

[42] http://www.ca3.uscourts.gov/opinarch/089050p.pdf

[43] Montana Federal Judge Reports Himself for Ethics Review After Admitting He Sent a Racist Email, ABA Journal: Law News Now, March 2, 2012, http://www.abajournal.com/news/article/montana_federal_judge_reports_himself_for_ethics_review_after_admitting_he_/

message, one of the recipients forwarded it on to the press, at which point the Judge was subjected to numerous public calls for his resignation. He then asked for an ethics investigation into his own behavior, [44] but before the investigation concluded, the Judge retired from the Bench.[45]

Judge McCree of Michigan was publicly censured for taking a cell phone picture of himself naked from the waist up and sending it to a court officer, and then not taking media reports and inquiries about the matter seriously. He allegedly responded to a reporter's questions about the photos by saying, "Hot dog, yep, that's me. I've got no shame in my game". According to the Michigan Supreme Court, Judge McCree "conducted himself in a flippant manner and did not give the interview the seriousness he should have. As a result, he brought shame and obloquy to the judiciary."[46]

In Texas, Judge Elizabeth Coker sent texts from the bench to an assistant district attorney who was observing a trial, instructing the ADA to pass the information to the ADA trying the case. Her actions eventually led to both a judicial commission investigation and an attempt to impeach her brought in the Texas House.[47]

VI. The Internet and Ethical Practice

A. The Firm Online

While we will not delve deeply into the specific rules for advertising and publicizing, there are some matters worth mentioning relating to oversight and involvement with law firm marketing. The first issue involves that identifier that is the new phone number: the domain name. A domain name is the "web address" or URL ("universal resource locator") used to identify websites. Must the web address match the firm name (with all of the limitations that

[44] Montana Judge to be investigated over anti-Obama e-mail, USA Today, April 6, 2012, http://www.usatoday.com/news/washington/story/2012-04-06/judge-racist-email-montana/54076036/1

[45] Fmr. Chief District Judge Cebull Retires, Email Scandal Over? April 4, 2013, http://blogs.findlaw.com/strategist/2013/04/fmr-chief-district-judge-cebull-retires-email-scandal-over.html?

[46] In re: Hon. Wade H. McCree, SC: 145895, RFI Nos. 2012-19839 , 2012-19863, Michigan Supreme Court (2012).

[47] Texas House Considers Impeachment Proceedings Against Judge, July 19, 2013, http://gaveltogavel.us/site/2013/07/19/texas-house-considers-impeachment-proceedings-against-judge/

matching would imply[48])? The answer comes directly from the rules themselves. RPC 7.5(e) provides:

> (e) A lawyer or law firm may utilize a domain name for an internet web site that does not include the name of the lawyer or law firm provided:
>
> (1) all pages of the web site clearly and conspicuously include the actual name of the lawyer or law firm;
>
> (2) the lawyer or law firm in no way attempts to engage in the practice of law using the domain name;
>
> (3) the domain name does not imply an ability to obtain results in a matter; and
>
> (4) the domain name does not otherwise violate these Rules.[49]

Thus domain names fit within the "motto" rule rather than the name rule for purposes of the Rules, and a firm can use a motto/trade name rather than the firm's precise practice name as its domain name.

The next issue involves responsibility for what the firm puts on the Web. Rule 7.1 prohibits lawyers from engaging in false advertising and in making false claims in their advertising, and as such forbids a lawyer "in the use or dissemination of any advertisement that: (1) contains statements or claims that are false, deceptive or misleading; or (2) violates a Rule." In addition, firms are required by Rule 5.3 to properly supervise non-lawyers in their employ. When a non-law employee at a firm in Louisiana "implied" on the firm's website that a former Louisiana governor was "a member of the firm, a governmental relations specialist, and a partner when in fact the former governor is not now nor has he ever been a licensed Louisiana attorney[,]" the firm's managing partner was disciplined for failing to oversee the non-law employee.[50]

---

[48] *See, e.g.,* New York State Bar Association Committee on Professional Ethics, Opinion 869 (May 31, 2011) ("A law firm may not include an area of law in the law firm name. A sole practitioner may use the terms "Firm" or "Law Firm" as part of the law firm name"). Note that this opinion specifically acknowledges that while under *Alexander v. Cahill*, 598 F.3d 79, 95 (2d Cir.), cert. denied, 131 S. Ct. 820 (2010), the ban on trade names as law firm names (as opposed to trade names as mottos) may be constitutionally suspect, the Committee will continue to apply it unless it is actually ruled unconstitutional.

[49] This last provision duplicates the introductory provision to this Rule found in Rule 7.5(a): "A lawyer or law firm may use internet web sites, professional cards, professional announcement cards, office signs, letterheads or similar professional notices or devices, provided the same do not violate any statute or court rule and are in accordance with Rule 7.1[.]"

[50] *In re Murphy J. Foster, III*, Supreme Court of Louisiana, Attorney Disciplinary Proceedings No. 10-B-2118 (Oct. 15, 2010).

A South Carolina practitioner also went astray of the rules when he misstated his qualifications (year of bar admission, experience in federal court) on his web page, and then continued those misrepresentations on sites such as LinkedIn and lawyers.com.[51]

Other things that are likely raise ethical concerns include the kinds of content that is permitted on a law firm website. Biographical data has been specifically approved, including past positions (with other law firms, for example). Favorable quotations from publications are also allowed, so long as they are not false, deceptive or misleading, and the required disclosures are present. [52]

Within the otherwise broader category of allowable content are links posted on a firm website. Recently the N.Y. Bar Association has concluded that, "A lawyer may include links to other businesses on the lawyer's web site provided neither the link nor the linked material involves misrepresentation or causes confusion."[53] Generally, links are allowed to offsite resources not under the control of the lawyer, but the purpose of the link, the nature of the linked site, and the relationship of the lawyer to the owner of the linked site are all relevant to any ethical inquiry. Informational sites are acceptable, but reciprocal links raise additional concerns. Where the reciprocal link constitutes advertising, the link is subject to Rule 7.1's advertising provisions and a link that is part of a cooperative business arrangement subjects the link to rule 5.8(a).

In addition, use of online discounters such as GroupOn and LivingSocial have been approved in a New York State Bar Association Committee on Professional Ethics,[54] citing with

[51] Newly Licensed Solo Reprimanded for Exaggerating Experience in Online Profiles, ABA Journal: Law News Now, February 1, 2012, http://www.abajournal.com/news/article/newly_licensed_solo_reprimanded_for_exaggerating_experience_in_online_profi/

[52] See, N.Y.S. Bar Association, Committee on Professional Ethics, Opinion 877 (September 12, 2011); note that the requirements of Rule 7.1 will apply when the maker of the quotation is paid, and that, in addition, the rules of the Federal Trade Commission on online disclosures will also be likely to apply (these require disclosure of payment for advertising or for a variety of other situations where payment may imply an undisclosed conflict of interest. *See,* 16 C.F.R. Title 16: Commercial Practices).

[53] NYS Bar Association, Committee on Professional Ethics, Opinion 888 (November 15, 2011).

[54] NYS Bar Association, Committee on Professional Ethics, Opinion 897 (December 13, 2011).

general approval a South Carolina ethics opinion that reached the same conclusion.[55] Such uses are subject to the standard attorney advertising requirements (such as labeling as attorney advertising and not being disceptive), as well as additional concerns regarding when a lawyer can keep the payment without actually rendering services (issues that the attorney should make sure are covered by the advertising agreement, a point not explicitly noted in the NYSBA Ethics Committee opinion). Advertising by text messaging has likewise been approved in the State of Ohio.[56] Note that not all online arrangements are likely to be so easily approved. Michigan has rejected the idea of lawyers paying a referral fee to for-profit websites where the fee structure is specifically linked to the referrals in question.[57]

B. Electronic Errors Are Bound to Happen

Misdirected E-mail is a fact of life in the information age. What happens when one lawyer receives a message clearly intended for an opposing party or attorney? In *Terraphase Engineering, Inc. v. Arcadis*, No. C 10-04647 JSW (N.D. Ca. 2010), the plaintiff's attorney mistakenly sent confidential information to an inside counsel for the defendants (due to not catching an improperly completed "autocomplete" address on the E-mail prior to sending it). Defendant used the information to form a counterclaim in the litigation, and plaintiff moved for a protective order, seeking to disqualify various lawyers involved in the action from continuing. Judge Jeffrey White granted the motion and issued an order disqualifying a defendant's inside, associate corporate counsel, along with the law firm currently representing the client, due to their reading of E-mail messages clearly intended for the opposing parties in the litigation. The Judge also removed the defendant's General Counsel from overseeing the litigation.[58]

[55] South Carolina Bar, Ethics Advisory Opinion 11-05 (2011); *see also*, State Bar of Arizona, Opinion 13-01: Internet Marketing Vouchers or Coupons (2013)(approving Groupon style discounters in theory but noting the practical difficulties of their ethical use).

[56] Supreme Court of Ohio, Board of Commissioners on Grievances & Disciplines, Opinion 2013-02: Direct Contact with Clients: Text Messages (2013) (distinguishing text messages from more direct, or "real time" communications with potential clients.

[57] State Bar of Michigan, Ethics Opinion, RI-365 (2013).

[58] *See*, Beware the Evolving Ethics of Reviewing E-mails, edd blog online (March 8, 2011); http://eddblogonline.blogspot.com/2011/03/beware-evolving-ethics-of-reviewing-e.html; *see also*, The Association of the Bar of the City of New York Committee on Professional Ethics, Formal Opinion 2012-1: Obligations Upon Receiving a Document Not Intended for the Recipient (2012)(noting that reading a misdirected message is not violative of ethics rules, but even reading privileged information may be).

The resulting message is clear: errors happen, but judges are unlikely to allow clients to benefit from reasonable errors made by the attorneys on the other side.

C. E-mail is not a Phone Call

Where two attorneys engaged in inappropriate and abusive E-mail exchanges during the course of litiation, those E-mail messages were not only used in their disciplinary proceeding, but were attached to the complaint filed with the disciplinary board. In this particular situation, the lawyers were allegedly attempting to schedule various aspects of an ongoing litigation matter, but were having what might be rather charitably defined as "difficulties." Short-tempers turned to snark, and snark turned to insults and exchanges including the following took place (among others). Defendant's attorney addressed Plaintiff's attorney as "Sparky" and Plaintiff's attorney responded by referring to defendant's attorney as "Corky."

Plaintiff's attorney also wrote the following to Defendant's attorney: "You are an ass clown and absolutely an ass clown. Shouldn't you be tending to your retarded son and his 600th surgery or something instead of sending useless E-mails. [sic] In fact, I think I hear the little retards [sic] monosyllabic grunts now; Yep, I can just barely make it out; he is calling for his ass clown. How sweet." This message followed an earlier one from the Defendant's attorney that included the following: "If you need to find indications of the 'retardism' that you seek, I suggest you look in the mirror, and then look at your wife . . . she has to be a retard to marry such a loser like you" and "Unfortunately, it looks like the better part of you was the sperm cells left on the back seat of the Ford Pinto."

The lawyers were both disciplined; the Defendant's lawyer received a public reprimand and was required to take a class in professionalism, while Plaintiff's attorney was suspended for 10 days and required to take an anger management class.[59]

In another case, a Texas lawyer referred to his opponent's attorney as a pansy and threatened him using vulgar language, again during scheduling of a deposition and various

[59] Note that this can happen in person, as well. *See*, Complaint in the Matter of David Alan Novoselsky, Before the Hearing Board of the Illinois Attorney Registration and Disciplinary Commission, Commission No. 2011PR00043 (September 2012), where the respondent was charged with calling opposing counsel and "bitch" and a "slut" while in a courtroom and during legal negotiations.

discovery disputes. The Texas lawyer lost his position as a partner at the firm and a sanctions motion was brought against him by opposing council.[60]

Finally, a Virginia lawyer was ordered to attend a "non-internet" anger-management course after sending an E-mail to a counsel who had been opposing counsel in an earlier case after that counsel was later indicted on an unrelated matter. The E-mail included suggestions that the attorney would comfort the receiver's wife while he was in prison, and that he (the indicted attorney) should look forward to being victimized in prison.[61]

The lesson here is that while exchanges such as these may have taken place between lawyers in the past, they were far more likely to have been part of an in-person or telephone conversation. As we move to more use of electronic communications, lawyers should be aware that E-mail is written, potentially permanent, and easily shared. An E-mail is not a phone call, and appropriate levels of decorum and professionalism must be shown by lawyers engaged in using electronic communications technologies.

As an aside, note that if addressed to the substance of an argument, rather than framed as a personal attack, such comments and "name calling" may be acceptable given current norms in U.S. Supreme Court Practice.[62]

D. Encryption and Electronic Transactions

While some messages may be misdirected or mislaid, others may fall into the hands of hackers or others who "overhear" the electronic communications. Lawyers are required to maintain client confidentiality, but to date ethics committees have not required lawyers to use encryption technology – technology that "locks up" messages and only allows unlocking with a key – while engaging in electronic communications. In 2010, the NYS Bar Association Committee on Professional Ethics issued its opinion that "A lawyer may use an online data

[60] Sanctions Motion Accuses Ex-Cozen Partner of Taunting 'Pansy' Opposing Counsel in Abusive Emails, ABA Journal: Law News Now, May 17, 2012, http://www.abajournal.com/news/article/sanctions_motion_accuses_ex-cozen_partner_of_taunting_counsel/

[61] Lawyers ordered to anger management, July 5, 2013, http://valawyersweekly.com/vlwblog/2013/07/05/lawyers-ordered-to-anger-management/

[62] For example, Justice Scalia, in his dissenting opinion in *Sykes v. United States*, wrote: "That incompatible variation has been neither overlooked nor renounced in today's tutti-frutti opinion." *Sykes v. United States*, slip op., Dissenting Opinion of Justice Scalia, p. 3. If calling majority opinions "tutti-frutti" is acceptable for a sitting Supreme Court Justice, it is hard not to argue that professional norms of civility have shifted away from politeness in recent years.

storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6."[63] The opinion also imposes a duty on the lawyer to follow current technology to ensure confidentiality is retained in the face of technological change. The opinion is consistent with other state bar opinions, such as those of California[64] and Alabama.[65]

The NYS Bar opinion sets out four elements that are relevant to making the determination of whether confidentiality is reasonably assured:

> 1. Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
>
> 2. Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
>
> 3. Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or
>
> 4. Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

The rules thus would seem to require a storage provider that provides confidentiality and that also provides portable data rather than proprietary data storage solutions. Other jurisdictions have reached similar results, though at times with subtle differences in articulation and detail.[66]

[63] NYS Bar Association, Committee on Professional Ethics, Opinion 842 (September 10, 2010).

[64] State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179 (2010).

[65] Alabama Ethics Opinion 2010-2 (2010).

[66] *See, e.g.,* Professional Ethics Committee of the Florida Bar Op. 10-2 (2011); Pennsylvania Bar Association Ethics Opinion No. 2010-060 (2010); Iowa State Bar Association Committee on Practice Ethics and Guidelines, Ethics Opinion 11-01 (2011).

These opinions are consistent with earlier opinions that did not require encryption in E-mail use, but still required the lawyer to follow practices intended to safeguard confidentiality.[67] Note that after the ABA Commission on Ethics 20/20 proposed changes to the Model Rules of Professional Conduct intended to further alter the duties placed on lawyers in relation to electronic communications emphasizing that lawyers must be aware of, understand, and make reasonable decisions about the technologies they use.[68] The rule was adopted, with new Model Rule 1.1 reading:

> *A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.*

And an amended comment 8 to Model Rule 1.1 reading:

> *To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.*

In addition to being competent when it comes to technology, a lawyer may have to help clients maintain competence, as well. When working with a client who is using employer provided E-mail, a lawyer may have an obligation (especially if the matter involves the employer) to notify the employee that E-mail communications may not be private and that they attorney client privilege may be waived when using employer provided E-mail.[69]

E. Being in Two Places at Once

A lawyer from Ohio established "a relationship" with a law firm in Florida that worked on cases involving consumer debt. As part of the relationship, the Ohio lawyer provided the Florida firm with his Ohio bar registration number and his electronic signature. The Florida firm used these details in cases without the lawyer's permission. The Ohio lawyer was suspended from

[67] *See*, *e.g.,* NYS Bar Ass'n, Committee on Professional Ethics, Opinion 709 (Sept. 16, 1998); *see also,* Assn'of the Bar of the City of New York Opinion 1998-2 (December 21, 1998).

[68] ABA Commission on Ethics 20/20 Initial Draft Proposals – Technology and Confidentiality (May 2, 2011) [see appendix for text of the proposed changes]

[69] American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 11-459 (August 4, 2011); *see also*, "Law Firms are Pressed on Security for Data," NY Times, March 26, 2014 (noting client pressure on law firms to secure computer and networking of data) http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/

practice for six months, but the suspension was stayed so long as he did not engage in further misconduct.[70]

F. Being in One Place and not Another

We all know that technology can be a distraction in modern life, but sometimes it can also lead to ethical violations. An attorney who was trying to arrange a settlement but who had not been able to reach his client about the matter went to court on the return date to appear. While outside the court room on his cell phone trying to reach his client, the attorney missed the case being called on the docket. The opposing attorney responded to the call and a default judgment was entered against the attorney's client. While the attorney argued he was trying to sort the matter out while he was out of the courtroom, by failing to check the status of the case with the clerk and to follow-up with the clerk before he left the courtroom he committed misconduct and was suspended from the practice of law for 60 days.[71]

G. Working Two Places at Once

In another case that would have been nearly impossible to imagine before the Internet arrived on the scene, an attorney working for the State of Kentucky was disciplined when he used State resources – time and the office's Westlaw account – to earn money by posting answers to legal questions on JustAnswer.com, an online question and answer forum. The Supreme Court of Kentucky publicly reprimanded the respondent for his actions. [72]

H. More problems with E-mail

In two separate cases, attorneys sent photos via E-mail or posted them on Facebook (thinking they were limited to just friends). In the first case, an attorney handling a wrongful death case sent a picture of the dead body to a friend and included disparaging remarks. As the

[70] Disciplinary Counsel v. Lorenzon, Slip Opinion No. 2012-Ohio-4713

[71] Attorney Grievance Commission of Maryland v. John Wayne Walker-Turner, Misc. Docket, AG No. 16, September Term, 2011 (this was Walker-Turner's second brush with discipline; he had earlier received a 30 day suspension for unrelated conduct).

[72] Matthew Scott Finley Movant v. Kentucky Bar Association, Supreme Court of Kentucky, 2012-SC-000465-KB (October 2, 2012)

firm monitored E-mail, the message was seen and his firm reported him to the disciplinary authorities.

In the second case, a public defender in Florida posted a photo of a client's underwear on Facebook. According to the Miami Herald:

> *[Defendant's] family brought him a bag of fresh clothes to wear during trial. When Miami-Dade corrections officers lifted up the pieces for a routine inspection, Recalde's public defender Anya Cintron Stern snapped a photo of Recalde's briefs with her cellphone, witnesses said.*
>
> *While on a break, the 31-year-old lawyer posted the photo on her personal Facebook page with a caption suggesting the client's family believed the underwear was "proper attire for trial."*

The posting led to a mistrial in the case (and the attorney was fired, as well). [73]

In a similar vein, the attorney defending George Zimmerman in the Trayvon Martin shooting case in Florida was pictured eating ice cream on his daughter's Instagram page with a caption that read, ""We beat stupidity celebration cones." #zimmerman #defense #dadkilledit The attorney later apologized for the posting.[74]

I. Trying to Influence Public Perception by Posting Criminal Discovery Video Online

A lawyer in Illinois tried to convince the public that his client had been framed, with police planting drugs on his client. The video, which the attorney received during discovery, was posted to YouTube and then linked from Facebook, where it received more than 2,000 views before a judge ordered it removed. The complaint alleged that the attorney violated rules relating to discovery materials. That the attorney took all of the relevant actions without informing the client, let alone obtaining the client's permission, was also noted in the complaint.[75]

[73] Lawyer's Facebook photo causes mistrial in Miami-Dade murder case, Miami Herald, Sept. 9, 2012, http://www.miamiherald.com/2012/09/12/2999630/lawyers-facebook-photo-causes.html

[74] Zimmerman attorney says daughter's Instagram post 'immature and insensitive,' apologizes, http://dailycaller.com/2013/06/29/zimmerman-attorney-says-daughters-instagram-post-immature-and-insensitive-apologizes/#ixzz2dyp4uFpT

[75] http://www.abajournal.com/news/article/ethics_complaint_claims_lawyer_tried_to_sway_potential_jurors_by_posting_di/; https://www.iardc.org/12PR0006CM.html; http://lawprofessors.typepad.com/legal_profession/2012/02/the-illinois-administerator-has-filed-a-complaint-allegingmisconduct-byan-attorney-who-represented-a-drug-defendant-the-com.html

J. Westlaw Access Not Allowed After Leaving Position

An attorney had helped his legal employer enter into an agreement with Thomspon-Reuters for the use of Westlaw. On leaving his position, the attorney tried to cancel the arrangement, but Westlaw would not allow cancellation of the contract, so the old office maintained payments on the contract. The attorney, who retained his Westlaw ID, began using the account when he took up his new legal position. His use was discovered and an ethical complaint was filed. The Supreme Court of Oregon, in reviewing a claim for reciprocal discipline (the misconduct occurred in Hawaii, and respondent was admitted in both Hawaii and Oregon), publicly reprimanded the responded for his actions.[76]

K. With Computers You Can Make Stuff Up (but shouldn't)

An attorney who was involved in a proceeding related to her children forged, in the words of the Court, "from whole cloth," an order of a court in New Jersey to show to authorities in Colorado. In discovering the forgery, ethics charges were brought and the respondent was publicly reprimanded for her actions.[77]

L. What's on the Web Can Be Found

When an attorney who was suspended from the practice of law continued to practice, it didn't take long before a magistrate found the listing of his suspension on the Supreme Court's website. A client also found the listing. Both the magistrate and the client notified the disciplinary authorities, and the attorney was suspended from the practice of law for two years (one year stayed if the attorney followed the required course of action outlined by the Court).[78]

In another case, an attorney who failed to take any action on a case while continually assuring the client that the case was underway – even after it was dismissed – was indefinitely

[76] In re The Reciprocal Discipline of EVERETT WALTON, Accused, OSB 12-70; SC S060606, Supreme Court Of The State Of Oregon (October 11, 2012).

[77] In The Matter Of Mara Yoelson, A/K/A Mara Yoelson Olmstead, Supreme Court Of New Jersey, Disciplinary Review Board, Docket No. DRB 12-018, District Docket No. XIV-2010-0296E, and VII-2011-0900E (April 19, 2012) (filed Sept. 5, 2012)

[78] Disciplinary Counsel v. Seabrook, 133 Ohio St.3d 97, 2012-Ohio-3933 (2012).

suspended by the Maryland Court of Appeals for his actions. The client found out about the true status of the case when she searched for the case on the Maryland case search website.[79]

M. You Can't Get Rid of What's on Facebook, But You Can Try (Though Maybe You Shouldn't)

An ethics opinion from the New York County Lawyers Association provides guidance for counseling clients on social media content. The opinion addresses the following:

> *It is the Committee's opinion that New York attorneys may advise clients as to (1) what they should/should not post on social media, (2) what existing postings they may or may not remove, and (3) the particular implications of social media posts, subject to the same rules, concerns, and principles that apply to giving a client legal advice in other areas*

While the answer to each is yes, it is a very soft, qualified yes, with quite a few caveats. Attorneys may not participate in the creation of false evidence, cannot suppress evidence, and cannot destroy evidence (evidence being material related to litigation). That said, the overall conclusion is that social media is part of the litigation strategy of the modern age, and lawyers can and should deal with it explicitly, though ethically.[80]

A Virginia lawyer could have been aided by the NYCLA's qualms, but confronted the issue of Facebook deletions prior to the opinion's issuance. The lawyer counseled his client to delete Facebook posts and content while the client was involved in litigation to which the Facebook content was relevant. Considered spoliation of evidence, the court reduced a wrongful death jury award and the lawyer was subsequently suspended from the practice of law for five years.[81]

[79] Client Learns Case Dismissed Through Online Search, July 5, 2013, http://lawprofessors.typepad.com/legal_profession/2013/07/client-learns-case-dismissed-through-online-search.html

[80] NYCLA Ethics Opinion 745 (July 2, 2013) [pdf], http://www.nycla.org/siteFiles/Publications/Publications1630_0.pdf; New York Ethics Opinion: Lawyers May Advise Clients to Delete Social Media Content, Legal Ethics Forum, July 19, 2013, http://www.legalethicsforum.com/blog/2013/07/new-york-ethics-opinion-lawyers-may-advise-clients-to-delete-social-media-content.html

[81] 5-Year Suspension For Telling Client To Delete Facebook Information, SBMBlog, August 12, 2013, http://sbmblog.typepad.com/sbm-blog/2013/08/5-year-suspension-for-telling-client-to-delete-facebook-information.html#sthash.FpLUzyis.dpuf

N. Friends, Following, and Linking-in: Connections in a Connected World

There are a variety of ways in which connecting to others online may implicate ethical requirements. Ethics opinions are split, for example, as to whether judges can friend lawyers who appear in their courts, with Florida deciding against[82] and New York allowing judges to join social networks and make such contacts where otherwise within the rules.[83] Note that at least one judge in North Carolina has been reprimanded for exchanging *ex parte* messages on Facebook concerning an ongoing case with an attorney on the case.[84] A judge who initiated a friend request with a litigant was disqualified from ruling on the case in question.[85]

As for attorneys, the questions that arise tend to be concerned more with whether information can be ethically gleaned from public web pages and public areas of social networking sites (NY has concluded it can)[86] and whether a lawyer or a lawyer's agent/employee can seek to "friend" a witness or other interested party who is unrepresented by a lawyer (friending someone represented by a lawyer would violate rules requiring that a lawyer avoid communicating directly with someone who is represented by a lawyer).

On this latter point, the Philadelphia Bar Association has issued an opinion that prohibits the practice of friending someone to gain information about them or matters related to litigation. The Bar Association opinion finds that seeking to friend someone while omitting the critical information as to why that friend request is being sent is deceptive in violation of Rule

[82] Florida Supreme Court, Judicial Ethics Advisory Committee, Opinion Number 2009-20 (Nov. 17, 2009).

[83] New York State Judicial Ethics Commission, Opinion 08-176 (Jan. 29, 2009); *see also,* American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 462, "Judge's Use of Electronic Social Networking Media (Feb. 21, 2013) (concluding that judges should be allowed to use social media, and that being "friends" does not immediately disqualify a judge in a case involving that attorney friend, but that judges must be cautious and watch for potential violations of judicial ethics).

[84] *See*, Judge Reprimanded for Friending Lawyer and Googling Client, ABA Journal Law News (June 1, 2009); http://www.abajournal.com/news/article/judge_reprimanded_for_friending_lawyer_and_googling_litigant/

[85] "Judge Must Recuse After Initiating Facebook Friend Request to Litigant–Chace v. Loisel" Legal Ethics Forum, January 28, 2014.

[86] New York State Bar Association, Committee on Professional Ethics , Opinion 843 (September 10, 2010); note that this opinion applies only to *publicly available* information. The NYS Bar Association has not weighed in on the discussion regarding friending, below.

4.2.[87] The NYC Bar Association, on the other hand, has issued a contrary opinion, and argues that the situation is like one that arises when a person sitting in a bar is approached by a lawyer's investigator. The investigator has no obligation to immediately disclose he or she is an investigator, but rather may engage the person in conversation hoping to uncover relevant information (so long as the investigator is not deceptive). In the same regard, the opinion opines, so may a person send a "blank" friend request to an unrepresented person as the blank request is not itself deceptive, and the person accepting that friend request and opening up their social networking activities to the investigator is the person taking the risk that the stranger asking to friend them does not have their best interests at heart.[88]

Another social networking issue to consider is the extent to which lawyers can interact with jurors via social networking or other communications technologies. The New York County Bar Association Committee on Professional Ethics has approved searching publicly available information on prospective jurors both prior to and during a trial.[89] Analogizing the situation to that which confronts lawyers who might wish to investigate other parties in litigation, the Committee concluded, "we conclude that passive monitoring of jurors, such as viewing a publicly available blog or Facebook page, may be permissible." That conclusion does not change for searching for information about jurors during trial, but notes that in this case, as lawyers are prohibited from talking to jurors during the pendency of litigation, the lawyer must take extra precautions to ensure that the juror does not become aware of the attorney's efforts. [90]

In this respect, fully understanding how a particular technology platform works is critical to the situation. Despite repeated appearances of claims to the contrary on Facebook, Facebook users are not aware when someone has viewed their public profile pages.[91] LinkedIn, however, allows you to see not only that "someone" has viewed your LinkedIn profile, but who that person is (if that person was LinkedIn member signed in at the time they viewed the profile). Checking

[87] Philadelphia Bar Association, Professional Guidance Committee, Opinion 2009-02 (2009); *see also*, San Diego County Bar Association, SDCBA Legal Ethics Opinion 2011-2, agreeing with the Philadelphia opinion, but based on a different provision, as California has not adopted the relevant ABA Model Rules as part of its ethics framework.

[88] Ass'n of the Bar of the City of New York, Committee on Professional Ethics, Formal Opinion 2010-2 (2010). Note that the opinion does not allow for any deception in seeking information in this regard.

[89] NYCLA Committee on Professional Ethics, Formal Opinion No. 743 (May 18, 2011).

[90] *Id.*, at page 3.

[91] *See*, *e.g.*, Cluley, Want to see who has viewed your Facebook Profile? Take Care…, Sophos "NakedSecurity Blog" July 23, 2010 [http://nakedsecurity.sophos.com/2010/07/23/viewed-facebook-profile-care/]

a juror's public Facebook page would be allowed under the County Bar's opinion, checking a juror's LinkedIn profile while logged in to LinkedIn would not. The American Bar Association has agreed in part with this reasoning – noting that lawyers can read juror social media postings and content – but disagreeing that simply because a juror may become aware of the lawyer's efforts the lawyer has "communicated" with a juror.[92]

Understanding the nature of the sites and the way they are structured – and the way they structure your information and your public facing profile – is also important.[93] LinkedIn, for example, currently provides an option for connections to recognize your skills and to be endorsed for your knowledge. LinkedIn has in the past included categories labeled "skills and expertise" and "specialties." These raised issues for lawyers as words like "specialty" are often viewed with skepticism by bar ethics committees. In these circumstances, the Philadelphia Bar Association opined that lawyers could list their practice areas under "skills and expertise," and could even rank their proficiency in those areas,[94] but could not indicate that they were "experts" in any particular areas. The New York State Bar Association Committee on Professional Ethics issued an opinion in the summer of 2013 that lawyers certified as specialists could list those areas under LinkedIn's "specialist" category, but limited that holding to individual lawyers, not firms, as firms cannot be certified as specialists.[95] Florida took a predictably conservative line, disagreeing with Philadelphia's conclusions in issuing guidelines for attorneys indicating that Florida attorneys who were not certified specialists should not list their practice areas under the "skills and expertise" category.[96] Even LinkIn's new formulation – endorsements – can raise

[92] American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 466: Lawyer Reviewing Jurors' Internet Presence (April 24, 2014).

[93] *See*, Nicole Black, Social Media, Ethics, and "Expertise": What's a Lawyer to Do? Law Practice Today, American Bar Association (November 2013) [http://www.americanbar.org/content/newsletter/publications/law_practice_today_home/lpt-archives/november13/social-media-ethics-and-expertise.html]; *see also,* Carolyn Elefant, Why New York's Recent Ethics Opinion on LinkedIn Shows the Folly of Regulating the Minutia of Social Media (August 30, 2013) [http://myshingle.com/2013/08/articles/ethics-malpractice-issues/why-new-yorks-recent-ethics-opinion-on-linkedin-shows-the-folly-of-regulating-the-minutia-of-social-media/]

[94] Philadelphia Bar Association, Professional Guidance Committee, Opinion 2012-8 (Nov. 2012).

[95] New York State Bar Association, Committee on Professional Ethics , Opinion 972 (July, 2013); note that LinkedIn subsequently changed its categorization system such that individual lawyers can no longer list specialties.

[96] The Florida Bar Standing Committee on Advertising, Guidelines for Networking Sites (April 16, 2013); The Florida Bar, Advisory Letter (Sept. 11, 2013).

problems where they suggest endorsements and connections endorse you for experience or expertise you don't actually have.[97]

As a final, and closing, note, online social networking sites are opening new opportunities that may implicate the rules in new and unique ways. For example, in an opinion from June of last year (2011), the New York State Bar Association, Committee on Professional Ethics, concluded that an attorney can offer a prize as an incentive for others to join the attorney's social network (with caveats, of course, such as that the lawyer not require the prize seeker to retain the lawyer, and that the lawyer award the prize randomly, among others).[98] This is the kind of situation that likely would have never arisen before the Internet became a part of everyday legal practice. No one would have had an opportunity to give a prize to others for "connecting" with them. Today, however, those opportunities are prevalent, and benefits of pursuing them – such as having an established network of people with whom to communicate legal practice news and events – are becoming clearer. The ethics committees have so far done a good job keeping up with technological changes and whether/how they affect law practice (the uncertainty of "friending" non-party witnesses aside), and it is important to keep up with developments in this area of professional conduct as technology and the law march forward.

[97] *See*, Dennis Kennedy, Is LinkedIn's Endorsement Feature Ethical for Lawyers? LawNewsNow, ABA Journal (Dec. 1, 2013) [http://www.abajournal.com/magazine/article/linkedin_endorsement_feature_draws_some_questions]

[98] NYS Bar Association, Committee on Professional Ethics, Opinion 873 (June 9, 2011).