PRACTICAL ISSUES INVOLVING SOCIAL MEDIA IN INSURANCE CLAIMS

Andrew L. Smith, Esq.

SMITH, ROLFES & SKAVDAHL COMPANY LPA

CINCINNATI, OH | COLUMBUS, OH | DETROIT, MI | FT. MITCHELL, KY | ORLANDO, FL | SARASOTA, FL

www.smithrolfes.com

I. Introduction

- Currently, over 750 million people use Facebook, over 175 million use LinkedIn, and over 100 Million use MySpace.

- Each month people spend over 750 billion minutes on Facebook, and during this time three billion photos and 180 billion posts are uploaded to Facebook.

- If Facebook were a country it would be the third most populated country in the world (behind China and India, and ahead of the United States).

II. Social Media is a Gold Mine of Information

A. Evidence at Trial

- Social media posts, comments, and photos can be used as evidence at trial to attack a witness's credibility, to show a witness's state of mind, to dispute damages, etc.

- Example: A plaintiff filed suit against a chair manufacturer alleging that she suffered permanent injuries restricting her from leaving her home. The court allowed discovery of the plaintiff's Facebook and MySpace accounts. Facebook pictures revealed the plaintiff standing happily outside of her home, and were detrimental to the plaintiff's case. *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (N.Y. 2010).

- Example: A Starbucks employee was fired for inappropriate conduct and threatening violence to fellow employees. The employee then sued Starbucks for sexual harassment, religious discrimination, and retaliation. The employee's MySpace page was submitted as evidence by Starbucks, where plaintiff stated: "Starbucks is in deep s**t with GOD!!! ...I will now have 2 to turn 2 my revenge side (GOD'S REVENGE SIDE) 2 teach da world a lesson about stepping on GOD. I thank GOD 4 pot 2 calm down my frustrations and worries or else I will go beserk and shoot everyone...." Based on the evidence submitted by Starbucks, the court granted summary judgment in its favor. *Mai-Trang Thi Nguyen v. Starbucks Coffee Corp*, 2009 U.S. Dist. LEXIS 113461 (N.D.Cal. 2009).

B. Juror Investigation

- Lawyers are now using social media to investigate potential jurors.

- Example: Amber Hyre, a juror in a West Virginia case in 2008, did not disclose that she was Myspace friends with the defendant, a police officer being tried on criminal charges. After the relationship came to light, a state appeals court threw out the defendant's conviction and ordered a new trial.

- Example: In March 2009, Stoam Holdings, a building products company being sued for allegedly defrauding two investors, asked an Arkansas court to overturn a $12.6 million judgment, claiming that a juror used Twitter to send updates during the civil trial. The juror, Jonathan Powell, sent Twitter messages including, "oh and nobody buy Stoam. Its bad mojo and they'll probably cease to Exist, now that their wallet is 12m lighter" and "So Jonathan, what did you do today? Oh nothing really, I just gave away TWELVE MILLION DOLLARS of somebody else's money." The trial court denied the motion seeking to overturn the verdict and the attorneys are currently appealing.

- Example: In a Michigan case, a 20 year old juror disclosed her verdict opinion on her Facebook page: "Gonna be fun to tell the defendant they're GUILTY." The juror was charged with contempt, fined $250.00, required to write a 5-page essay on the Sixth Amendment, and removed from the jury. The violation was discovered by the defendant's son, who just happened to be searching for the jurors on Facebook.

- Example: In December 2009, Baltimore Mayor Sheila Dixon was convicted by a jury of embezzlement for stealing gift cards. After the verdict, her lawyers initially asked for a new trial in part because five of the jurors were communicating among themselves on Facebook during the deliberation period, and at least one of them received an outsider's online opinion regarding how the jury should decide the case.

- Jurors' inappropriate use of the internet, including postings on Facebook and Twitter, has led to 21 mistrials in the past two years.

- California and Florida have implemented new jury instructions to advise jurors not to discuss an active case through social media.

- Example: When jurors were chosen for the perjury trial of baseball star Barry Bonds, they were barred from using social media as they considered the case.

III. Methods and Scope of Permissible Discovery

A. Social Media is Discoverable

- Civ.R. 26 and 34: A party may request relevant, non-privileged electronically stored information that is within the possession, custody, or control of the responding party.

- Courts allow discovery of personal information posted on a social networking website if it is relevant to the litigation and the discovery request is narrowly tailored.[1]

- One court compelled interrogatory responses disclosing a party's social networking website usernames, logins, and passwords. *McMillen v. Hummingbird Speedway, Inc.*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. 2010).

---

[1] *See United States v. Villanueva*, (11th Cir. Feb. 15, 2009), 2009 U.S. App. LEXIS 3852; *Beye v. Horizon Blue Shield of New Jersey* (D.N.J. 2008), 568 F.Supp.2d 556; *Ledbetter v. Wal-Mart Stores, Inc.* (D.Col. Nov. 13, 2009), 2009 U.S. Dist. LEXIS 113117; *Romano v. Steelcase, Inc.* (N.Y. 2010), 907 N.Y.S.2d 650; *McMillen v. Hummingbird Speedway, Inc.* (Pa. Sept. 9, 2010), 2010 Pa. Dist. & Cnty. Dec. LEXIS 270; *EEOC v. Simply Storage Mgt., LLC*, (S.D.Ind. May 11, 2010), 2010 U.S. Dist. LEXIS 52766; *Bass v. Miss Porter's School* (D.Conn. Oct. 27, 2009), 2009 U.S. Dist. LEXIS 99916; *Mackelprang v. Fidelity Natl. Title Agency of Nevada, Inc.* (D.Nev. Jan. 9, 2007), 2007 U.S. Dist. LEXIS 2379. Several Ohio and 6th Circuit cases have relied on information from social networking websites in their opinions. *See State v. Gaskins*, 9th Dist. No. 06CA0086-M, 2007-Ohio-4103; *Burns v. May*, (1999), 133 Ohio App.3d 351, 728 N.E.2d 19; *State v. Berry* (2008), 145 Ohio Misc.2d 55, 882 N.E.2d 502. However, no Ohio or 6th Circuit cases discuss the discoverability of information located on social networking websites in detail.

See also Canadian Courts: Leduc v Roman (Feb. 20, 2009), 2009 CarswellOnt 843 (court noted that it was "beyond controversy" that a person's Facebook pages may contain relevant documents; that other Canadian cases had permitted into evidence photographs posted on a person's Facebook page; it is reasonable to infer from the social networking purpose of Facebook, that even if a person only maintains a private profile with the public profile merely listing their name, that relevant information exists on their limited-access private pages); *Kent v Laverdiere* (ON.S.C., Apr. 14, 2009), 2009 CanLII 16741 (as plaintiff asserted that accident disfigured her and lessened her enjoyment of life, any photos on Facebook or MySpace showing her in healthy state, enjoying life, would be relevant); *Bishop v Minichiello* (CanLII, Apr. 7, 2009), 2009 BCSC 358 (defendant's motion for production of plaintiff's computer's hardrive so it could analyze how much time plaintiff spent on Facebook granted as the information sought was relevant to the issues in the case); *Goodridge v King* (ON.S.C. Oct. 30, 2007), 2007 CanLII 51161 (in action in which plaintiff claimed various injuries including loss of enjoyment of life and disfigurement following a car accident, photos posted by plaintiff on her Facebook account was evidence to the contrary, showing her socializing and dating); *Kourtesis v Horis* (ON.S.C. Sept. 24, 2007), 2007 CanLII 39367 (in proceeding concerning costs, court noted that during trial, Facebook photos of plaintiff were important element of case; apparently plaintiff testified that she no longer had a social life because of her injuries, yet the photographs taken after the accident, showed her at a party).

- Courts generally hold that users of social networking websites lack a legitimate expectation of privacy in the materials intended for publication or public posting.[2]

- Facebook policy states that "it helps you share information with your friends and people around you," and that "Facebook is about sharing information with others." http:www.facebook.com/policy.php.

- MySpace is a "social networking service that allows Members to create unique personal profiles online in order to find and communicate with old and news friends;" and, is self-described as an "online community" where "you can share photos, journals and interests with your growing network of mutual friends," and, as a "global lifestyle portal that reaches millions of people around the world." http://www.myspace.com/index .cfm?frseaction=cms.veiwpage.

- The privacy policies of social networking websites usually disclaim responsibility for breaches of privacy measures. Facebook's policy explicitly states, "please keep in mind that if you disclose personal information on your page * * * this information may become publicly available." Moreover, "[Facebook] may disclose information pursuant to subpoenas, court orders, or other requests (including civil and criminal matters) if [Facebook] have a good faith belief that the response is required by law." *Id.*

- As *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650, 656 (N.Y. 2010), states: Indeed, as neither Facebook nor MySpace guarantee complete privacy, Plaintiff has no legitimate reasonable expectation of privacy. * * * **Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist.** Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites,

---

[2] *See also Moreno v. Hanford Sentinel, Inc.* (Cal. 2009), 172 Cal.App.4th 1125 (holding that no person would have reasonable expectation of privacy where person took affirmative act of posting own writing on MySpace, making it available to anyone with a computer and opening it up to public eye); *Beye v Horizon Blue Cross Blue Shield of New Jersey* (D.N.J 2008), 568 F.Supp.2d 556 (stating "[t]he privacy concerns are far less where the beneficiary herself chose to disclose the information."); *Dexter v Dexter*, 11th Dist. No. 2006-P-0051, 2007-Ohio-2568 (holding that there is no reasonable expectation of privacy regarding MySpace writings open to public view); *EEOC v. Simply Storage Mgt., LLC*, (S.D.Ind. May 11, 2010), 2010 U.S. Dist. LEXIS 52766 (stating "a person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery").

given the millions of users, "[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking." (emphasis added).

- In *EEOC v. Simply Storage Mgt.*, 2010 U.S. Dist. LEXIS 52766 (S.D.Ind. May 11, 2010), the court permitted an employer to obtain discovery of an employee's social networking pages even though the employee set privacy settings to "private" and the information was not available to the general public.

B. Methods of Discovery

- Social media postings can be discovered the same way as any other documentary evidence: interrogatories, requests for production, requests for admissions, and subpoenas.

- Sample discovery requests:

  INTERROGATORY NO. 1: State the name, web address, and user name for all blogs, online forums, and social networking websites that Plaintiff has belonged or had a membership to from April 1, 2010 to the present.

  REQUEST NO. 1: All online profiles, comments, postings, messages (including without limitation, tweets, replies, retweets, direct messages, status updates, wall comments, groups joined, activity streams and blog entries), photographs, videos, e-mails and online communications (including those posted by Plaintiff or anyone on plaintiff's behalf on Facebook and Myspace), from April 1, 2010 to the present that:

  1. refer or relate to the allegations set forth in the complaint;

  2. refer or relate to any facts or defenses raised in the answer;

  3. reveal, refer or relate to any emotion, feeling or mental state; or

  4. reveal, refer or relate to events that could reasonably be expected to produce a significant emotion, feeling or mental state.

- Email: Social networking website records may be recovered from a user's home or business email account. The email account may contain messages the user posts. Facebook allows a user to submit, via email, updates for publication on his or her Facebook wall. Facebook often

emails a user with notices and copies of content of messages posted by others for the benefit of the user. Myspace and LinkedIn have similar features.

- Facebook history download: Facebook now has a feature allowing a user to download and print his or her entire history in a document format.

C. Subpoena Problems

i. The Stored Communications Act

- Electronic communications holders like Facebook, Myspace, and LinkedIn refuse to produce records containing content of electronic communications based on the Stored Communications Act ("SCA").

- 18 U.S.C. § 2702(a)(1): "A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."

- Every court addressing the issue has stated that electronic communications holders may not produce content records in response to a civil subpoena and cannot be compelled by court order to do so under the SCA.[3]

- Exceptions: The SCA does not include a general exception for civil subpoenas. However, civil subpoenas from individuals seeking ESI from their own social networking sites are enforceable. Additionally, with user consent, social networking websites can release a user's records. 18 U.S.C. § 2701(c)(2); 18 U.S.C. § 2702(b)(3).

- LinkedIn provides its own model user consent form. http://forthedefense.org/file.axd?file=2010%2f5%2fLinked+In+Release+Form+2010521.pdf.

- Several cases have stated that a party may be compelled to grant consent.[4]

---

[3] *See O'Grady v. Superior Court* (Cal. 2006), 139 Cal.App.4th 1423, 44 Cal.Rptr.3d 72; *Theofel v. Farey-Jones* (Cal. 2004), 359 F.3d 1066; *In re Subpoena Duces Tecum to AOL, LLC* (Va. 2008), 550 F.Supp.2d 606; *Federal Trade Comm. v. Netscape Comm. Corp.* (Cal. 2000), 196 F.R.D. 559; *Flagg v. City of Detroit* (E.D.Mich 2008), 252 F.R.D. 256; *Bower v. Bower* (D.Mass. Apr. 5, 2011), 2011 U.S. Dist. LEXIS 36677.

[4] *See O'Grady v. Superior Court* (Cal. 2006), 139 Cal.App.4th 1423, 1446, 44 Cal.Rptr.3d 72 ("Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions."); *Flagg v. City of Detroit* (E.D.Mich 2008), 252 F.R.D. 256 (if the litigant has the ability to obtain "control" over such information by providing consent to the ISP, then the litigant must provide such

ii. Company Policies

- Social networking websites have stringent company policies for responding to subpoenas.

- According to Facebook's policy, "you must personally serve a valid California or Federal subpoena on Facebook. Out-of-state civil subpoenas must be domesticated in California." http://www.facebook.com/help/?safety=law.

- A subpoena should include the user's full name, Facebook profile URL, school, networks, birth date, known email address, IM account ID, phone number, address, and period of activity.

- Facebook charges a mandatory, non-refundable processing fee of $500.00 per user account in responding to a subpoena. *Id.*

D. Deletion is Spoliation of Evidence!

- Because the contents of most social networking websites is electronically stored information ("ESI"), the rules of preservation, production, and spoliation should logically apply to the contents on social networking websites.

- If you update your Facebook page when you know that it may contain potentially relevant information to foreseeable litigation, you may be spoliating evidence.

- Advice: Lawyers must address these issues early on in litigation. Ask you client about his or her social media uses. You must advise your client to preserve all information on his or her social media profiles. Do not advise your client to delete potentially damaging posts, comments, and photos.

IV. Evidentiary Concerns and "the technological heebee jeebies"[5]

- Generally, documentary evidence must satisfy four rules of evidence: (1) relevance; (2) hearsay; (3) authentication; and (4) the best evidence rule. Of particular concern is the authentication requirement.

---

consent as part of its discovery obligations); *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 U.S. Dist. LEXIS 113117 (D.Col. Nov. 13, 2009) (compelling "consents allowing Social Networking Sites to produce the information sought in defendant's subpoenas").

[5] As stated in *Griffin v. State,* 2011 Md. LEXIS 226, at *22 (Md. Apr. 28, 2011).

- *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 544 (D.Md. 2007), recognized that authenticating electronically stored information presents a myriad of concerns because "technology changes so rapidly" and is "often new to many judges."

- Social media concerns: timeliness, and authorship. Because websites constantly change, the proponent must show that an item comes from the relevant time. Because people can potentially hack into a user's profile and it is easy to create a profile under another person's name, the proponent must prove up the site's authorship. [6]

- The evidence necessary to support a finding of authentication is quite low in Ohio, even lower than the preponderance of the evidence. *Burns v. May*, (1999), 133 Ohio App.3d 351, 728 N.E.2d 19.

- In *State v. Bell,* , 145 Ohio Misc.2d 55, 2008-Ohio-592, 882 N.E.2d 502, at ¶33, the court held that electronic communications found on the defendant's MySpace website could be authenticated through testimony that:

---

[6] In *People v. Lenihan* (N.Y. 2010), 30 Misc. 3d 289, 911 N.Y.S. 2d 588, the court precluded a party from confronting witnesses with MySpace photographs on authentication grounds "[i]n light of the ability to 'photo shop,' edit photographs on the computer."

In *United States v. Jackson* (7th Cir. 2000), 208 F.3d 633, Jackson was charged with mail and wire fraud and obstruction of justice after making false claims of racial harassment against the United Parcel Service in connection with an elaborate scheme in which she sent packages containing racial epithets to herself and to several prominent African-Americans purportedly from "racist elements" within UPS. *Id.* at 635. At trial, Jackson sought to introduce website postings from "the Euro-American Student Union and Storm Front," in which the white supremacist groups gloated about Jackson's case and took credit for the UPS mailings. *Id.* at 637. The court determined that the trial judge was justified in excluding the evidence because it lacked an appropriate foundation, namely that Jackson had failed to show that the web postings by the white supremacist groups who took responsibility for the racist mailings "actually were posted by the groups, as opposed to being slipped onto the groups' websites by Jackson herself, who was a skilled computer user." *Id.* at 638.

But See In *In the Interest of F.P.* (Pa. 2005), 2005 PA.Super 220, 878 A.2d 91, the court considered whether instant messages were properly authenticated pursuant to Rule 901(b)(4) (distinctive characteristics). In the case, involving an assault, the victim, Z.G., testified that the defendant had attacked him because he believed that Z.G. had stolen a DVD from him. The judge admitted instant messages from a user with the screen name "Icp4Life30" to and between "WHITEBOY Z 404." *Id.* at 94. Z.G. testified that his screen name was "WHITEBOY Z 404" and that he had printed the instant messages from his computer. In the transcript of the instant messages, moreover, Z.G. asked "who is this," and the defendant replied, using his first name. Throughout the transcripts, the defendant threatened Z.G. with physical violence because Z.G. "stole off [him]." *Id.* On appeal, the court determined that the instant messages were properly authenticated through the testimony of Z.G. and also because "Icp4Life30" had referred to himself by first name, repeatedly accused Z.G. of stealing from him, and referenced the fact that Z.G. had told high school administrators about the threats, such that the instant messages contained distinctive characteristics and content linking them to the defendant. *Id.*

1. the victim had knowledge of the defendant's e-mail address and MySpace username;

2. the electronic printouts appeared to be accurate records of the victim's electronic conversations with the defendant; and

3. the communications contained code words known only to the defendant and his alleged victims.

- Useful Ohio Rules of Evidence concerning social media authentication:

  - **901(b)(1) (witness with personal knowledge);**
  - 901(b)(3) (expert testimony);
  - **901(b)(4) (distinctive characteristics);**
  - 901(b)(7) (public records);
  - 901(b)(9) (system or process capable of producing a reliable result);
  - 902(5) (official publications).

- In *St. Clair v. Johnny's Oyster and Shrimp, Inc.*, 76 F.Supp.2d 773, 774 (S.D.Tex. 1999), the court was very skeptical of information from website postings. The court stated: There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. **For these reasons, any evidence procured off the Internet is adequate for almost nothing.** (emphasis added).

- *Commonwealth v. Williams*, 456 Mass. 857, 926 N.E.2d 1162 (Mass. 2010), denied the admission of evidence from MySpace and suggested that greater scrutiny be used because of the heightened possibility for manipulation by other than the true user or poster. The witness, Ashlei Noyes, testified that she had spent the evening of the murder socializing with the defendant and that he had been carrying a handgun. She further testified that the defendant's brother had contacted her "four times on her MySpace account between February 9, 2007, and February 12, 2007," urging her "not to testify or to claim a lack of memory regarding the events of the night of the murder." *Id.* at 1172. At trial, Noyes testified that the defendant's brother, Jesse Williams, had a picture of himself on his MySpace account and that his MySpace screen name or pseudonym was "doit4it." She testified that she had received the messages from Williams, and the document printed from her MySpace account indicated that the messages were in fact sent by a user with the screen name "doit4it,"

depicting a picture of Williams. *Id.* The Supreme Court of Massachusetts determined that there was an inadequate foundation laid to authenticate the MySpace messages, because the State failed to offer any evidence regarding who had access to the MySpace page and whether another author, other than Williams, could have virtually-penned the messages: Although it appears that the sender of the messages was using Williams's MySpace Web "page," there is no testimony (from Noyes or another) regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc. Analogizing a MySpace [message] to a telephone call, a witness's testimony that he or she has received an incoming call from a person claiming to be "A," without more, is insufficient evidence to admit the call as a conversation with "A." Here, while the foundational testimony established that the messages were sent by someone with access to Williams's MySpace Web page, it did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than Williams could communicate from that Web page. Testimony regarding the contents of the messages should not have been admitted. The court emphasized that the State failed to demonstrate a sufficient connection between the messages printed from Williams's alleged MySpace account and Williams himself, with reference, for example, to Williams's use of an exclusive username and password to which only he had access. *Id.* at 1173.

- *Griffin v. State*, 2011 Md. LEXIS 226, at *22 (Md. Apr. 28, 2011), states: We agree with Griffin that the trial judge abused his discretion in admitting the MySpace evidence pursuant to Rule 5-901(b)(4), because the picture of Ms. Barber, coupled with her birth date and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout, given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment. The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches" language.

- *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 555 (D.Md. 2007), states that the following factors influence courts in ruling whether to admit internet postings:

    1. The length of time the data was posted on the site;

    2. whether others report having seen it;

3. whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations);

4. whether the owner of the site has elsewhere published the same data, in whole or in part;

5. whether others have published the same data, in whole or in part; and

6. whether the data has been republished by others who identify the source of the data as the website in question.

- *Griffin v. State*, 2011 Md. LEXIS 226, at *34-35 (Md. Apr. 28, 2011), suggested the following methods of authenticating social media postings:

1. ask the purported creator if she indeed created the profile and also if she added the posting in question, i.e. "[t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be."

2. search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question.

3. obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it.

V. Ethical Concerns

A. Informal Discovery

i. Publicly Available Information

- Where access to a party or witness's information is unlimited and unrestricted, there are no ethical issues in viewing the page's contents. *State ex. Rel. State Farm & Cas. Co. v. Madden*, 451 S.E.2d 721, 730 (W.Va. 1994).

- Social media information is publicly available in much the same way as materials on a publicly available website. New York State Bar Assn. Op. 843 (2010).

- Oregon Bar Assn. Op. No. 2005-164, (2005), held that an attorney can access publicly available social media posts because "a lawyer who reads information posted for general public consumption is simply not communicating with the represented owner of the web site." "Accessing an adversary's Public Web site is no different from reading a magazine article or purchasing a book written by that adversary."

ii. Private Information — "Friending" the Enemy

- Most people change the privacy settings so that you must "friend" a person to see a person's page. In some circumstances, lawyers have created false profiles to solicit a "friend request" to a target. In others, lawyers have used investigators or third-parties to become "friends" with the target and solicit information.

- Rule 8.4(c): A lawyer cannot "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation."

- Rule 4.1(a): A lawyer shall not knowingly "make a false statement of material fact or law to a third person."

- In Philadelphia Bar Assn. Op. 2009-02, (2009), a lawyer asked a third-party, whose name a key witness would not recognize, to contact the witness through her Facebook page. The third-party did not misrepresent who he was, but did not reveal his association with the lawyer. The Ethics Committee found that the lawyer's activities violated Rules 4.1 and 8.4(c) reasoning that the lawyer's use of the third-party was deceptive. The third-party's failure to disclose his association with the lawyer constituted the omission of a highly material fact, which if known to the witness, may have led to the denial of a friend request. *Id.*

- New York Bar Assn. Op. 2010-2, (2010), addressed the issue of whether a lawyer or his agent could use deception to gain access to a non-party's personal social network pages. The Ethics Committee concluded that while a lawyer or lawyer's agent may not use deception to friend someone, he can send a friend request, so long as he identifies himself using his real name and profile. *Id.*

B. Advertisement

i. Client testimonials and endorsements are prohibited in Ohio.

- Rule 7.1: A lawyer shall not make or use a false, misleading, or nonverifiable communication about the lawyer or the lawyer's services.

- Comment 2: A truthful statement is misleading if it omits a fact necessary to make the lawyer's communication considered as a whole not materially misleading. A truthful statement is also misleading if there is a substantial likelihood that it will lead a reasonable person to formulate a specific conclusion about the lawyer or the lawyer's services for which there is no reasonable factual foundation.

- Comment 3: An advertisement that truthfully reports a lawyer's achievements on behalf of clients or former clients may be misleading if presented so as to lead a reasonable person to form an unjustified expectation that the same results could be obtained for other clients in similar matters without reference to the specific factual and legal circumstances of each client's case. An unsubstantiated comparison of the lawyer's services or fees with the services or fees of other lawyers may be misleading if presented with such specificity as would lead a reasonable person to conclude that the comparison can be substantiated.

- Example: A lawyer who Tweets that he just obtained a $750,000 verdict in a medical malpractice case violates Rule 7.1 by creating unjustified expectations for future clients.

- According to Bd. of Commrs on Grievances & Discipline Op. 2000-6, 2000 Ohio Griev. Discip. LEXIS 6 (Dec. 1, 2000), at syllabus: "It is improper under the Ohio Code of Professional Responsibility for a law firm's Web site home page to include quotations from clients, even with their consent, describing the general nature of the legal services provided, responsiveness of the law firm, and other non-substantive aspects of the law firm's representation. Such client quotations constitute client testimonials[7] prohibited under DR 2-101(A)(3); may be misleading to the public under DR 2-101(A)(1) and (C) depending upon the content of the quotation; are claims regarding the character of a lawyer and the quality of a law firm's services that cannot be verified by reference to objective standards under DR 2-101(A)(4); and involve the lawyer or law firm in improperly requesting that a client recommend or promote the law firm's services to others under DR 2-103(C)."[8]

[7] Testimonial is defined as (1) A formal or written statement testifying to a particular truth or fact; (2) A written affirmation of another's worth or character; or (3) Something given as a tribute for one's service or achievement. Thus, a testimonial includes objective statements of a truth or fact as well as subjective affirmation of worth or character. A statement made by a client regarding the nature of the legal services provided is a statement of truth or fact. A statement made by a client as to law firm's responsiveness to the client's need is an affirmation of the character of the lawyers within the firm. Bd. of Commrs on Grievances & Discipline Op. 2000-6, 2000 Ohio Griev. Discip. LEXIS 6 (Dec. 1, 2000), at *6.

[8] DR 2-103 corresponds to Rules 7.1.

- Bd. of Commrs on Grievances & Discipline Op. 1989-24, 1989 Ohio Griev. Discip. LEXIS 30 (Aug, 18, 1989), at * 2, states: "In our view, a client's testimonial regarding his or her lawyer misleads the public into believing that similar results can be achieved if they hire that lawyer, thereby creating an unjustified expectation. In addition, testimonials are subjective statements regarding the quality of a lawyer's services which cannot be verified by reference to objective standards established by the profession. Such statements of quality are generally banned because they are not capable of objective verification and mislead the public. * * * Advertisements containing client testimonials are not permitted under the Ohio Code of Professional Responsibility."[9]

ii. Be wary of the LinkedIn recommendations function.

- The "recommendations function" of LinkedIn allows your connections (i.e. your friends) to write recommendations—even unsolicited and unexpected—on your profile. Users must accept the recommendations before they are posted on the user's profile. Thus, it is imperative that lawyer's pre-screen and analyze any recommendation to ensure that it conforms with the ethics rules before posting it for the public to view.

- Example: A recommendation that states "Stan Chesley is the best trial lawyer in town" violates Rule 7.1 because it is nonverifiable and creates unjustified expectations.

C. Solicitation

- Rule 7.3: A lawyer shall not by in-person, live telephone, or real-time electronic contact solicit professional employment from a prospective

[9] *See also* S.C. Eth. Advisory Op. 99-09 (1999) (once the lawyer became aware of the advertisement, the lawyer should counsel the client to conform the advertisement to the Rules of Professional Conduct and that, if the client refused, the lawyer's continued representation of the client may imply the lawyer's authorization or adoption of the advertisement); S.C. Eth. Advisory Op. 00-10 (2000) (by claiming a website listing, a lawyer takes responsibility for its content and is then ethically required to conform the listing to all applicable rules); S.C. Eth. Advisory Op. 09-10 (2009) ("Client comments may violate Rule 7.1 depending on their content. 7.1(d) prohibits testimonials, and 7.1(d) and (b) ordinarily also prohibit client endorsements. In the Committee's view, a testimonial is a statement by a client or former client about an experience with the lawyer, whereas an endorsement is a more general recommendation or statement of approval of the lawyer. A lawyer should not solicit, nor allow publication of, testimonials. A lawyer should also not solicit, nor allow publication of, endorsements unless they are presented in a way that is not misleading nor likely to create unjustified expectations. The inclusion of an appropriate disclaimer or qualifying language may preclude a finding that a statement is likely to create unjustified expectations or otherwise mislead a prospective client."); Philadelphia Eth. Op. 91-17 (1991), and Pennsylvania B. Assn. Eth. Op. 88-142 (1988) (clients' "soft endorsements" of lawyers were held not to violate the rules; an example of a "soft endorsement" includes a statement such as "the lawyer always returned phone calls and always appeared concerned").

client when a significant motive for the lawyer's doing so is the lawyer's pecuniary gain.

- Social networking websites such as LinkedIn, Facebook, Twitter, and Myspace fall within real-time electronic contact.

- Example: By posting the statement "if you are looking for a DUI lawyer I can give you my fees…. just email me," a lawyer violated Rule 7.3.

D. Specialist and Expert Designation

- Rule 7.4(e): A lawyer shall not state or imply that a lawyer is a specialist in a particular field of law, unless (1) the lawyer has been certified as a specialist by an organization approved by the Supreme Court Commission on Certification of Attorneys as Specialists; and (2) the name of the certifying organization is clearly identified in the communication.

- LinkedIn has a "specialties function," which allows users to post their specialties on their profile page. By using the specialties function, a lawyer can potentially violate Rule 7.4.

- DR 2-105(A)(6)[10]: A lawyer may not claim or imply special competence or expertise in a field of law.

- The "answers function" of LinkedIn poses potential ethical concerns. When you answer questions the readers vote on your answer. If enough readers vote for your answer, LinkedIn automatically designates you as an expert. Therefore, using the "answers function" could violate Rule 7.4.

E. Confidentiality

- Rule 1.6: A lawyer generally shall not reveal information relating to the representation of a client unless the client consents to the disclosure.

- The duty of confidentiality includes all information relating to the client gained through the lawyer-client relationship, no matter how the information is obtained.

- The casual nature of social networking websites tend lure people into posting information that they should not be posting.

- Example: In one Tweet a lawyer violated Rule 1.6 by stating "Just talked to my client who totally lied to me about all the facts."

[10] DR 2-105 corresponds to Rule 7.4.

- Example: The Illinois Attorney Registration and Disciplinary Commission disciplined Kristine Ann Peshek, an experienced public defender, for discussing a case on her blog when she posted "This stupid kid is taking the rap for his drug-dealing dirtbag of an older brother because he's no snitch." She regularly referred to client by their names and jail identification number, and vented about her cases on her blog.

F. Candor Towards the tribunal

- Rule 3.3: A lawyer shall not knowingly make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer.

- Facebook users regularly update their profile status. Many judges report ethical violations where lawyers make statements in court that are not consistent with their Facebook status update. Some lawyers post status updates criticizing or disagreeing with rulings by judges.

- Example: In Texas, a lawyer requested a continuance because she had to attend her relative's funeral. However, that lawyer posted that she was on vacation on Facebook. Needless to say, the judge checked her Facebook page and caught her lying in violation of Rule 3.3.

- Example: A Florida lawyer was reprimanded for calling a judge an "evil unfair witch" in a blog post.

G. Lawyer-Client Relationship

- It takes very little to create a lawyer-client relationship.

- An initial interview between a lawyer and a person who in good faith is seeking to hire the lawyer creates a duty of confidentiality. *Togstad v. Versely, Otto, Miller & Keefe*, 291 N.W.2d 686 (Minn. 1980).

- Under ABA Model Rule 1.18, a person who discusses with a lawyer the possibility of forming a lawyer-client relationship is deemed a prospective client.

H. Competence

- Rule 1.1: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation."

- Comment 6: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing

study and education and comply with all continuing legal education requirements to which the lawyer is subject.

- In *People v. Fernino*, 851 N.Y.S.2d 339 (N.Y. 2008), the court held that the issuance of a friend request via a social networking site constituted a "contact" in violation of a temporary restraining order.

- For family-law practitioners and criminal-defense attorneys who represent clients subject to no-contact orders, Rule 1.1 may require them to warn their clients of the potential dangers of social-networking sites.

- According to the American Academy of Matrimonial Lawyers, 66% of divorce attorneys use Facebook as their primary source for online evidence. Is a family-law attorney competent if he ignores social media based on this statistic? Is a divorce attorney who ignores media as a source of possible evidence similar to a prosecutor who fails to conduct a criminal background check on a defendant's key alibi witness?

- The duty of competence requires that an attorney ask his or her client about whether the client uses social media. The attorney should also advise the client to preserve any potentially relevant social media information.

I. Preserving Evidence

- Rule 3.4(a): A lawyer shall not "unlawfully obstruct another party's access to evidence; unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value; or counsel or assist another person to do any such act."

- Just as deletion of social media may be spoliation of evidence, deletion may also violate Rule 3.4. A lawyer likely has an affirmative duty to ensure the preservation of a client's social media profile if the profile contains potentially relevant information to a dispute.

J. Trial Publicity

- Rule 3.6(a): "A lawyer who is participating or has participated in the investigation or litigation of a matter shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter."

- Example: At the end of a "trial from hell," in which he was second chair for the State, Florida Assistant State Prosecutor Brandon White posted about the case on his Facebook page. His post was written as a parody of the

theme song from *Gilligan's Island* and described his own performance during the trial as "totally awesome." At the time White posted the update, the jury had completed deliberations but had not returned its verdict, so the risk that the post would "materially prejudice" the outcome of the case was not significant. Wilson posted an entry on his blog that identified the crimes, the first name of the defendant, and the name of the judge, whom he described as "a stern, attentive woman with thin red hair and long, spidery fingers that as a grandkid you probably wouldn't want snapped at you." As a result of his posts, the judgment was vacated and remanded for a new trial.

K. Contacting Unrepresented Party

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

- In New York State Bar Assn. Op. 843 (2010), the Ethics Committee noted that if a party was represented, a lawyer's attempt to affirmatively friend the party (instead of simply viewing the party's publicly available page) could be a communication with a person represented by counsel in violation of Rule 4.2. *Id. See also* Oregon Bar Assn. Op. No. 2005-164, (2005) (holding that attorney can access publicly available social media posts because "a lawyer who reads information posted for general public consumption is simply not communicating with the represented owner of the web site").

- Be aware of Rule 4.2 when seeking social media through informal discovery.

L. "Friending" Lawyers and Judges

- Bd. of Commrs on Grievances & Discipline Op. 2010-7, 2010 Ohio Griev. Discip. LEXIS 7 (Dec. 3, 2010), at syllabus, states that "[a] judge may be a 'friend' on a social networking site with a lawyer who appears as counsel in a case before the judge."

- However, to comply with Jud. Cond. Rule 1.2, a judge must maintain dignity in every comment, photograph, and other information shared on the social networking site.

- To comply with Jud. Cond. Rule 2.4(C), a judge must not foster social networking interactions with individuals or organizations if such

communications erode confidence in the independence of judicial decision making.

- To comply with Jud. Cond. Rule 2.9(A), a judge should not make comments on a social networking site about any matters pending before the judge – not to a party, not to a counsel for a party, not to anyone.

- To comply with Jud. Cond. Rule 2.9(C), a judge should not view a party's or witnesses' pages on a social networking site and should not use social networking sites to obtain information regarding the matter before the judge.

- To comply with Jud. Cond. Rule 2.10, a judge should avoid making any comments on a social networking site about a pending or impending matter in any court.

- To comply with Jud. Cond. Rule 2.11(A)(1), a judge should disqualify himself or herself from a proceeding when the judge's social networking relationship with a lawyer creates bias or prejudice concerning the lawyer for a party.

- To comply with Jud. Cond. Rule 3.10, a judge may not give legal advice to others on a social networking site. *Id.*

- Other state's ethics opinions.[11]

---

[11] Kentucky Ethics Committee answered a "Qualified Yes" to the question: "May a Kentucky judge or justice, consistent with the Code of Judicial Conduct, participate in an internet-based social networking site, such as Facebook, LinkedIn, Myspace or Twitter, and be 'friends' with various persons who appear before the judge in court, such as attorneys, social workers, and/or law enforcement officials?" Ethics Committee of the Kentucky Judiciary, Formal Judicial Ethics Op. JE-119 (2010).

In South Carolina, Advisory Committee on Standards of Judicial Conduct, Op. 17-2009 (2009), the South Carolina committee concluded that "[a] judge [magistrate judge] may be a member of Facebook and be friends with law enforcement officers and employee's of the Magistrate [magistrate judge] as long as they do not discuss anything related to the judge's position as a magistrate." The committee noted that "[a]llowing a Magistrate to be a member of a social networking site allows the community to see how the judge communicates and gives the community a better understanding of the judge." *Id.*

A Florida committee answered "No" to the question of "whether a judge may add lawyers who may appear before the judge as 'friends' on a social networking site." Florida Sup.Ct., Judicial Ethics Advisory Committee, Op. 2009-20 (2009). "The Committee believes that listing lawyers who may appear before the judge as 'friends' on a judge's social networking page reasonably conveys to others the impression that these lawyer 'friends' are in a special position to influence the judge." *Id.*