SOCIAL MEDIA IN CLAIMS INVESTIGATION – THE SMELL OF "TWEET" SUCCESS

By Daniel W. Gerber

Daniel W Gerber Dan has a distinct practice counseling clients on social media and the law. In this vein, he develops claims/underwriting guidelines and provides in-house training on social media issues for several clients in the insurance sphere. Mr. Gerber is past chair of the Defense Research Institute's (DRI) Social Media Task Force. He currently serves on DRI's Board of Directors and is Chair of DRI's membership committee. He also is currently a member of the Board of Directors for the Defense Association of New York (DANY). Dan has 20-plus year's accumulated knowledge handling "bet the company" insurance difficulties. CBS's 60 Minutes undertook two exposés on separate matters Dan directed. His experience ranges from litigating billion-dollar insurance and reinsurance disputes; breaking down misunderstood wordings and policy issues; resolving regulatory quagmires; and providing proactive guidance to clients. Dan oversaw a team that resolved over 1,500 Superstorm Sandy claims -- acting as national coordinating counsel for several insurers. He has immense understanding of all facets of international insurance markets from London to Bermuda. During the Greek financial crisis, he coordinated with the Greek government on insurance solutions. In this regard, Dan brings unique cross-border transactional and regulatory expertise in portfolio transfers and insurance structural arrangements. He is a Registered Foreign Lawyer in England and Wales. In conjunction with being a US ARIAS certified arbitrator, Dan acts as an arbitrator, umpire and mediator of insurance and reinsurance disputes. He also offers expert testimony in complex insurance and extra-contractual matters. Dan has over 3,000 followers on his daily insurance-related Twitter feed @insurerereport.

Introduction

Perhaps the vast expansion of electronic social networking into our culture is best captured by a 2009 New Yorker cartoon. The cartoon in the June 1, 2009 issue depicts a firing squad and an officer saying to a condemned man: "Last tweet?" Cartoonbank.com, David Sipress, http://www.cartoonbank.com/item/130799 (June 1, 2009). There is little doubt that social networking through mediums such as Twitter, FaceBook, MySpace, and Linkedin has become an established type of participatory communication. NewsBusters, Will Social Networking Sites Like FaceBook Destroy Our Society?, http://newsbusters.org/blogs/noel-sheppard/2009/08/25/will-social-networking-sites-facebook-destroy-society (August 29, 2009).

As a result of the explosion of information available on-line, claim professionals and defense counsel are discovering that social media is useful for uncovering relevant information on claimants. This includes: postings about the incident (i.e. discussing the injury or visits to doctors, boasting about a lawsuit, or describing trips or activities inconsistent with claims); photographs showing a plaintiff engaged in post-accident activities; photographs showing plaintiff in a poor light (i.e. drinking, using drugs); descriptions of education/experience/skills in the "more professional" networking sites (such as LinkedIn), indicating ability to mitigate damages.

It is becoming more and more apparent that by utilizing social networking tools, claim professionals increase the chance of successful claim resolution. One must, however, understand the processes and have a strategy. Success Stories, http://webworkerdaily.com/2009/06/16/real-life-twitter-business-success-stories/ (June 16, 2009).

Understanding Social Media Resources

In order understand the application to claim's investigation, it is important to understand the various media and their different applications. Twitter, for example, is a focused medium. It allows a person to send messages of up to 140 characters in length to anyone who "follows" him or her. Messages (*i.e.* "tweets") can be sent on any topic. In many respects it is like a mini-blog. A blog is different than a website in many respects. A website is static. A blog on the other hand is a running stream of content-driven posts that all fall within the subject matter of the blog.

Tweets are instantaneous and can be received on cell phones as text messages, in email or through other web portals such as FaceBook or LinkedIn. Anyone can choose to follow someone else on Twitter. A user can prevent a "follow" by "blocking" that person, but Twitter is more free-style than other social networking sites like FaceBook where a user must invite another user to be a "friend". This, of course, means that a claimant with a Twitter account opens themselves up to the world. This is, in part, because anyone else can see who follows him or her, and anyone else can become a follower of that person

Of course, Twitter and blogging are just two medium used in social networking. By far, the most utilized outlets are sites such as LinkedIn, MySpace, and FaceBook. Each of these sites allows users to set up a profile that others can view, and allows others to connect their profiles to other users. Each site varies in the method and amount of information exchanged once one user is connected with another. LinkedIn is more suited to the business world than FaceBook and MySpace. For example, LinkedIn allows users to send an "Introduction" to someone so that two people might do business together. FaceBook allows users to send someone a "teddy bear." LinkedIn allows users to share expertise by answering questions posted by other users. FaceBook allows users to share how they are feeling by adding applications like "Happy Island," "My Personal Weather," or "Care Bears".

As a result of the differences, LinkedIn is better suited for vocational information, while sites like FaceBook and MySpace may be best suited to unveil personal information about a claimant and his or her claim.

Additional sites should not be overlooked. In particular, claimants have taken to knowingly creating video and photographic accountings of their lives in the internet. Sites such as YouTube are used to post videos for the world to see. Sites such as Flickr and Photobucket are used to upload, share and print photographs. Claimants visit forums about medical conditions and often make comments in these forums.

Understanding the Power of Social Media

The amount of information available about people through these sites is astounding. Google CEO Eric Schmidt during a Keynote Address to Mobile World Congress in February 2010 stated that "[T]hese networks are now so pervasive that we can literally know everything if we want to . . . What people are doing, what people care about, information that's monitored, we can literally know it if we want to …" Computer World, Feb. 18, 2010. This vast amount of information is already having an effect on courts and claims. Several courts have banned jurors from using social media. *As "Tweeting" Grows, the Question of Jury Taint Arises*, Pittsburg Tribune-Review, February 9, 2010; Twitter Crackdown in Baltimore Circuit Court, Baltimore Sun, February 9, 2010. Plaintiff lawyers often advise their clients on their first meeting to discontinue using social media. *First Thing Lawyer Tells New Clients: Shut Down FaceBook Account*, ABA Journal Law News Now, February 9, 2010. Lawyers have even found themselves in hot water for posting personal views on social networking sites. *Hennepin County Prosecutor Accused of Anti- Somali Posting on FaceBook*, Star Tribune, February 17, 2010

Utilizing Social Media

Basic investigation can take place with respect to almost any person on any social media site. Name searches can be made in the site's search engine or on Google. Several blog specific search engines exist such as blogdigger.com. The amount of information available once a profile is found will depend upon a person's privacy settings. The more difficult question ethically is whether to attempt to "friend" a claimant on FaceBook or "follow" them on Twitter. In other words, should a social media investigation include creating a directly electronic relationship with the claimant?

The danger begins once a claim professional or lawyer steps outside of the controlled feed from a regular source and starts into the quick back and forth exchange that characterizes social networking at its best. Lawyers are prohibited from communicating with parties known to be represented by counsel, and it is untested whether courts would extend that rule to an insurer who is investigating a claimant clandestinely through social media.

The Stored Communications Act creates a criminal offense and civil liability for whoever "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and by doing so "obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. §2701. In *Van Alstyne v. Electronic Scriptorium Ltd.*, 560 F.3d 199 (4th Cir. 2009), the plaintiff sued employer for sexual harassment and employer countersued for business torts. The boss accessed the employee's AOL account using her password. The Jury awarded $400,000, including punitive damages, which was affirmed on appeal.

In light of potential liability, it is best to proceed with caution before creating a direct relationship with a claimant as part of a social media investigation. Inquiry should be made as to whether corporate policies are in place governing this type of investigation, and further inquiry should be made with counsel as to the appropriate boundaries. In addition, there are several well-qualified investigative firms that know precisely how to utilize social media in investigations. .

Once a matter is in suit, however, it is important that several questions are asked in the discovery process. Some of these include:

1. Do you have a computer, laptop or Netbook? (At home or at work?)
2. What do you use it for?
3. Do you send e-mails to your co-workers?
4. Have you ever gone into a chat room, message board or posted on any website?
5. Do you blog?
6. Do you have online e-mail (Yahoo, AOL, G-Mail)? Do you access this through work?
8. Are you on FaceBook? Twitter? LinkedIn?
9. Have you visited any medical related sites to examine your condition (i.e. WebMD.com or health related chat rooms?)
10. Do you have visit a union website?
11. Have you posted any videos on YouTube? Ever used the internet to post photographs or upload prints for ordering?

Discovery should be used to establish relevance of the home or office computer, internet accounts or other electronic devices. At a minimum, initial discovery demands should seek: (1) authorizations for social networking sites; (2) identification of social networking sites; (3) screen names, logon and passwords; and (4) release of information from social networking sites

If necessary, a court order can be sought against the plaintiff to "freeze" the computer and its contents. Forensic analysis of plaintiff's home computer or electronic devices may lead to email, or social media that contradicts the claim. This analysis will also ascertain any destruction of evidence (drive wiping programs, reformatting, or loss of the hard drive, destruction of the computer, or deletion of specific files). For example, the court in *Foust v. McFarland*, 698 N.W.2d 24 (Minn. 2005), affirmed the trial court's adverse inference charge against plaintiffs in auto accident case for using a "WipeInfo" program to permanently delete data from computer hard drive.

It is important to realize that social networking sites want to appear to protect users. FaceBook, MySpace, and Twitter currently receive thousands of requests from law enforcement and civil litigation and want to discourage these requests.
According to FaceBook's Deputy General Counsel Mark Howitson, FaceBook is "looking for a fight". *Legaltech*, February 1, 2010. As such, FaceBook will not hand over any information on its 350 million users without a subpoena. Even then, the

company will only provide basic subscriber information unless that user gives his or her consent. In addition, FaceBook is only responding to California subpoenas and orders.

Gathering Evidence from a Social Media Site

If a social media user makes information publicly accessible, a lawyer may view the content as would any other member of the public. But what if the lawyer is thwarted by privacy settings? May the lawyer engage in trickery to get around them?

1. Limits on the Use of Deception

An ethics opinion issued in 2009 by Philadelphia Bar Association offers one 'perspective.
Phila. Bar Ass'n Prof Guidance Comm. Formal Op. 2009-02 (2009). A lawyer representing a party to a lawsuit sought to learn more about an adverse witness. The lawyer asked the bar association's ethics committee whether he could ask a third party who was not affiliated with the pending litigation to send the witness a Facebook "friend request." The third party would give his or her true name" but would not reveal the affiliation with the lawyer or the true purpose for which the information was being sought.

On their face, ethics rules might appear to forbid even a modicum of trickery, no matter how good the cause. Rule 8.3(c) forbids lawyers from engaging "in conduct involving dishonesty, fraud, deceit or misrepresentation." In general, lawyers may not ask their agents e.g., friends or investigators - to do what the lawyers themselves are ethically forbidden to do. Model Rules of Professional Conduct R. 8.3(c) (2009).

The use of minor trickery to gather evidence is not universally regarded as ethically forbidden, however. Judicial decisions in various jurisdictions specifically permit the use of some pretense or misdirection in gathering evidence for litigation. Civil rights "testers" - e.g., individuals pretending to be interested in renting an apartment - have been used since the adoption of civil rights laws to gather evidence of impermissible discrimination. *See, e.g., Apple Corps Ltd v.Int'l Collectors Soc'y*, 15 F. Supp.2d 456 (D.N.J. 1998); *Gidatex, S.r.L. v. ' Campaniello Imps., Ltd*, 82 F. Supp.2d 119 (S.D.N.Y. 1999).

Notwithstanding its acknowledgment of decisions allowing lawyers' investigators to dissemble in some contexts, the Philadelphia bar opinion considered it impermissible to use deception to gain access to an adverse witness's Facebook profile, even for the legitimate purpose of seeking evidence of perjury. In the committee's view, the lawyer's surrogate is ethically obligated to disclose the true motive for seeking access. In light of ethical limits on impermissible deceit, a subsequent article offered this advice: avoid using third parties to contact counsel, parties, or witnesses without expressly disclosing that the communication is on behalf of the lawyer, law firm, or client; never use deception or misrepresentation in communications including use of aliases and screen names that do not clearly identify you; always clearly identify yourself and the purpose of

your communication; understand and follow user rules associated with sites. Tiffany Williams, Facebook: Ethics, Traps, and Reminders, 35 A.B.A. Litig. News 4 (2009).

More recently, the New York State Bar Association concluded that a lawyer who represents a client in litigation, and who has access to the Facebook or MySpace page used by another party in the litigation, may access and review the public social networking pages of that party to search for potential impeachment material. As long as the lawyer does not "friend" the other party or direct a third person to do so. New York State Bar Association, Committee on Professional Ethics, Opinion 843 (September 10, 2010).

2. Limits on Communications With Represented Persons

The Philadelphia opinion suggests that to avoid misleading the opposing witness, a lawyer should straightforwardly ask permission for access to her Facebook profile. Here, another ethical limit comes into play, namely, Rule 4.2(a), which governs communications represented parties. The rule provides: "In representing a client, a lawyer shall not communicate or cause another to communicate about the subject of the representation with a party the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the prior consent of the other lawyer or is authorized to do so by law."

Rule 4.2(a) does not forbid all communications with a represented party, but only those on "the subject of the representation." A request for access to a user's profile is not, at least explicitly, on the subject of the representation. It would be different if the ethics rule were read to impose an outright ban, or if other relevant law did so. Of course, other electronic media may provide for greater give-and-take. If the lawyer corresponds with the represented party in a chat room or in other contexts where the lawyer is not just reading but is actually communicating back and forth on the subject of the . representation, the lawyer risks crossing the lines established by Rule 4.2.

A decision out of Suffolk County in New York(J. Spinner), permitting the defendant in a personal injury action to gain access to the private portions of plaintiff's Facebook and MySpace accounts (including deleted info.) by showing that the limited public information that was available on those accounts was inconsistent with the claims being made by the plaintiff in her lawsuit. Specifically, plaintiff's Facebook photo showed her smiling outside her home; plaintiff was claiming that as a result of the accident, she was largely confined to her home and bed. The Court also took note that "review of the public portions of Plaintiff's MySpace and Facebook pages reveals that she has an active lifestyle and has traveled to Florida and Pennsylvania during the time period she claims that her injuries prohibited such activity." Justice Spinner found that:

> In light of the fact that the public portions of Plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain

> further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action. Preventing Defendant from accessing . . . Plaintiff's private postings on Facebook and MySpace would be in direct contravention to the liberal disclosure policy in New York State. . .
> To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.

In opposition to the motion, plaintiff claimed that she had a reasonable expectation of privacy, which the Court noted was belied by the clear language contained in the Facebook and MySpace user agreements. Neither Facebook nor MySpace guarantees the complete privacy of its users. The Court found that plaintiff had "consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings" and that, regardless, defendant's need for the information outweighed plaintiff's privacy concerns. *Romano v. Steelcase, Inc*., 2006-2233, NYLJ 1202472439237, at *1 (Sup. SU., Decided September 21, 2010).

Procedural and Discovery Limits

Procedural rules and norms may impose other limits, as may Rule 4.4(a), which prohibits lawyers from representing clients through means that have no substantial purpose other than to embarrass, delay, or burden a third person. The publication of depositions through the social media to embarrass an opposing party or witness may implicate these restrictions. For example, in *Seaman v. Wyckoff Hgts. Med. Ctr., Inc*., 202005 NY Slip Op 25188 (N.Y. Sup. Ct. 2005), a New York court sanctioned lawyers for acting in bad faith when they videotaped a deposition and then provided the videotape to the television program, "A Current Affair." On the other hand, a Texas plaintiff's lawyer got off more cheaply in 2008 when he posted an excerpt from a video deposition on YouTube. Judge Orders Counsel to Remove Deposition Excerpt From YouTube, Law.com (December 9, 2009). The court ordered the lawyer to remove the video from YouTube until the transcript of the deposition had been filed but permitted the lawyer to re-post the video afterward, when it became a public record, as long as it had a disclaimer that the video was only an excerpt of the complete deposition.

Once a jury is selected, the risk that jurors will learn about a case through the media is greater now than ever before. Courts routinely instruct jurors not to read about the case, but the public is increasingly conditioned to check the internet for the latest information. Mistrials caused by jurors who cannot resist using computers to conduct their own investigation are an increasing problem. John Schwartz, As Jurors Turn to Web, Mistrials Are Popping Up, N.Y. Times, Mar. 17,2009, available at

http://www.nytimes.com/2009/03/18/us/18juries.html F I; also See John Schwartz, A Legal Battle: Online' Attitude VS. Rules of the Bar, N.Y. Times, Sept. 13,2009, at Al (discussing a criminal conviction which was set aside when a lawyer sent tweets about a case while serving as a juror). The exceptions include that a lawyer may discuss "information contained in a public record" and may make statements "that a reasonable lawyer would believe is required to protect a client from the substantial prejudicial effect of recent publicity not initiated by the lawyer or the lawyer's client."

A trial lawyer now has new outlets to use to tell the client's story. The lawyer's blog - or a post on someone else's blog - are among the options offered by electronic media (or Twitter, if the client's story is a very short one). A blog has advantages over a newspaper or television interview, since the lawyer has control over what is posted (although not over what others post thereafter). But if a lawyer crosses the line by posting information that may taint a jury, that will also be visible and perhaps indelible. Statements posted by a lawyer on a blog before a case goes to trial will be available to prospective jurors - and, later, to actual jurors. The posting won't go away. Therefore, lawyers would do well to be aware of the limits of Rule 3.6. Of course, clients themselves are not subject to these limits. Sophisticated corporations may discuss their cases on their websites or in other electronic media and may engage public relations experts to assist. Their trial lawyers have no obligation to stop them. But may their trial lawyers assist? Ru1e 8.4(a) says that lawyers may not violate ethics rules "through the acts of another." Does that mean that lawyers may not encourage their clients to talk about their cases in the electronic or social media and assist clients in formulating what to say? Perhaps doing so is acceptable, since the public will not identify the client's words with the lawyer, thereby avoiding the presumably greater risk to the integrity of judicial proceedings that results when lawyers do the talking. But opinions in other contexts are skeptical when lawyers use their clients as their puppets. At minimum, may the trial lawyers advise clients who decide independently to exploit social media to spin their cases? Surely, clients who are inclined to do so are better off with legal advice. But whether and to what extent trial lawyers may provide such assistance seems so far unresolved.

Don’t Forget to Look in the Mirror

While the impact of social media is vast, it may also pose serious consequences for an insurer or policyholder. While it is important to investigate and know as much as possible about the claimant, it is key in today’s world to understand all information available about a policyholder or corporate witness. A very professional company witness’ credibility can be destroyed by plaintiff’s counsel’s reference to her “MySpace” posting. Companies should consider well-planned social networking policies which reinforce the consequences of ill-advised social networking. From an insurer’s perspective, consideration should be given to potential additional areas for discovery in bad faith litigation.

Tying It All Together

Of course, electronic social networking is not a substitute for normal investigation and personal interaction. It is, however, an additional valuable tool. With the advent of new means of communication come several obstacles, as well as opportunity. No doubt there will be abuses of social networking by an unscrupulous few. It is imperative, however, that claims professionals and counsel embrace and understand social media, and use it appropriately.

DRAFT SOCIAL MEDIA POLICY

When it comes to expressing opinions about anything having to do with the law, _____ (the "firm") employees are in a special position and have some limitation that other industries do not have. Statements in public forms may inadvertently create an attorney-client relationship, and may also violate the rules prohibiting law firm advertising.

The firm supports open dialogue and the exchange of ideas. It regards blogs and other forms of online discourse as primarily a form of communication and relationship among individuals.

When the firm wishes to communicate publicly —whether to the marketplace or to the general public—it has well established means to do so. Only those officially designated by the firm have the authorization to speak on behalf of it.

However, the firm believes in dialogue among employees and with our partners, clients, and members of the many communities in which we all participate. Such dialogue is inherent in our business model of innovation, and in our commitment to the development of open standards. We believe that employees can both derive and provide important benefits from exchanges of perspective.

As a firm, we trust — and expect — employees to exercise personal responsibility whenever they participate in social media. This includes not violating the trust of those with whom they are engaging. Each social media tool and medium has proper and improper uses. While we encourage all of our employees to join a global conversation, it is important for employees who choose to do so to understand what is recommended, expected and required when they discuss firm-related topics, whether at work or on their own time.

All of the firm's information systems hardware and software, all electronic files and data, voice messages, and electronic messages are the property of the firm, whether composed, received or sent by the employee. The Firm may monitor the usage of computers, the internet, postings, and/or voicemail/e-mail by partners and employees, including a list of telephone numbers called and/or websites accessed by an individual. The Firm may also access computer files, data, and e-mail/voicemail messages stored in computers used by partners and employees. No individual can expect privacy in terms of his or her use of Firm computers, internet, employment related postings and/or voicemail/e-mail. All partners and employees who use the Firm computer network or other systems consent to monitoring and access by the Firm as a condition of their use. For the purpose of this Policy, the Firm's computer network also includes, but is not limited to, laptop computers and handheld electronic devices (e.g., cell phones, smartphones, personal digital assistants) provided, and/or paid for, or reimbursed for the cost of use by the Firm.

The Firm's computers, internet access and voicemail/e-mail communication systems are to be used for business purposes, meaning that the use of such equipment and systems must be job-related. Limited, occasional or incidental use of these systems for personal purposes is acceptable, if done in a professional manner that does not interfere with work and is consistent with business use. However, such personal use of these systems is subject to the terms of this policy, including, but not limited to, Firm ownership, access to and monitoring of partner and employee internet usage, voicemail/e-mail communications, and computer files or records, as well as the disclaimers required below.

The following guidelines should be followed when creating and/or publishing content, and participating in social media online:

Think first. Remember you are publishing in a public forum, so don't publish anything that you wouldn't want to be viewed by your family, colleagues or the general public. Since content is easily transferred and replicated across the internet, it is nearly impossible to delete content once it has been published. Whether you're posting personally or professionally, don't write anything that you would not feel comfortable being published with your name in the New York Times.

- Check your posts or comments for spelling and accuracy.
- Write clear headlines. Write each headline so that it makes sense out of context; many people will see only the headline of your post.

The Internet is not anonymous. Everything written on the Web can be traced back to its author one way or another and very easily. Information is backed up often and repeatedly and posts in one forum are usually replicated in other through trackbacks and reposts or references. Social media providers such as Facebook, MySpace, etc. receive thousands of subpoena per month seeking information from their servers.

There is no clear line between your work life and your personal life. Always be honest and respectful in both capacities. With the ease of tracing authors back from their posts and the amount of information online, finding the actual identity of a poster from a few posts and a screen name is not impossible. This creates an avenue for outside parties to link your personal writings to those you've done in a professional capacity. Always write as if everyone knows you. Never write anything you wouldn't say out loud to all parties involved. Understand the privacy settings of various social media. For example, FaceBook's default setting is that all photographs are open for anyone to view. If you have not changed the setting, any of your photos are a few clicks away from being viewed by anyone you interact with professionally.

Avoid hazardous materials. Do not post or link to any materials that are defamatory, harassing or indecent. Do not defame the firm, your colleagues or industry organizations or peers by publishing statements that are harmful and/or untrue. Do not post content that is mean-spirited, illegal, fraudulent, obscene, threatening, infringing of intellectual property rights, invasive privacy or otherwise injurious or objectionable. Do not make post anything offensive, such as slurs, epithets or anything that may be construed as

harassment or disparagement based on race, color, national origin, sex, age, disability, religious or political beliefs, or any other protected status under federal or state law. Firm policies prohibiting sexual and other harassment are applicable to internet access and all uses of Firm information systems.

Don't promote other brands with the firm's brand. Do not promote personal projects or endorse other brands, causes or opinions. Be sure to respect third party copyrights. If a personal opinion must be posted, clearly state to all readers this does not represent the opinions of the firm. Do not participate in internet based surveys without prior authorization from management.

Don't pad your own stats. Do not create anonymous or pseudonym online profiles in order to pad link or page view stats. Also, do not comment on your own or another's posts in order to create a false sense of support.

Always trackback. When reposting or referencing a post on one of the firm's sites, provide a link to the original post or story.

Identify yourself. When relevant, identify your affiliation with the firm and your area of concentration. Qualify the geographic limits of your and our practice, so as not to engage in the unauthorized practice of law in an unlicensed jurisdiction.

Do not qualify your work. Do not post statements regarding the quality of your work nor the firm's.

Do not return fire. If a negative post or comment is found online about the firm or yourself, do not counter with another negative post. Seek help from the Facilitation Committee in defusing these types of situations.

Maintain client confidentiality. Work for clients and the identities of our clients must be held in confidence to the extent appropriate for that client and client relationship. You must comply not discuss any client matters or any facts or circumstances related to them on social media. Communications through social media are not guaranteed privacy by the privacy policies of the providers themselves and posting are subject to subpoena by third parties. No communications about any firm or client matters should be made through social media or through any email (other than the firm's). Realize that answer questions about a topic in an on-line forum may lead to that party believing you are offering legal advice. Also be aware of unintended conflicts of interest you can create by posting in a forum on a topic when in fact we represent parties on that topic or in that matter. Do not disseminate any client, internal, or confidential documents, information or data without explicit management authorization. Authorized users do not have an expectation of privacy. All voicemail, e-mail, postings, keystrokes, actions and computer files are subject to review by the Firm. Thus, even though you use a password and may be able to classify messages or files as, for example, "personal and confidential" or "private," those messages and files remain subject to inspection and review by the Firm at any time. Monitoring may include printing and reading all electronic files and communications

entering, leaving or stored in these systems, or listening to voicemail messages entering, leaving or stored in these systems. Because of this, users may not create an impression with those outside the Firm who send them messages that those messages are confidential from the Firm.

Be mindful of creating an attorney-client relationship. It is recommended that you not advise any course of action with respect to a particular set of facts. There can be a fine line between supplying legal information and supplying legal advice. Focus on new and interesting things happening in your area of expertise. Be careful about asking specific questions. Be mindful that you may create a conflict with a current client.

Disclaimers. You should make it clear that you are expressing views that are your own and not those of the firm.

Follow the law. This should be obvious. In particular, be cautious of securities law violation and copyright violation. Use caution when publishing text, pictures, video or other content that was not created by the firm. Unless specifically licensed otherwise, all created content is protected by copyright. If you want to use copyrighted material, you must obtain written permission from the original author of this content

Linking v. Republishing: Whenever possible, link to content elsewhere on the Web instead of republishing Give proper attribution to other sources.

Use of logos or service marks. The firm's logo or service mark cannot be used in any social networking without the express written permission of the managing partner.

Blogs and Personal Websites

Employees are prohibited from speaking on behalf of the Firm through internet communications even if conducted outside of work, unless authorized by management. Partners and employees may not reveal confidential Firm information or trade secrets through their personal websites and should also ensure compliance with any potentially applicable securities regulations and copyright/trademark protections. In addition, partners and employees should refrain from making any harassing, discriminatory, defamatory, or otherwise unlawful comments.

If you create a blog. Neither the title of the blog nor the URL of the blog may include the firm's name without the express written permission of the managing partner, or his designee. If you create a law-related blog, then you are required to advise the managing partner or his designee. If you create a blog, you may receive communications requesting legal advice. Always begin any response by advising the person that you cannot give legal advice to anyone who is not your client. You may then advise the person how to become a client and that we must understand the question further in order to run an appropriate conflict check.

Commenting on blogs. You should treat the comments you make on another blog the same as you would treat posts on your own blog.

LinkedIn

LinkedIn is a powerful professional online networking tool. **Recommendations are particularly problematic.** In some jurisdictions they can be viewed as testimonials and attorney advertising. Attorneys should be cautious in providing recommendations for other attorneys for that reason. If you receive a recommendation, carefully consider if it appropriate to post on your profile. No firm employees or partners should recommend other firm employees or partners without the permission of the managing partner or his designee.

Do not leave your "connections" open for view to others. Doing so may give away certain client confidences and also provide advantage to the firm's competitors. Also, consider carefully before giving a recommendation to an expert that the firm uses regularly and who should have the appearance of independence. Giving such a recommendation, or receiving one, may create an issue for cross-examination of the expert.

No attorney should list anything under the "specialties" portion of his or her Linkedin profile. In addition, no attorney should participate in the "answers" portion of Linkedin, as doing so may lead Linkedin to list you as an "Expert" in a particular area. Stating you are a specialist or expert is a potential violation of rules of professional conduct. Participation in groups on Linkedin is permitted and encouraged. If you create or manage a law-related group on Linkedin, you are asked to advise the managing partner or his designee. No group should contain the firm logo or name without the express written permission of the managing partner or his designee.

Prospective Employees or Partners

No firm employee shall view or research any social networking site of a prospective candidate for employment at the firm without the permission of the managing partner, or his designee.

Current Employees and Partners

Current employees and partners may connect and communicate with each other via and through social media, subject all the guidelines herein. No employee or partner is obligated, nor should they be made to feel obligated, to connect with another partner or employee and may simply ignore a request to connect or communicate with that person. Any inappropriate use of, exploitation of, or other misuse of social media among employees or partners should be reported to the managing partner and/or his designee.

Facebook/MySpace/Twitter/Other Social Network Sites

Although these are largely personal social tools, if you are a member of the firm's network or list the firm on any of these type of media, then your activity in these types of sites impacts the firm as well as your personal image. These guidelines are applicable to your use of these sites. The default setting for FaceBook is to have any photos you post open to the public. Any of the firm's client's may Google you and your FaceBook page is likely to be near the top of the search. As such, and as discussed above, you should strongly consider changing default privacy settings to make picture inaccessible to the public. To the extent that you do not change privacy settings or use any sites to connect with professionals in business organizations for which the firm pays for you to be involved, then your conduct, photos, fan pages, follows, postings and activities should be of a nature that would never be offensive or unprofessional.

The Judiciary

No firm employees or partners should become connected through a social networking site with a member of the judiciary (or his or her staff) without advising the managing partner or his designee. If the request s made from a member of the judiciary, contact the managing partner or his designee for further guidance before accepting the connection. No comments should be made on any social media site regarding any personal or professional opinions regarding a member of the judiciary or any of his or her staff.

Wikipedia and Web Postings

Any edits you make to Wikipedia or any other web site/blog while using a company computer can potentially be tied back to the company. Even an anonymous edit marks the editor with its Internet Protocol (IP) address. This IP address can easily be tied back to the firm. Google tracks all searches and saves them by IP address. Thus, your Google searches can be tracked back to th firm as can almost all internet activity. The Firm does log internet activity and can trace activity back to individual users.

Twitter

Be professional, kind, discreet, authentic. Represent us well. Remember that you can't control it once you hit "send". As anyone can follow you on Twitter, check your followers from time to time to see if any are inappropriate or offensive in terms of description or photos.

Don't forget your day job.

You should make sure that your online activities do not interfere with your job or commitments to customers. Unless used in advancement of firm goals and objective, social media should not be utilized by administrative staff during normal work hours.

Violations

Any concerns about violation of this policy should be brought to the immediate attention of the managing partner. You are solely responsible for, and will be held accountable for, any and all information or materials, in any form, that you post or publish through any form of online social media. Consistent with and to the extent permitted by any applicable laws, social media sites may be monitored by firm staff. You may be subject to discipline, up to and including termination, if your usage of social media (regardless of whether occurring during work time or through the firm computer network) violates this or any other relevant employee policy or otherwise conflicts with the interests of the firm If the firm determines that you have violated your obligations under these guidelines, the firm has the option to take certain steps which may include, among others, warnings, suspension, probation, and discharge.

If you have any questions, comments or concerns regarding this policy, please feel free to contact the managing partner.