



SMALL BUSINESS

Imagine a lawyer has just finished a grueling deposition preparation session with an uncooperative but important witness for her side of the case. Tired and a bit frustrated, Mary vents by updating her Facebook status while in the taxi on the way home:

“Absolutely drained after spending six hours prepping Mr. No-clue for deposition. Who’s in for dinner?”

In this post, Mary “tags” a few of her friends, among them Dave, who also happens to be a lawyer. But what will Mary do when Dave happens to be Facebook friends with the opposing counsel, who can see that Dave is tagged in Mary’s post, and uses this serendipity as ammunition at cross-examination like this:

**Question:** Mary, did you meet with the counsel to prepare for your testimony today?

**Answer:** Yes.

**Question:** Are you aware that counsel has questioned your competence and the accuracy of your memory regarding the facts in this case?

Following an event such as this, professional liability coverage would undoubtedly become a necessity. But there are preventative steps lawyers can take to avoid such claims – as long as they remain diligent from behind their keyboards.

Social media, blogs and other interactive internet-based platforms allow lawyers to reach out broadly to colleagues, clients and potential clients. But, posting on “personal” social accounts doesn’t exempt lawyers from confidentiality breaches, violations in ethics, or state or federal privacy and data security laws. Not to mention certain social actions could potentially mislead clients or fall short of the standard of care. Thus, while lawyers must keep pace with today’s forms of communication, they also must consider the risks presented by new technologies and how to control those risks.

What follows is an examination of some of those risks and ways to help address them.

## Social Media Potential Pitfalls

Think twice before posting. Participation on Facebook, Twitter and LinkedIn can be both socially and professionally beneficial. But, lawyers also risk breaching confidentiality or undermining relationships with courts, witnesses or clients through even the most seemingly innocuous status updates, comments, likes and shares.

The lawyer with the difficult deponent mentioned earlier not only is likely to be embarrassed before her client and the court, but also could face a professional liability claim when the witness refuses to cooperate in presenting essential facts at trial and the client’s case is lost as a result.

A lawyer who uses social media to alert friends that he must cancel dinner with the post, “Unexpected meeting at XYZ Corp. equals long night of work ahead,” may inadvertently tip someone off regarding XYZ’s plans for a business transaction, potentially leading to violations of state or federal insider trading laws. This risk is exacerbated by the seemingly infinitely long reach of Internet posts, coupled with the lack of control over the message once it is posted online.

Even if you delete a post after second-guessing its appropriateness, a dozen people have likely seen it within a matter of minutes. And the post isn’t limited to your followers and friends; the update is susceptible to being shared with friends of your friends, and their friends, over and over again. Similarly, lawyers or law firm employees who “friend” clients and communicate with them over public and semi-public media risk inadvertent waivers of privilege and unanticipated breaches of confidentiality.

Remember: Judges can and do look at social media updates to monitor compliance with directives and veracity of statements by criminal defendants, litigants and attorneys. In one situation, documented in the July 21, 2009 issue of ABA Journal Law News Now, a lawyer asked a judge for a continuance after the death of her father. The judge granted the request, but later reprimanded her after seeing pictures of the lawyer partying on the beach during the continuance period.

Further, lawyers should not presume that the use of privacy settings on social media will provide protection of posted information from discovery in the event of litigation. The law continues to evolve in this area, and courts have taken differing positions on this.

### Stay away from social “creeping.”

Social media risks are not limited to those arising from a lawyer’s sharing of information. Lawyers must also be careful when searching social media profiles for information about witnesses and other parties. It is established and expected that lawyers can review public sites to gather such information. But, they may not do so surreptitiously; “pretexting” by instructing an investigator to “friend” a non-party witness in the hope of gaining access to potentially damaging information on the witness’ protected social media profile would violate ethics rules prohibiting conduct involving dishonesty, fraud, deceit or misrepresentation. See, e.g., Phil. Bar Prof. Guidance Comm. Op. 2009-02. Evidence obtained this way would likely be rejected in court. On a related note, are you aware that when you look up someone on LinkedIn, they get a notification that you viewed their profile? This is good to keep in mind when researching a client or opposing councils’ credentials. Do you want them to know you’re looking into them?

Any breach of candor to the tribunal can compromise a client’s position before the court, with the jury or with the opposing party, raising the risk that a lawyer will face a claim for failing to provide adequate representation if the client is displeased with the outcome of the case.

### Managing Social Media Risks

Ultimately, the most important risk control technique when using social media is to simply think before typing. It’s important to recognize that, even with all the privacy settings turned on, nothing that gets posted online is 100 percent private. Most information related to a lawyer’s work should not be shared publicly.

With that admonition in mind, risk control in the social media setting should focus on limiting access to information about any representation. When using social media, lawyers and law firms should:

- Examine the security and privacy policy of any social media website before deciding to participate.

- Use available security and privacy protections to limit the reach and use of posts by others. This includes settings requiring prior approval of friend requests, or that provide users with alerts regarding who has chosen to follow updates or pages.
- Regularly revisit the security and privacy provisions of the site to monitor changes and react accordingly. (Most social media channels notify users when their privacy policies or terms of service change.)
- Set written rules for posting by office employees and professional staff on both personal and firm pages, clearly directing that only appropriately public information be shared. Consider applicable employment laws in formulating the rules. Monitor all posts on a regular basis, and inform employees of this in the rules.
- Monitor and adapt as the technology develops. The types of social media available on the Internet will continue to evolve. The ability to post data instantaneously and in real time from handheld devices continues to raise new challenges for lawyers, for instance. When a new type of social media becomes available, consider the need to revise firm rules regarding their use.
- Be careful about what their social profiles reveal. On some sites, such as LinkedIn, participants can receive rankings or recommendations regarding expertise based on their participation in question-and-answer forums. In some jurisdictions, answering those questions could be a violation of ethics rules prohibiting specialization or certification statements. In any jurisdiction, answering such questions could cause a lawyer to be held to a higher standard of care when faced with a professional liability claim.

Often the most important risk control approach is to use thoughtfulness, caution and common sense. While communicating professional practices on social media to your employees is the first step in managing these risks, you’ll want to have professional liability coverage in your corner, should the worst occur.

To learn more about how to keep your business protected, call 877-724-2669 or email [ServiceCenterSales@cna.com](mailto:ServiceCenterSales@cna.com).

