CNA PROfessional COUNSEL℠ Advice and Insight into the Practice of Law

New Technology and Law Practice Risk

Imagine a lawyer has just finished a grueling deposition preparation session with an uncooperative, less-than-brilliant but important witness for her side of a case. Understandably tired and a bit frustrated, she vents to her friends by updating her Facebook status while in the taxi on the way home:

> "Absolutely drained after spending 6 hours prepping Mr. No-Clue for deposition. Why do I get all the nut jobs?"

At the same time, in an elevator across town, an attorney hurriedly responds to a client's message by texting,

> "No Problem!"

The lawyer's text seemed clear enough, but what did it really mean? Was the lawyer agreeing to handle something? Suggesting that nothing needed to be done? Or, was the reply dripping with sarcasm because the problem was very big, indeed? While texting may now be ubiquitous, it is far from the most reliable way to ensure clarity and understanding when communicating with clients – or anyone else.

And what will the first lawyer do when a friend who comments on the post happens to be friends with opposing counsel, who can see the original status update and uses this serendipity as ammunition at cross-examination like this?

> Question: Did you meet with 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?

Lawyers must embrace technology changes that affect and improve how they provide service to clients. This obligation is rooted in ethics rules (e.g., Model Rule 1.1) requiring competence in all aspects of client representation, and in established precedent that measures a lawyer's standard of care against the standards and practices expected of other lawyers in similar circumstances. The best evidence that courts expect lawyers to adopt new technologies may be the fact that many now accept *only* electronically filed pleadings. Judges also regularly direct lawyers to use the Internet and other technologies to carry out judicial orders, and courts and ethics committees anticipate that lawyers will examine public postings and other Internet-based information when investigating witnesses, parties and even clients.

Beyond the legal requirements, keeping up with technology is simply good business. Social media, blogs and other interactive "Web 2.0" platforms allow lawyers to reach out broadly to colleagues, clients and potential clients. And remote use of technology – including Software as a Service (SaaS), Hardware as a Service (HaaS), online collaboration tools and other "cloud computing" processes – allows law firms to avoid investing in costly licenses, equipment or real estate.

But, it seems every innovation raises some new way for a lawyer to breach confidentiality, violate ethics rules or state and federal privacy and data security laws, potentially mislead clients, or fall short of the standard of care. Thus, while lawyers must keep pace with technological change, 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

One type of technology that lawyers have been embracing – like just about everyone else – is social media. Participation on Facebook, MySpace, Legal Onramp, Twitter and others 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.

The lawyer with the difficult deponent mentioned earlier not only is likely to be embarrassed before her client and possibly 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. If even one friend of the person who placed the original post comments on the update, that update is susceptible to being shared with the commenter's 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.

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.

Social media risks are not limited to those arising from a lawyer's sharing of information. Lawyers must also be careful when searching web sites 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.

Furthermore, 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.

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*. 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. Lawyers using social media tools 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;

- Separate personal pages from professional ones;
- 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 hand held 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.

Even when using the privacy and security settings provided, recognize that no social media post is truly private. Be truthful and circumspect, remembering that anything posted online should be treated as a public statement that will remain accessible virtually forever – to friends and foes alike.

The Risks of Online Professional Networking

Some social media sites are geared toward the business community and ask participants to fill out profiles that include questions about areas of concentration, specialization or expertise. On some sites, 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.

Lawyer standard of care is established by reference to practices of other lawyers in similar circumstances and to the specific expectations established between lawyer and client. If a lawyer suggests that a client can expect a higher level of expertise or performance because the lawyer is especially experienced in an area of practice, the lawyer will be held to that high standard if faced with a professional liability claim. Profile

statements on a lawyer's or firm's web page or social media site suggesting special expertise could be sufficient to set such expectations.

To help control these risks, lawyers can:

- Decline to participate – for example, avoid LinkedIn's automatic "expert" designation by not answering questions in the "Answers" area;
- Choose to not "claim" any site-generated profiles on web sites such as AVVO, Martindale Hubbell, SuperLawyers or other rating or locator sites;
- Specifically disclaim any responsibility for profiles they become aware of that they did not generate to avoid allegations that they have responsibility for the content.

Outsourcing and Online Tools

The remote use of software and/or hardware supplied and owned by outside vendors follows many models. Because these processes remain fluid, the risks are difficult to fully articulate, although some are clear. For example, there are obvious risks arising from the simple fact that the lawyer is relinquishing control over client information and work product to an outside vendor, which increases the potential for breaches of confidentiality and privacy as well as the loss of important data.

There also is the risk that data will become inaccessible due to the application of foreign rules or laws the lawyer never even considered would apply to the stored data. In many arrangements using SaaS or HaaS remote data-storage the vendor stores and moves data from place to place and jurisdiction to jurisdiction without conferring with the customer. For instance, if the data is moved to servers located in the European Union (EU), the data might be subject to the EU's tight restrictions on transfer of personally identifiable information. As a result, the lawyer might be unable to access that data when necessary.

The lawyer also could lose access to data if the vendor went out of business, changed hands or was unscrupulous in some way. Some authors have even suggested that simply giving the vendor access to the data

could constitute a breach of confidentiality or privacy that jeopardizes privilege protection or violates privacy regulations. To help manage these types of risks, lawyers should:

- Investigate vendors and review their privacy and confidentiality policies and processes. Consider whether they conform with attorney confidentiality and accessibility obligations. If not, do not utilize the vendor. If possible, obtain an indemnification agreement applicable to any breach of these obligations;
- Always use the security protections provided, including passwords, encryption and updated firewalls;
- Restrict access to stored records, and monitor the activity of those who do have access.

Shared storage and other remote access services both present and help manage privacy and confidentiality risks. For example, when information is stored remotely rather than on office servers or laptop computers, the risks associated with fire, theft or natural disasters in the office are eliminated. The use of remote collaboration sites, in which users share documents in real time, lowers the risk of transferring metadata to those who should not have access to it.

Conclusion

As lawyers embrace technological changes affecting the way they communicate and provide service to clients, they have an obligation to competently manage their use and to comply with confidentiality and privacy obligations. Lawyers must remain cognizant of the risks new technologies raise and understand how to address those risks. This can be challenging, as technology frequently develops well ahead of applicable rules and laws. At times the technology in question is already obsolete by the time adjudicatory bodies issue guidance or decision makers update rules.

Often the most important risk control approach is to use thoughtfulness, caution and common sense – such as following up an abbreviated text message with a phone call to ensure there is no confusion. Otherwise, "No problem!" could lead to very real problems for attorneys and their clients.

October 2010