# The dangers of social networking and how to avoid them

Although social networking tools offer lawyers many interesting new ways to interact with people in both personal and work spheres, there are some risks associated with using them. Before you venture into social networking, consider Section 5.5 of the Law Society's Practice Management Guideline on Technology ("Technology Guideline"). It states, "Lawyers should have a reasonable understanding of the technologies used in their practice or should have access to someone who has such understanding."

## Don't talk to or about clients or their matters

Social networking tools have complex and confusing privacy settings and most people are not entirely sure who can see the content they are posting. And blurting out something about a client on any social network, in particular anything sensitive or confidential, is a bigger blunder than the proverbial comment on an elevator because hundreds or even thousands of people can potentially access the information. Keep in mind Rule 2.03 of the *Rules of Professional Conduct* which states, "Lawyers using electronic means of communications shall ensure that they comply with the legal requirements of confidentiality or privilege." This rule clearly applies to social networking activities. It is tempting, and potentially very helpful, to toss out a question or seek strategic advice on a social network, but remember, even generic questions or comments about a matter you are handling could be read and recognized by someone involved with the matter. At the more social end of things, confirming a lunch date is probably not a problem – unless the fact you act for the client is confidential. And in that case you shouldn't even be "friends" with the client.

## Know and respect the marketing-related *Rules of Professional Conduct*

When using social networks make sure you comply with Rule 3 and the other guidelines which govern the marketing and advertising of legal services. Section 5.8.2 of the Technology Guideline states that, "Lawyers making representations in generally accessible electronic media should include the name, law firm mailing address, licensed jurisdiction of practice, and email address of at least one lawyer responsible for the communication." This information is on most websites and blogs, but is often overlooked on Facebook pages and Twitter bios (and it won't fit in a tweet!). You are free to offer your services via social networking tools, but keep in mind the restrictions on contacting recovering or vulnerable potential clients, distributing electronic advertisements directly and indiscriminately to large numbers of people.

## Avoid the unauthorized practice of law (UPL)

Lawyers need to appreciate that any content they post on the Internet can easily be accessed from anywhere in the world. Ontario lawyers practising law in other jurisdictions by providing legal services on the Internet should respect and uphold the law of the other jurisdiction, and not engage in the unauthorized practice of law. If you include the jurisdiction in which you are licensed to practise in your online content and posts, your clients will understand where you can and can't practise.

## Avoid conflicts of interest

The very nature of social media makes you more vulnerable to conflict of interest situations. Much of the information posted on social networking sites is public, and people frequently use an email or online name that is shortened or different from their usual name when communicating online. To avoid conflicts of interest when using social networking tools, lawyers should take reasonable steps to determine the actual identity of people they are dealing with and be very careful about what information they share.

## Don't give legal advice AKA avoid phantom clients

Providing legal information is fine, and indeed is helpful when you are looking to market yourself. However, you should be very careful never to give legal advice online. Unfortunately, the information/advice distinction can become quite blurred when a lawyer and non-lawyer communicate online, especially when the lawyer is providing answers to specific questions posed by a client. A lawyer-client relationship can be formed with very little formality. Be cautious about saying anything online that might be construed as legal advice. Include a disclaimer on your blog and within any information you post online. And remember, in Ontario the onus is on the lawyer who seeks to limit the scope of the retainer, and if there is an ambiguity or doubt, it will generally be resolved in favour of the client. Having a record of what was said or not said in a social networking exchange could help you defend yourself against a claim that you gave legal advice online.

## Protect your identity

One of the hidden risks of social networking is identity theft. Social network profiles can include information such as your birth date, university, mother's maiden name, etc. This information is often the answers to standard challenge questions that banks, credit card companies and others use to verify your identity. Someone intent on stealing your identity could visit social networking sites and gather information about you. Having your identity stolen can have severe consequences. It's not only stressful to have to restore your true identity, but also takes time and money and can leave you with a bad credit rating. The lesson is clear: don't help a fraudster steal your identity.

## Be polite and professional

With search tools such as Google, the vast Internet becomes a small town. With a few clicks your existing and potential clients can easily find almost everything that you ever said or posted on the Internet. It can be extremely difficult if not impossible to delete information once it is posted online. For these reasons you want to be civil and professional in all your online activities. Use proper spelling and grammar. Avoid using short forms for words. Exercise good manners and be polite. A good rule of thumb: Don't say anything you wouldn't say in person or that you would not want your mother to read on the front page of the newspaper tomorrow morning. And never ever start or continue a "flame war" – an ongoing sequence of hostile messages between two or more people. By their nature, flame wars attract a lot of attention, making it even more likely a client will find them. And be careful with social networks that post information about what you are doing online – see the adjacent sidebar.

## Making the wrong friends

In the world of social networking, people you have never met will want to be your "friend." It's nice to be popular, but there are differences between real friends and virtual friends. Knowing more people is great when it comes to marketing, but as the degrees of separation increase from you, two connected people will know less and less about each other, and the potential for a referral also becomes less likely. Think strategically about whom you want to be friends with and be careful not to be friends with someone who could embarrass you. For example, if you are a litigator, you probably don't want to be friends with any judges or experts, as it wouldn't look good to your opposing counsel. Ethics panels in the United States have said it is not proper for lawyers to become friends with someone to dig up information about them for use in a litigation matter. To decide whether to accept an invitation to be a friend, you need to consider the nature and purpose of the particular social network. It may be fine to cast a wider net on some networks. However, on more professional or personal networks, you will want to be more selective. Consider these general approaches:

- Invites from people you just don't know: Yes on Twitter; no on Facebook or LinkedIn.
- Invites from people you know by name only: Yes on Twitter and LinkedIn; no on Facebook.
- Invites from people you barely know: Yes on Twitter and LinkedIn; judgement call on Facebook.
- Invites from people you know but don't really like or respect (or want to be associated with): These can be awkward, but it is best to say no thanks or just ignore them.

## Don't blur your personal and professional lives

When Facebook was almost entirely a personal social network, it was easier to keep your personal and professional online presences separate. Now that many social networking tools are becoming connected and taking on more of a commercial aspect, it is becoming much harder to have separate online identities. People are using different strategies to deal with this. Some refuse to have a personal presence on Facebook as they feel it is almost impossible to keep a private "personal" site. For the personal safety of family and loved ones, most criminal lawyers post nothing personal online. Others will lock everything up and only link to their close personal friends. And some are creating a personal site for only their closest friends, and a fan page for business or professional contacts. On sites that are more commercial or professional, people will put up business information and be careful about how much personal information they post. ■

Dan Pinnington is vice president, claims prevention and stakeholder relations.

## Is Facebook secretly sharing what you are reading and watching?

During a recent phone call with one of my colleagues, we had a bit of a chuckle over a rather risqué video that one of our mutual friends had apparently just viewed online. Think clothing-optional antics by a celebrity in Vegas. As it happened, a few minutes before our call, we had both seen a Facebook update telling us that our friend had just watched a particular video. Our friend likely had no idea that the videos he was watching were being shared with the world via Facebook.

Some sites will automatically share your online activities (what you are watching, reading, buying, etc.) with your Facebook friends. These sites may warn you about this sharing the first time you visit them. This usually happens when you click through to look at an article or video that someone you know has shared. A little window will pop up with a vague warning before the article you want to read appears. You frequently consent to the sharing simply by proceeding to the article, although occasionally you will be asked to consent by clicking a checkbox. In most cases, this will be the one and only warning you get. From that point forward, an update will automatically be posted to your Facebook page with a description and link to every item you watch or read on that site. This is called "frictionless" sharing. The number of sites using frictionless sharing is growing and has included Amazon, Netflix, Spotify, Ticketmaster, Autotrader, TripAdvisor, Urbanspoon, Pinterest, and FourSquare.

Go to your Facebook Privacy settings page and review the list of apps you have installed and what they are sharing. And while you're at it, check the privacy and sharing settings on the other social media tools you use. Put a reminder on your "to do" list or calendar to review your permissions once a quarter or even monthly. Remember that checking your permissions helps protect your privacy.