# the scary side of Social Media

BY RUSS BANHAM

Ten years ago, a careless comment made about a boss or co-workers at the water cooler bred gossip, at worst. Today, when written in a text, blog, e-mail or on Facebook, such utterances can result in a lost job or worse—stiff liability charges for the inflammatory statements. A decade ago, a photo of you drinking beer in high school was shown only to close friends. Today, thousands of similar photos that should remain private are posted online, affecting children's college admission and employment prospects.

Self-display has never felt more affirming, nor has it been more risky. Social networking invites an alarming range of financial exposures for businesses and individuals, including libel, slander, defamation of character, invasion of privacy and copyright and trademark infringement. Personal security dangers, educational and career consequences and longstanding business reputational repercussions are also at risk.

"The perils embedded in social media are just beginning to be understood," says Jim Kane, president of HUB International Personal Insurance, a Chicago-based insurance brokerage. "Things you said that you wish you hadn't are preserved forever, creating tremendous liabilities. This virtual world is a new society, and people aren't sure about the rules of engagement."

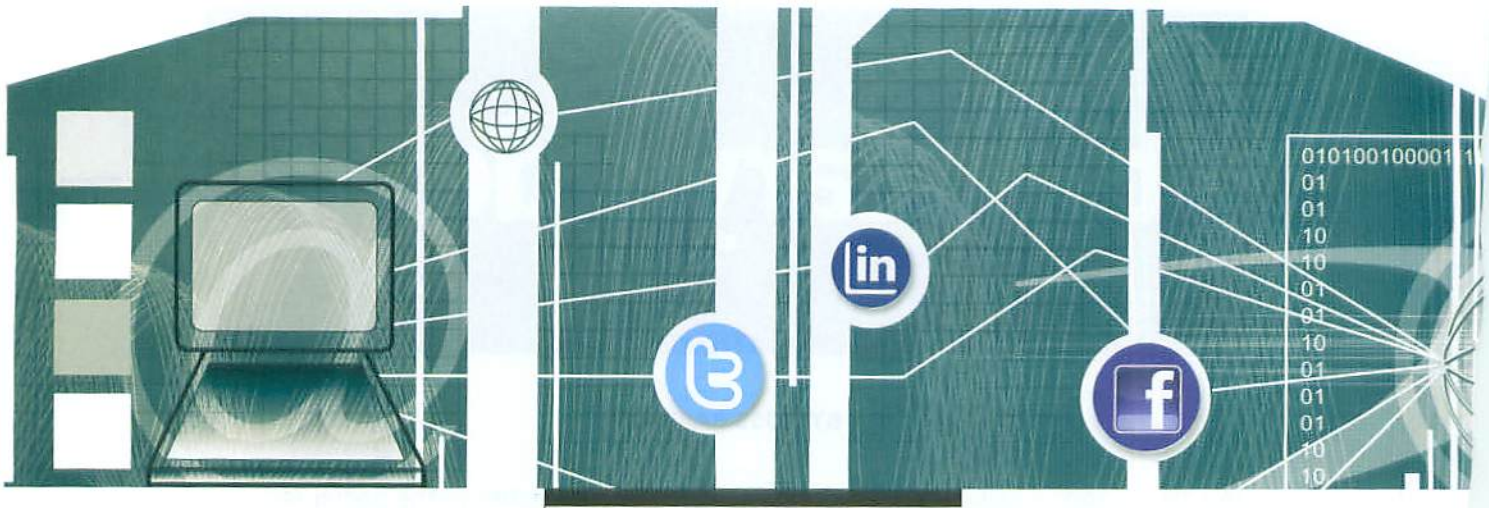
## Privacy Breaches in the Social Net

Facebook recently posted its 500 millionth user account. The cultural upheaval represented by the social media site and other online phenomena like Twitter, YouTube, MySpace, Flickr, LinkedIn and Tumblr was quick and defining. Already, these platforms and sites are playing a vital role in global geopolitics and commerce. Twitter, for example, has been wielded to mobilize large groups of people to protest government actions and elections, and support agendas from environmental causes to school closures.

People have lost their anonymity and, to a large degree, their privacy. An ongoing Wall Street Journal investigation charges Facebook with providing access of the names of users and, in some cases, the names of their "friends" to advertisers and Internet tracking sites. The newspaper alleges that even users who have set their profiles to the strictest privacy settings are at risk.

What is done with this information? The data can be "scraped" by a market research company to determine your interests and then sold to companies to send you targeted advertisements. "The current young generation is freely allowing their buying patterns to be tracked," says Kane.

The more personal information available, the greater the risk of harm to that individual, he adds. ▶




Kane notes a particularly distressing case of data scraping, cited in a Wall Street Journal article in October. "There is a website called PatientsLikeMe.com, where people tell personal stories about their emotional disorders, such as depression and bipolar disease," he says. "It turned out that a market researcher was scraping the messages and selling the data. People using the site said they felt extremely violated by what they saw as an invasion of their privacy. Although many used pseudonyms, imagine the impact on their careers and lives if they hadn't and the information became public."

Another growing exposure is identity theft. In July, a hacker named Ron Bowles legally collected and published online the personal details of more than 171 million Facebook users in a downloadable file. Exposed to the public were the users' account names, phone numbers, URL profiles, e-mail addresses and the names of individuals listed as "friends." While such information alone may not expose these individuals to undue risk, it opens the door to identity theft crimes if other personal identifying data, such as Social Security and credit card numbers, are illegally obtained to profit at the victim's expense.

A group of researchers at Carnegie Mellon tapped several social media sites to accurately predict the Social Security numbers for 8.5% of users born in the U.S. between 1988 and 2003. The researchers determined that an individual's date and state of birth are sufficient to guess at his or her Social Security number—often with great accuracy. "In a world of wired consumers, it is possible to combine information from multiple sources to infer data that is more personal and sensitive than any single piece of original information alone," said Project Leader Alessandro Acquisti, associate professor of information technology and public policy at Carnegie Mellon's Heinz College.

## Reputations Run Wild?

Social networking content opens up the potential of brand damage for corporate clients. Companies can face huge reputation implications if private or proprietary information is breached and leaked. "If you are a company tasked with maintaining private information on your customers and this information is disseminated to the public, your reputation is at stake," says Lilia Rocha, vice president at Momentous Brokerage, a Van Nuys, Calif.-based brokerage specializing in the insurance and risk management needs of celebrities and sports stars. "The same applies to an employee who makes an unflattering, unkind or erroneous statement about the company, its partners and customers, or his or her colleagues."

—R.B.

## Social Content Creates Liability

Each month more than 25 billion pieces of content are shared on Facebook, and every hour more than 24 hours of video are uploaded to YouTube. According to a survey by Nielsen, Americans spend one-third of their online time communicating and networking on social media sites, or writing blogs, e-mail and instant messages. What they are writing may encourage litigation. A recent survey of more than 1,000 people by Chubb indicates that 20% of respondents had written about a negative product or service experience on a social networking site. Thirty-seven percent of the respondents earning six figures or more annually had made such posts. Yet, only 2% stated that their attorneys had reviewed their comments prior to posting them.

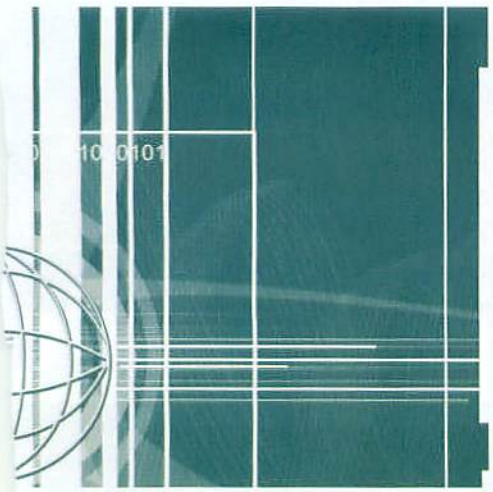
"From a content perspective, everyone using social media is considered a publisher, whether they are a company using it for branding purposes or a high net worth person using it to interact with others," says Ken Goldstein, Chubb worldwide media liability manager. "This creates intellectual property liabilities like copyright and trademark infringement. While professional journalists are trained in such liability matters, non-professionals may simply cut and paste another's work in a blog or post without crediting the original writer."

Case law is just beginning to be developed on the liability risks attending social networking. Rock singer Courtney Love was recently sued by her former fashion designer for "derogatory and false" comments allegedly made about her on Twitter. It is the first libel lawsuit in the website's history. Similarly, a defamation lawsuit was filed against actress Kim Kardashian by Dr. Sanford Siegal, the creator of the "Cookie Diet," for publishing alleged defamatory statements about the diet on her Twitter account.

While these cases involve celebrities, more ordinary Americans are also at risk. In another lawsuit, a landlord filed suit against a former tenant for tweeting that her apartment was "moldy." "Even saying something as seemingly innocuous as your job is 'boring,' assuming your boss or colleagues are your Facebook friends, can get you fired," Kane says.

## Getting Coverage for the Exposure

Despite these risks, many companies fail to take steps to reduce their exposure to loss. According to a 2009 survey by Travelers, less than 50% of employees utilize privacy settings on social media sites, and



only 36% were aware of their employers' policies regarding social media use. Other findings in the "Social Media/Networking Usage Trends Report" include:

- 34% of employees agree with the statement, "Employers should not be able to use anything employees post online against them, regardless of content."
- 30% think, "It's okay to post information online about your employer as long as it is true."
- 64% were "not at all" or "not very" concerned about online postings causing professional damage.

Personal and business exposures like the ones described above are being addressed by the property-casualty insurance industry through new policies, enhanced coverages and unique risk management services. "The atypical threats created by social networking are not contemplated in standard general liability or property policies, requiring in some cases an expansion in the coverage criteria," says Mike Daigle, president and CEO of DataRisk LLC, a Portsmouth, N.H.-based brokerage that specializes in technology risk and insurance. "In some cases you're going to need a specialized professional liability policy to address the magnitude of risks in the new virtual society."

Corporate clients can purchase media liability policies that absorb libel, slander, defamation and intellectual property liability, exposures that are typically excluded in general liability policies. Individuals should check the exclusions on homeowners' policies and ensure ample additional liability limits via umbrella insurance. For example, identity theft isn't a normal peril covered at high limits in these policies.

Chartis offers several optional add-ons to its homeowners policy. One responds to the loss of money, securities and personal property due to identity theft schemes. The endorsement enables clients to be reimbursed for the full amount of the loss, as opposed to the monetary limit in standard homeowners policies. Another new feature provides additional coverage if an incident that originates through social media results in a traumatic event or a violent threat.

## Safety at Stake

Beyond social networking causing reputational damage, far more serious is the alleged cyber-bullying that is reported to have led to the suicide of a gay student at Rutgers University. Equally worrisome is a study by Internet security consultancy AVG in Australia indicating that eight out of 10 children under the age of two have their pictures displayed on a social media site worldwide. This exposes the children's images and even their potential location to pedophiles, what AVG refers to as "stranger danger."

"The cyber world is an extension of the physical world, and yet people tend to separate the two," says Chris Falkenberg, president of Insite Security, a security and risk management consultancy. "Would you allow your child to go off with a stranger in the real world? Of course not. Yet, many parents fail to police their children's activities in chat rooms and social media sites."

Kane says adults are also subject to injury or burglary. "There are applications that allow someone who is a runner, for example, to post his or her running plans that day, where they plan to run and for how long," he notes. "You've now potentially alerted a burglar that you're not home or a stalker where you plan to be."

—R.B.

## Get Proactive on Risk Management

Kane says risk management is critical to "protect you from your own stupidity." Share the following tips with clients to help reduce their exposure to social media risks, courtesy of HUB International and Chartis:

- On Facebook and other social media sites, take advantage of the highest security settings and only allow "friends"—not "friends of friends"—to see your profile.
- When creating a profile, choose a different year of birth than your actual one.
- Be parsimonious with your "friendships." If you don't know the person in the real world, do not friend them in the cyber world.
- Make sure that your friend really is who she says she is. Follow up your friend requests with an e-mail, text or phone call.
- Make your children friend you. This enables you to watch them, and them to know that you're watching.
- Don't post or tweet your location or when you're going to be any place specific, to reduce the chance of being burglarized.
- Search for yourself using search engines like Google and people search sites like Pipl to find out what is being said about you, and then contact websites that have posted inaccurate or personal information to remove it.
- Consider investing in online reputation management services that will monitor the Internet for information about you.

Jerry Hourihan, senior vice president and national marketing manager for the Private Client Group division at Chartis, says more than insurance is required to manage social networking and related risks. "Our belief is that these exposures require not just specialized insurance coverage but proactive risk management to ensure losses don't happen," Hourihan explains. "Physical harm to a family member cannot be repaired by an insurance policy."

**Banham (Russ@RussBanham.com)** is an IA senior contributing writer.