THINK TWICE BEFORE YOU TWEET:
PRACTICING RESTRAINT IN A TWITTERING, LINKEDIN, FACEBOOK WORLD

Kevin K. Ho

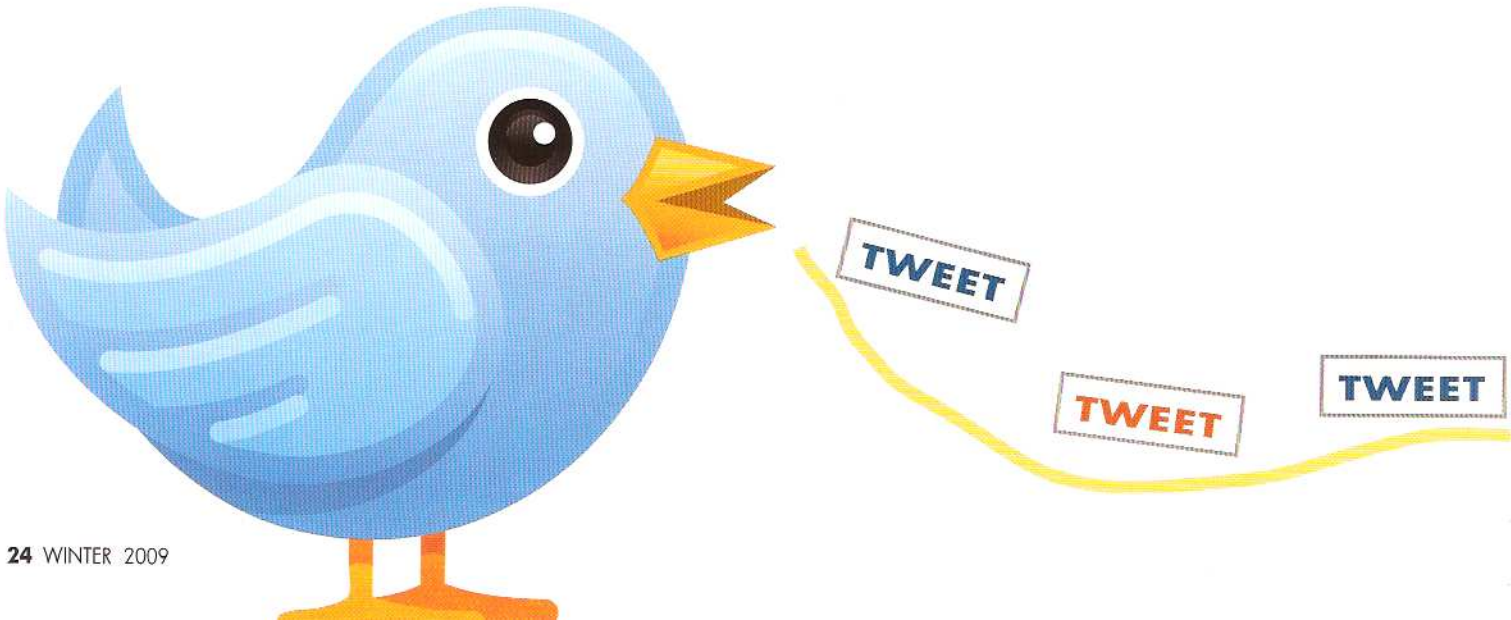
A stray remark isn't what it used to be. Today, a careless and innocuous remark or gripe made in passing can be broadcast to the world by just one mouse click or social network "status update." The consequences can end an employee's career or compromise a company in a matter of seconds.

The reason: Web 2.0. The Internet's evolutionary step, Web 2.0 lets users instantly broadcast and access vast amounts of information that is stored, aggregated, and disseminated to a wide audience from computers, cell phones, and mobile devices alike.

THE NEW "BIG THREE"

Integral to Web 2.0's growth are online social networking sites. Like in-person networking, online social networking allows people to connect. But unlike traditional networking, online connections and relationships are structured and potentially visible to the entire Internet. Three companies, Facebook, LinkedIn, and Twitter, have emerged as the relevant "Big Three" of Web 2.0 social networking. These sites are vast clearinghouses where companies and professionals can network and market themselves. Unlike their predecessors, the Big Three have leveraged Web 2.0 to allow an instantaneous, unedited, and constant flow of information to be posted, disseminated, and accessed from anywhere. And all of the Big Three sites allow users, and their friends and "followers," instantaneous access to each other's posted content.

According to the Pew Center more than 60 percent of employed American adults who use the Internet or email at work and more than 35 percent of adult Internet users have a social networking profile. Thus, it's clear legal professionals and their clients need to understand what social networking means as this area remains unsettled legally.



"You Are What You Tweet"

Twitter enables its users to post to their accounts, through a computer or mobile device, 140-character real-time messages and "updates" ("tweets"), which other users can follow on their own devices. A Twitter update ranges from the mundane to the relevant, but in all cases is contemporaneous and instant. Twitter receives an average of 50 to 60 million visits per month, and its users include individuals and companies wishing to market directly to other users. Tellingly, Twitter's terms of use cautions its users:

"You should only provide Content that you are comfortable sharing with others. . . . What you say on Twitter may be viewed all around the world instantly. You are what you Tweet."

What typically gets individuals into trouble is posting comments, content, or photos online imprudently. Because posting is instant, users can post to the Big Three in the heat of the moment. A user can change privacy controls and can remove content, but default settings are "public"—meaning all is available for everyone, including supervisors and competitors, to see.

And, unlike memories that fade, content posted online does not. In its terms of use, Facebook advises its 300 million users, "When you delete . . . content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time. . . ." Thus while a user may forget about what he or she posts on Facebook, LinkedIn, Twitter, or other sites like MySpace, the content itself can take on a life of its own.

Employers can be held responsible for using online content improperly against current (and prospective) employees, for defamatory or trade secret content an employee posts, and, sometimes, for posting potentially market-sensitive content prematurely.

Enquiring Minds Want to Know

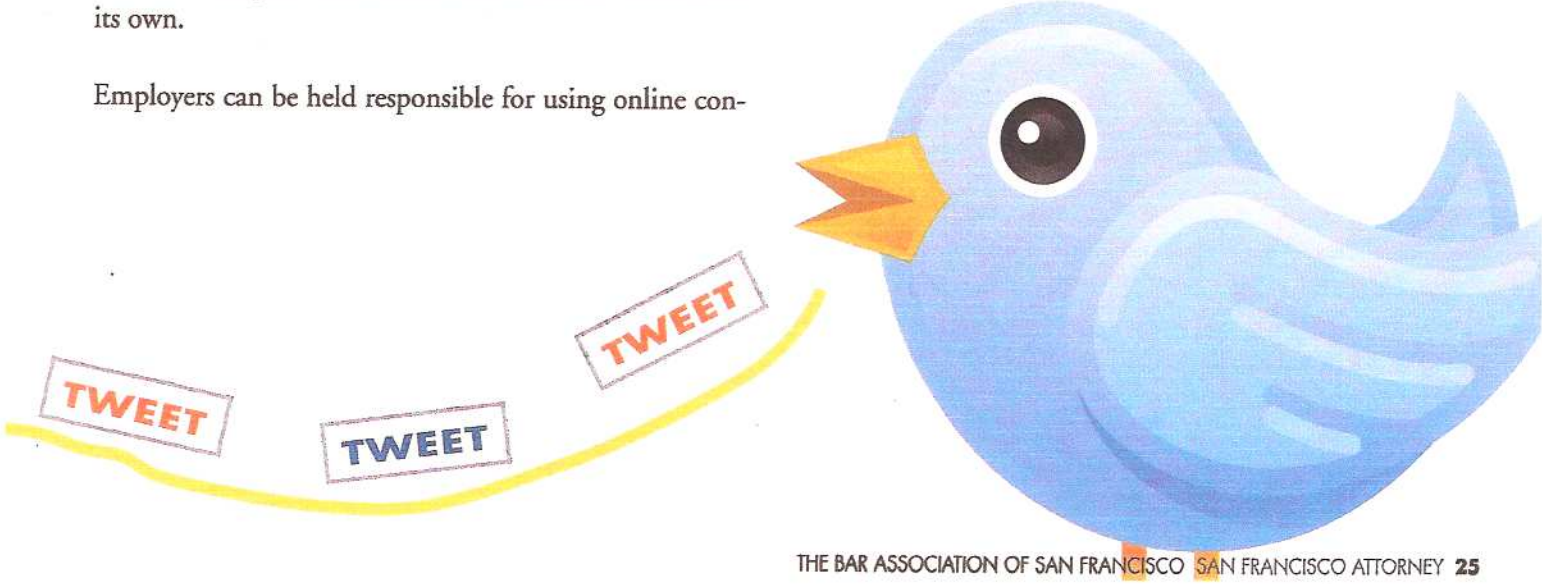
Jared Callahan, business development director for Novato-based background check company Employment Screening Resources (ESR), says most human resources professionals are now using social networking tools in their hiring practices.

Callahan says social networking sites are being used to source candidates or, in some instances, to screen a candidate, but only cautiously so.

"Most employers are cognizant of the fact you need a signed consent for any data you collect on a person," he says. "They understand this extends to social networking sites."

ESR, which serves more than five hundred Bay Area companies, advises its clients to use informed background check consent forms that clearly and specifically state that background checks will include social networking sites. Being specific, Callahan says, gives candidates fair notice, which many people need.

"There's a general consensus among candidates that even though information is out there, a social networking site is



semiprivate." Callahan says the misconception was especially prevalent among eighteen to twenty-four year olds, 75 percent of whom have a social network profile according to the Pew Center. "Anything you do online is automatically recorded; it goes somewhere. So don't do anything that will come back to haunt you, because you'll have a lot of explaining to do."

By adding social network screening to background checks, employers risk claims of unfair discrimination on embarrassing but otherwise legal behavior. Other pitfalls include violating equal opportunity employment laws like the Americans with Disabilities Act (ADA) or Title VII. Callahan says social network screening could implicate fair credit reporting standards, too, which require an opportunity to respond to any damaging information a background search could produce.

"What if you see a MySpace page for someone and there's pictures of them putting back a twelve-pack?" Callahan asks. "If you don't hire them, are you discriminating against them for a legal behavior? What about if they're an alcoholic under ADA?"

Callahan says that most of ESR's clients will only ask about social network screens, but like a resume, a social network screen may overwhelm.

"Even though it's available, you can get just as good results with a [standard] background check," he says. "The sheer nature of it may display things you don't want to know about a candidate or things that are not relevant to the job. What are you going to do when you find this all out? How can you unring the bell?"

Loose Lips Sink Ships

Issues change after a candidate is hired. Employees owe various duties to an employer including loyalty, maintaining confidential information, keeping trade secrets secret, and refraining from disparaging or harassing coworkers. Employers must respect employee's rights to free speech, privacy, and freedom from harassment or defamation and should evaluate and judge employees accurately.

Twenty-year veteran legal recruiter Barbara Levenson, a principal with Levenson Schweitzer, Inc., an attorney placement firm, cautions employees and job candidates about what they post online. "People seem to think that if its in cyberspace it doesn't count." But, she says, it does. "Whenever you're writing something online, ask yourself how you would feel if this were on the front page of the *New York Times*. If you don't want the world to see it, then don't put it out there."

The leading professional networking site, LinkedIn, similarly warns its 48 million users that "you must consider and decide, yourself, the extent to which you wish to reveal information about yourself to the large community of LinkedIn Users and to LinkedIn. . . ."

Trade Secrets Lost (and Found)

California's adoption of the Uniform Trade Secrets Act protects a very broad category of proprietary, valuable, and sensitive information from misappropriation. (Civil Code §§3426–3426.11). The current rule governing trade secret disclosures on the Internet, from *DVD Copy Control v. Bunner,* 116 Cal. App. 4th 241, 255 (2004), is outdated. *Bunner* says a trade secret may not lose its protection simply by being published on an obscure or transient Internet site, but will if the information is "quickly and widely republished to an eager audience."

Once information is released to the Web 2.0 world, taking it back is virtually impossible. While an employer can

assert claims against its employee, this will be little solace if valuable information is disclosed. Indeed, the *Bunner* court held any injunction to prevent future harm was useless as the harm was already done.

Employers are expected to take reasonable efforts to maintain trade secret secrecy, but policing every employee's "tweet" or "status update" twenty-four hours a day is impracticable. Besides, implicit in the Big Three's appeal is that information can be published (and republished) "quickly and widely."

Kevin Ho

Most employers use announced workplace Internet monitoring and usage policies, but these should be updated by adding a Web 2.0 policy when appropriate; otherwise a policy could be ineffective. See, for example, *Quon v. Arch Wireless,* 529 F.3d 892 (9th. Cir. 2009) (text message privacy not addressed in general computer usage policy).

Even with an articulated policy, the law is unclear on how much privacy an employee can expect with work Internet access. Even more tenuous is regulating an employee's off-duty, off-site conduct. California Labor Code sections 96(k) and 98.6, for example, prohibit adverse employment actions "for lawful conduct occurring during nonworking hours away from the employer's premises."

Other Risks

There are other risks employers must manage. What happens if an employee disparages, harasses, or discriminates against someone online? If employees form an online group to gripe about a company's policies, they could be engaging in collective and concerted labor organizing implicating the National Labor Relations Act but could also be harassing a fellow employee.

Comments employees post online could be imputed to the employer vicariously and directly. During work hours, a Cisco employee blogged about a competitor, and both he and Cisco were sued in two lawsuits. One settled just days before a jury was supposed to hear the case while the other is set for trial in early 2010. See *Albritton v. Cisco Systems* and *Ward v. Cisco Systems* (E.D. Texas, 2008-cv-89; 08-cv-4022).

Many victims of Twitter posts, for example, are now suing for defamatory tweets. For example, a fashion designer recently sued Courtney Love for defamation. On Love's MySpace blog and on the designer's Twitter page, Love threatened the designer's life and accused the designer of being a thief, a drug user, and a criminal. In a motion to strike, Love has claimed comments were made in a public forum and were of a public nature. The case—*Simorangkir v. Love* (Los Angeles Superior Court, Case No. BC410593)—remains open as of this writing.

All of these cases show that defamation and libel principles can be applied to online contexts, although courts have still yet to rule on the contours of online free speech rights under California law and public policy protections.

You're Fired

In California employment is "at-will" (Cal. Labor Code §2922). While free speech rights have been implicated in traditional workplace cases, Web 2.0's public-private sphere adds new complications when employees are terminated for disloyal, embarrassing, or insubordinate online comments.

While employees can limit their audience on the Big Three's Web sites, one California appellate court recently

said that, even though a poster attempted to limit her audience, her MySpace post was still open to the public at large, and a privacy expectation was unreasonable. *Moreno v. Hanford Sentinel*, 172 Cal. App. 4th 1125, 1132 (2009). The *Moreno* court said MySpace was neither an obscure nor transient Web site. The fact that the poster removed her content days later was irrelevant as she affirmatively made content available to any person with a computer and "thus opened it to the public eye."

What to Do? A Good Defense Is a Good Offense

Because Web 2.0 workplace privacy and free speech law remains unsettled, the best way to deal with these issues is through prospective policies that highlight termination as a possibility for defined online conduct.

Recommending employees is also tricky. If employers are willing to provide references, they must do so carefully. References that describe an employee's strengths but omit shortcomings may expose the employer to liability. Many employers simply follow a "no-reference" or a limited reference policy to avoid these concerns altogether.

For employees who post résumés online, Levenson urges consistency. "If you have different versions of your résumé, be sure to keep the core information the same," she says. For example, don't put different GPAs or schools. "People will compare. Be sure to be consistent."

Indeed, Callahan echoes. "There's an idea of common sense," he says. "Use some when you're social networking. The best bet is to be smart and take the five minutes to clean up your sites; [otherwise] you're screening yourself out of whatever position you're applying to."

Both Callahan and Levenson say they agree that, used correctly, social networking can be a positive way of self-branding on the Internet. "It's a good thing to let your network grow," Levenson says. "The more ways people can find a way to connect, the better. As long as you do it prudently."

Kevin Ho is a fifth-year attorney based in San Francisco. He grew up with the Internet and has focused on emerging online legal and social issues as a reporter, blogger, and attorney. Naturally, he has accounts on LinkedIn, Facebook, and Twitter, and he can be found at www.kevinho.org.