

# CAPTURING QUICKSILVER: RECORDS MANAGEMENT FOR BLOGS, TWITTERING AND SOCIAL NETWORKS

By Sharon D. Nelson, Esq. and John W. Simek  
© 2009 Sensei Enterprises, Inc.

Have you caught the Twitter bug yet? If not, you can be assured that some within your law firm have indeed gotten the bug. And what are they saying, when sending their “tweets” via Twitter? Stupid stuff like “walking the dog” and “when did I get so darn fat?” But they are also saying “the Smith, Smith and Smith law firm is EVIL” and naming names. And “we’re working on a case that’s going to put Acme Corporation in a stock market tailspin.”

Twitter, if you don’t know, is a free social networking and micro-blogging service that allows its users to send and read other users' updates (otherwise known as tweets), which are text-based posts of up to 140 characters in length. Updates are displayed on the user's profile page and delivered to other users who have signed up to receive them. That’s a very short explanation – learn more at <http://twitter.com>.

Do you have a “pish posh” reaction to Twitter? Maybe you should rethink that feeling, if you do.

From the *National Law Journal*: “Beware, Your ‘Tweet’ on Twitter Could Be Trouble”  
Subheader: Latest networking craze carries many legal risks

And is a tweet done on firm resources a “record” for purposes of retention requirement and, ESI preservation/production? It probably depends. If it is a company tweet, probably yes. A personal tweet, probably no. Probably. Much of this remains unsettled ground.

If you find that scary, you’re not alone. For a while, record managers thought they had the universe pretty well covered with e-mail and company approved programs. After a while, some of them caught up with instant messages. But Twitter, blogs and social networks have given almost everyone a Goliath-size headache. Whether you are thinking in terms of your own law firm or your clients, you must now consider these new technologies.

## **So how do Records Managers deal with this constantly evolving world?**

New technology bedevils records management (RM). Worse yet, the minute RM catches up to technology, technology leapfrogs ahead with something else to cause consternation.

Douglas Winter, who heads the electronic discovery unit at Bryan Cave, stresses that tweets are no different from letters, e-mail or text messages – they can be damaging and discoverable,

which is especially problematic for companies that are required to preserve electronic records, such as the securities industry and federal contractors. Yet another compliance headache is born.

Tom Mighell of Fios suggests that we may find a post from a proud employee that says “Our brakes are fine. I’m an engineer on that product. We went to 5X tolerance, so you can be rougher on them than you think. Don’t worry.” As Tom points out, after that post, “you’ve got potential product liability in 140 characters.”

Nolan Goldberg, of Proskauer Rose, has noted that you can get yourself in a lot of trouble in Twitter’s 140 character limit. Many folks don’t realize that “tweets” (Twitter postings) create a permanent record and that the tweets can go anywhere. Add to that the fact that, like IMs and e-mails, these quick electronic messages are often composed when someone is angry or frustrated or even under the influence of too much wine – sometimes leading them to display poor judgment. Though Twitter does not release the number of folks registered to use it, industry experts report that 3.4 million unique visitors visit Twitter each month – and that number is growing exponentially.

Twitter is by no means alone. There is also Yammer, and present.ly (no that’s not a typo) – and surely many more to come. Enterprise versions are just beginning to emerge, but there is currently precious little policy to govern them. For the most part, microblogs are being treated as blogs from a corporate policy perspective.

## **Blogs**

As blogs have exploded in popularity over the last few years, so have cases in which employees have disclosed trade secrets and insider trading information on their blogs. Blogs have also led to wrongful termination and harassment suits.

There should, of course, be a company policy about blogging at work or about work. Many companies sanction blogs – Microsoft has hundreds of them. One case has suggested that employers may have the right to prevent employees from accessing blogs while at work, which may fend off some of the dangers associated with blogging. *Nickolas v. Fletcher*, 2007 U.S. Dist. LEXIS 23843 (E.D. Ky. Mar. 30, 2007).

If blogs are allowed at work, the company needs to maintain blog archives where retention is mandated under laws or regulations. Blogs do indeed create a “paper” trail, for better or worse. Corporate blogging vs. individual employee blogging present different challenges – one clearly speaks for the corporation. The other may or may not, depending on the circumstances.

One notable recent case, from October of 2008: at the Transportation Security Administration’s official blog, a former officer blogged about a Newark officer arrested for stealing from passenger’s luggage, assuring readers that TSA has zero tolerance for theft and citing the number of officers terminated for theft. This was followed by probing comments from blog visitors

disputing the number of officers terminated and asking for hard data about compensation for victims. Not necessarily welcome comments for TSA. Blogs, clearly, can be a Pandora's box.

Enterprise blogs require security and authentication and audit trails. Likewise, it should be possible to search them, issue reports, etc. Control over enterprise blogs can be appliance based, an enterprise application or though software as a service (SaaS). As the example above shows, an enterprise will certainly want to consider whether to allow comments!

Audit trails should capture all changes, including new posts, changed or deleted posits, and comments and discussion. They should capture context, including who posted/commented, what posts are read and what posts are trackbacked.

One wit has suggested a very simple corporate blog policy: "Don't be stupid."

## **Social Networks**

The lifeblood of many employees is their social networks, including MySpace, Facebook, LinkedIn and Plaxo. Besides being a gigantic 'time suck,' these sites abound with risks for business as most businesses do not monitor their employees' sites and therefore all the risks associated with blogs apply here. Many experts believe that companies are well advised to use filters to block access to all social networking sites at work. At the very least, this action will keep the posts from being company records. On the other hand, genuine business usage of these sites has grown tremendously and it may be very difficult to allow business usage and forbid personal usage, no matter what a company's policy may say.

A 2008 independent survey commissioned by FaceTime Communications (based in the U.K. but we have no reason to suspect the answers would be much different here) found that roughly 80 percent of employees use social networks at work – and for BOTH personal and business reasons. The work-related purposes were for professional networking, researching and learning about colleagues.

As may be obvious, checking the social networking sites of potential employees may be wise, as an employer may get some sense of trouble brewing in the future, a lack of discretion, angry entries, a TMI (too much information) proclivity, etc.

Is employer monitoring of social networking sites really happening in the wild? The authors did an ad hoc online survey – though everyone said an employer had a right to monitor, no one actually knew of an employer who WAS monitoring personal sites. Likewise, others in the field have not yet been able to cite a case where social networking was involved to the detriment of the employer, but the consensus is clear – just wait a bit – it's coming.

## **Toss or Keep?**

From our viewpoint as folks involved in computer forensics, if you don't have to keep data and can't think of a reason why you should keep it, toss it. You'll save a fortune if you become embroiled in litigation. Shrinking the data to search will shrink the volume of potentially responsive data that must be reviewed.

Some of the emerging technologies are fluid (comments on blogs, ever-expanding discussions on wikis, changes on social networking sites, etc.). How do you manage something that isn't static and that has multiple authors? Snapshots are one method – and risk assessments are performed to determine how often snapshots must be taken. Periodic archiving is another possibility though it is a headache (again) to figure out how to schedule it. Training is helpful – employees need to understand that they are creating “records” when they use these technologies and think before they create records, bearing the risks of the records they create in mind.

### **The Web 2.0 World**

It's a brave new world, and most corporations and law firms are having a heck of a time dealing with it. It can involve huge costs, business disruptions, public embarrassment and, gulp, legal liability. Management of Web 2.0 records is limited at best, often chaotic and duplicative. This is a huge challenge for record managers.

And ponder this Web 2.0 risk scenario from Michael Cobb: “Suppose you're the CIO of a company that dominates its market to the point where competitors are grumbling about monopolistic practices. Some of your employees decide to “help” by going on the offense, denigrating these grumbling competitors in off-site blog posts and wiki entries, tagging negative stories on the Web, posting slated questions on LinkedIn, fostering criticism on FaceBook and so on. Then the company is hit with a lawsuit by its competitors for engaging in an alleged smear campaign. Your general counsel proclaims innocence and tries to limit the scope of discovery, but is compelled by law to agree to hand over all relevant ESI.”

Again, interesting. Your opponents will have trolled the Web for data. Can you claim ignorance? Must you produce these off-site communications by your employees? Can you afford not to know about Web 2.0 data? These are questions that are giving CEOs (and their lawyers) the willies.

### **Conclusion**

The law relating to emerging technologies (and we haven't covered wikis, unified messaging, VoIP, instant messaging, among others) is vastly underdeveloped, which presents a formidable challenge to records managers. If you have any guiding principle, make it this: Content, not form, drives retention requirements. Policies governing records in your law firm or business should address all forms of communications – and you'll need to review these policies at least annually in light of newly evolving technologies. Looking for solace? Think job security. No business today can be without records managers and the lawyers who counsel them.

*The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) [www.senseient.com](http://www.senseient.com)*