

Planning a company social network?

Don't forget privacy issues

Jay Cline

April 10, 2008 ([Computerworld](#))

Large corporations seem to be tripping over themselves in their rush to tap into the social networking phenomenon by deploying their own versions of online user communities. But by trying to shoehorn this generation's Woodstock into a corporate wingtip, they may be assuming risks that even the best social networks haven't fully addressed.

I have to admit: I'm one of those over-35 types who think they're hip because they have a [BlackBerry](#) but are deaf to the siren songs of text messaging and [Facebook](#). People like me think we have a hard enough time managing e-mail without getting sucked into a black hole of endless texting and friending. We're the cold showers in charge of corporate policy, and you'll have to warm us to the idea of deploying a "CitiBook" or "myHomeDepot" for corporate staff.

But despite our skepticism, the nearly universal use of social networking sites among those entering the workforce is thrusting this issue onto boardroom agendas around the country. We have to meet the expectations of our younger workers, the human resources department's argument goes, so that we can attract them and get the most out of them.

We heard the same argument during the dot-com boom, by the way, to explain why we needed to let new hires dress in pajamas and bring their parrots to work.

More sober IT departments have also been making a case for policy decisions on social networks, however. They see the large amounts of time users are spending on Facebook, [Flickr](#) and [LinkedIn](#). They worry about the productivity of their own IT staffers, the security risks of importing social-networking applications into the computing environment, and the

privacy risks of employee and customer data leaving the core network through these new channels.

To get ahead of the curve, traditional IT security managers have already blocked employee access to social networking sites as well as free e-mail services. The more daring chief information security officers are siding with HR, lobbying for internal social networks that redirect employees' attention inward, where they can be safer and more productive. Legal departments, for their part, are raising these questions:

- What if an employee posts to the corporate site revealing photos or a political rant? Is the company prepared to define its acceptable-use policy in detail, laying out what is obscene and which political or religious viewpoints are unacceptable? Will it assign someone to patrol content and respond to user complaints?
- What if an employee posts revealing photos or slanderous remarks about another employee? What if an employee appropriates another employee's image to promote a side business? Will it be enough from a legal perspective to have a process in place to remove content that harms another employee?
- What if an employee's extramarital relationship becomes a topic of discussion on the corporate site? Does the company proactively remove the content, or wait to become party to a divorce proceeding?
- When interviewing internal candidates for an executive position, should we consistently exclude or include a review of their profiles and postings on the corporate social network?
- Does the social network violate the company's own privacy policy by falling short of privacy principles regarding notice, choice and access?
- If an employee in the U.S. posts sensitive information about a European employee, does that constitute a cross-border data transfer in violation of [EU](#) privacy rules?

With these kinds of risks, is it even worth considering deploying a corporate social network? Mike Spinney, principal of communications consultancy [SixWeight](#), thinks it is.

"As a new generation enters the workforce, companies believe they're on the horns of a dilemma: lock out the social networking sites and deal with

discontented employees, or leave access unfettered and absorb a loss of productivity," he said. "But the issue isn't black and white. As a communications medium, there may be benefits to taking advantage of online social networking for developing valuable professional relationships. Companies need to become educated on the nuances of the various utilities and develop strategies and policies that take into account both the risks and the benefits."

But with nobody in HR, IT or legal departments wanting to devote staff to be the moral cops of the corporate social network, companies are often left with few options: They can automate content scanning and deletion, they can build a set of controls into the network that fosters a culture of both sharing and professionalism, or they can do both things.

What kind of controls would meet this goal? The Safe Harbor privacy principles provide an excellent framework:

1. **Notice.** During the registration process, *require* new users to successfully complete an online training module and test about the acceptable uses of the site, the privacy risks and controls available to them, and the sanctions for policy violation. Define what sensitive personal information is and prohibit posting it. Prohibit anonymous posts. Users' optional use of the site conveys their consent to be monitored.
2. **Data integrity.** During the site setup process, don't require employees to post more than what is known about them in the company phone book -- their names, positions, e-mail addresses and phone numbers. Automatically delete an employee's page upon job termination.
3. **Access.** Give users access to and control over what they add and subtract to their online profiles, and give them an effective way to search for their names on other employees' pages and photo tags.
4. **Choice.** In order to post photos and remarks, users must use a utility that enables any other identifiable user to report a complaint about the post or even delete it, giving employees the ultimate choice over what is said about them on others' pages. Companies with European operations may even need to require employees to obtain the

consent of other employees before posting their photos. Prohibit users from signing up other users to the network

5. **Security.** Prevent external access to the social network and the downloading of noncompany applications.
6. **Onward transfer.** To limit data sharing with third parties, prevent third-party ad serving, and set a new user's default settings to share his profile only within his own division.
7. **Enforcement.** Prominently post the network's acceptable-use criteria on the home page, regularly rotating the content to keep it fresh. Automatically scan for objectionable content. Include prominent links for abuse reporting throughout the site, and automatically suspend an employee's access to the network while a complaint about him is being investigated.

It has been said that U.S. fighter pilots dominated their foreign counterparts in World War II in part because the boys were fascinated with their cars and subsequently knew better than any how to fix and manage their flying machines. The new generation's facility with ubiquitous computing technology may give it the same edge in confronting this century's new threats to human liberty. The real question remains, How are risk-averse corporations going to plug in?

Jay Cline is a former chief privacy officer of a Fortune 500 company and now president of [Minnesota Privacy Consultants](#). You can reach him at cwprivacy@computerworld.com.