Workplace Social Networking Nightmares

By Lynne Eisaguirre

If you're not on LinkedIn, Facebook or Twitter, you're becoming unusual these days. And if you haven't thought about how you and your organization are being portrayed on these outlets, you're potentially putting both yourself and your company in danger.

According to a new Deloitte LLP Ethics & Workplace survey, http://www.deloitte.com/view/en_US/us/press/Press-Releases/press-release/4185f6b085912210VgnVCM100000ba42f00aRCRD.htm 60 percent of business executives believe that they have a right to know how employees portray themselves and their organizations in online social networks, yet a mere 17 percent of them said that they have programs in place to monitor and mitigate the possible reputational risks related to the use of social networks. Less than a quarter have formal policies on the use of social networks for employees but, ironically, nearly half of employees responded that detailed guidelines wouldn't change their behavior online.

Employees disagreed that their employer had a right to know about their off work, online behavior. Younger workers were especially vehement, with 63 percent of 18-34 year old respondents asserting that employers have no business monitoring their online activities.

What's the possible mischief with this disconnect? At least one-third of the employees in the Deloitte survey said they never consider what their boss or customers might think before posting material online, leaving your brand vulnerable. A leak of confidential company information also looms as a risk. For

those companies who are using these outlets to promote their own brand, an even larger issue exists.

Employees may also post harassing, damaging or defamatory information about their co-workers or bosses. I conducted one recent workplace investigation where an employee posted pictures of her new boss in a low cut blouse on Facebook along with the comment "she's a slut!" What can or should a company do in these situations?

TIPS: Handling Workplace Social Networking

As far as the law is concerned, according to Barb Grandjean, a Denver employment lawyer, "This is an evolving area and there is no clear guidance for employers and little case law. Employers will be required to balance a number of competing considerations when deciding how to handles these situations. Employers should revisit their electronic communications policies because they likely do not cover the newer types of communications."

For material posted on a publicly accessible Internet page, employers would seem to have the same right as anyone in the general public to access the posting, and, generally can take action based on the posting's content. However, one danger area I have noted when advising managers on this issue is that if they access a *restricted* website or social networking site without proper authorization, they face potentially significant exposure under the Stored Communications Act and state privacy laws. *Robert Konop v. Hawaiian Airlines, Inc.* http://www.internetlibrary.com/cases/lib_case32.cfm is one leading case on point.

Another problem is that in states like CO, CA and NY, which bar employers for taking action based on legal off-duty conduct (such as smoking or political protests), there is more of a concern. I think that even there, however, because employees do owe their employers a duty of loyalty, violating the duty of loyalty

to the employer by bashing it online may be a legitimate ground for discipline.

What about criticizing or harassing comments about fellow employees or supervisors? If it's just general grousing, the employer probably can't do anything about it because of the lawful off duty conduct statute. But if company information is being shared or significant harassing statements being made, the employer probably could argue that they fit within the exception to the statues because it creates a conflict of interest for the employer. Once you're on notice of the harassment, you have a duty to investigate and to stop it when and if it bleeds back into the workplace.

Clearly, if the employees are doing this on company time using the company's equipment and servers, you can design your policies so that you have a right to monitor their activity. I would also suggest creating policies that, even on their own time, they can't engage in conduct that would violate the workplace policy against harassment, disclose confidential information or trade secrets, or violate their duty of loyalty to their employers.

A related issue is giving a recommendation on LinkedIn. Here, I advise managers that they should follow the company's general policy on recommendations. Many companies these days require managers to simply give out name, rank and serial number, nothing more.

In summary, be safe rather than sorry while the courts are sorting out this issue. Talk with your attorney and IT experts about monitoring activity, and then revise your policies and train employees and managers based on their advice.