

September / October 2009

## MANAGING THE WEB 2.0

### Issues facing companies as a result of employees' online social networking and blogging

“Follow us on Twitter” or “Become a Fan on Facebook” are phrases that have become commonplace today. More and more people have turned to social networking sites and blogs to obtain information, stay connected with family and friends and voice their opinions on a variety of topics, and as a result businesses face a new set of questions and dilemmas with regard to their employees' use of such media.

A study published by Deloitte earlier this year entitled *Social networking and reputational risk in the workplace* surveyed 2,000 working adults and 500 business executives concerning their opinions regarding the privacy of online activity, its potential effect on employers and the rights of employers to monitor their employees' social networking sites. The results of this study are eye-opening and clearly underscore the need for businesses to educate themselves and address the issues that can arise as a result of their employees' use of online social networking sites, blogs and other “Web 2.0” applications.

#### **NEGATIVE “PUBLICITY” ON THE WEB**

One major concern that most employers share is the potential for the disclosure of sensitive or confidential information and the adverse effect of negative posts by their employees on blogs and social networking sites. The results of the Deloitte survey confirm that employers have good reason to be concerned. According to the study, 74% of the employees surveyed believe that it would be “easy to damage a company's reputation using social media.”

#### **PRIVACY CONCERNS**

Complicating the equation for employers is the fact that employers and their employees also have

widely divergent views on the topic of whether employers should access and monitor employees' social networking pages. The Deloitte study found that 53% of the employees surveyed feel that their social networking pages are personal and that their employers should not view those pages. On the contrary, 60% of executives surveyed believe that they have a right to know what their employees post online.

Some companies have hired a “blogging monitor” whose job is to comb the Internet for posts involving the company or its products or services and to notify designated company personnel regarding the content of those posts. The company and “blogging monitor” may in some instances respond to negative posts. A company that decides to hire a “blogging monitor” must be careful to set guidelines regarding what sites the monitor may access and how the company may respond to negative posts to avoid legal issues and further negative publicity.

Obviously, if employees do not limit access to their blog posts or social networking pages, there can be no expectation of privacy and employers may review those pages. The more difficult situation for an employer involves employee sites or pages which have privacy settings in place such as password protection. A recent jury verdict in a case against the Hillstone Restaurant Group in New Jersey makes it clear that employers do not have a right to access such pages unless they are given express permission or consent. In the case, management viewed a MySpace page set up by employees of one of their Houston's restaurants in New Jersey as a place to “vent about any BS we deal with at work without any outside eyes spying on us” after a

Route to:

---

---

---

manager of the restaurant obtained the e-mail address and password of an employee, who was a member of the group, and then shared that information with members of upper management. The site contained content of an extremely defamatory nature regarding certain policies of Hillstone and managers and customers of the individual restaurant, and the employees who set up the site were terminated. The jury found that the employee who provided access at her manager's request did so only because she feared adverse employment consequences, and as a result the Hillstone Restaurant Group violated the Federal Stored Communications Act, 18, U.S.C. 2701, et seq., and New Jersey invasion of privacy laws, because its managers accessed the password protected site "without authorization."

### **CORPORATE POLICIES**

Because an employer does not have carte blanche to access its employees' social networking sites, what can an employer do to protect itself from the damage that can be caused to its reputation in cyberspace?

One very simplistic approach is to prohibit access to social networking sites and blogs from computers on the company network. According to the *2007 Electronic Monitoring & Surveillance Survey* published by the American Management Association in February, 2008, over 65% of companies use some kind of internet blocking software to prohibit employee access to certain sites with 50% of those companies blocking access to social networking sites and 18% to external blogging sites. While such a policy will prohibit unwanted internet surfing and the use of company computers for negative posts, the gain in productivity could be offset by the negative effects of preventing employees from effectively networking with friends and past colleagues or conducting research for business purposes and a decrease in employee morale particularly among younger, more technologically savvy employees. Such a policy also does not protect an employer from the harm that could come from negative comments concerning the company posted to blogs and social networking pages by employees on their personal time using their own computers.

Most commentators recommend that a company craft a corporate policy regarding social networking and blogging by employees but

caution that there is not a uniform template. There are, however, some common bits of advice that appear in the available literature on the subject. Any blogging or social networking policy should remind employees that negative or disparaging comments regarding the company posted to blogs or social networking pages are a breach of their duty of loyalty to their employer which may result in termination (particularly in at-will employment states). The company's anti-harassment and discrimination policies should be incorporated into the blogging and social networking policy. Employees should be encouraged either to refrain from identifying themselves as employees of the company in blog or social networking posts or to include a disclaimer that states that their opinions are personal in nature and do not reflect those of their employer. A blogging and social networking policy should also prohibit the use of company logos, or other intellectual property, or the disclosure of any confidential or proprietary information, whether intentionally or inadvertently, in any posts made by an employee. Once an employer has developed a social networking policy, the employer should publicize it, educate and train employees regarding the policy and obtain a signed acknowledgment of the policy from each employee.

Companies cannot afford to ignore the dangers that are presented by their employees' online social networking and blogging activities. However, they must also refrain from taking actions that result in other negative consequences. In this author's opinion, the most well stated principle for formulating a company policy on social networking and blogging is the following found in an article by H. Christopher Boehning and Daniel J. Toal entitled "Social Networking Data Presents Challenges" and published in the July, 2009, *New York Law Journal*: "Policies should encourage personal responsibility and treat employees like adults, while also explaining and underlining the risks for the company and the consequences of wrongful social networking behavior."

—Rick Carter

---

© 2009 SRA International, Inc. All rights reserved, including electronic reproduction or alteration. This SRA Update is published six times annually for the clients of Sanford Rose Associates – now in our 50<sup>th</sup> year of Finding People Who Make a Difference®.