Connecticut Law Tribune

FEBRUARY 1, 2010
VOL. 36, NO. 5 • $10.00

An ALM Publication

CTLAWTRIBUNE.COM

Keeping A Watchful Eye On Web. 2.0

Businesses must guard against employees spreading confidential information

By CHARLES L. HOWARD and CHRISTOPHER R. DRURY

Even as many businesses struggle to adapt their technology and personnel policies to deal with the improper use of e-mail and its potential for unauthorized disclosure of confidential and proprietary information, technology has created new Web 2.0 applications that generate additional risks of unauthorized disclosure.

Today, Web 2.0 encompasses online social networking sites such as Facebook and MySpace, web-based applications such as Google docs, video-sharing sites like YouTube, wikis, blogs, and micro-blogging services like Twitter. The defining characteristic of Web 2.0 applications is that they permit users to interact with other users to create content, as opposed to passively viewing information that is simply presented to them. Since much of the information is transmitted on third-party servers and through the Internet, just the process of finding out who may be doing what is daunting.

Yet, it is precisely these seamless features that make Web 2.0 applications particularly problematic to businesses. Not only are employees spending an incredible amount of time on these sites, both for business purposes and personal reasons, but they do so with a casualness of communication that creates a greater risk of disclosure of sensitive workplace information. And to further complicate matters, discovering what employees may be doing and saying presents its own set of challenges.

Why Businesses Care

The short answer is two-fold: people are spending an incredible amount of time texting and accessing social networks during work time, and they often reveal information they should not be disclosing about their employers or workplaces.

A study by Nielsen Online reported that the time spent by users of social networking sites such as Facebook, Twitter, and MySpace increased from almost 9 billion total minutes in 2008 to more than 19 billion minutes in 2009. According to another report by Nucleus Research, nearly half of all online workers use Facebook at the office and one in every 33 employees has built their entire profile during work hours. The financial impact to businesses resulting from loss of employee productivity is clear.

Charles L. Howard

Christopher R. Drury

Organizations are also at risk with respect to the disclosure of confidential information through inadvertent or intentional dissemination and sharing by their employees. A June 2009 survey commissioned by Proofpoint, an Internet security and data loss prevention company, revealed that 34 percent of the participating organizations had suffered a loss of sensitive data, 18 percent had investigated data loss via a social networking site or other Web 2.0 application, and 38 percent had begun monitoring outbound e-mails to prevent data leaks, up from 29 percent in 2008.

People often post messages without seriously considering the nature and impact of what they are sharing. Depending on the information being shared, the risks to businesses can be severe. For example, a spur-of-the-moment update of a profile by an employee who expresses frustration because he has to spend the weekend finalizing the details of an acquisition involving his company could have serious repercussions for both the employee and the company. Similarly, what may otherwise seem a casual comment could, in fact, result in the disclosure of sensitive information. An employee might, for example, post a comment in a discussion with her friends about the difficulty she has encountered in testing a product for her company or the inattentiveness of a supervisor. Once that information is posted, it may be shared with others and could ultimately be the key piece of information in a products liability lawsuit.

Straightforward Steps

Left unsecured and unmanaged, widespread use of Web 2.0 applications and

Charles Howard is a partner at Shipman & Goodwin LLP and a member of the Intellectual Property Group. He is also chair of the firm's E-Discovery and Information Governance Group. Christopher Drury is a litigation associate at the firm and is a member of both the Intellectual Property Group and the E-Discovery and Information Governance Group.

eDiscovery
Technology and Law

social networking sites creates the potential for both loss of productivity, as well as the loss of confidential information. At the very least, businesses should consider taking three straightforward steps.

The first step is to learn about the new technologies and determine the extent to which employees are accessing social networking sites and using social media while at work, for what purpose (business or personal), and what may be an appropriate workplace response.

The question is not whether employees are going to use social media, because nothing is really going to halt the Web 2.0 trends identified above. Rather, the question is whether the employer should limit access to business purposes only or prohibit access to the sites during work hours on business owned equipment. The answer to that question raises both technical and policy implications. While motivated employees who are technically savvy will likely find a way to bypass any such restrictions and obtain access to the sites, there are ways that access can be routinely blocked or monitored.

In addition, appropriate policies can clearly articulate what activities are permitted or prohibited and serve to place employees on notice that they have no expectation of privacy in messages sent through their employers' equipment or system. Once a policy has been developed, of course, it is worse than useless unless compliance is monitored and enforced. Businesses should make employees aware that their actions are subject to monitoring and that failure to adhere to company policy could result in disciplinary action and/or dismissal. Nevertheless, before an organization begins to monitor its employees' activities, it should consult with counsel to ensure that it does so in such a way that does not violate any privacy or employment laws.

The second step is employee education. Businesses need to explain to their employees how the use of social media and other Web 2.0 technologies – whether at work or outside of work – can have a workplace impact if they disclose confidential or sensitive information, or if the information they post online reflects negatively on their employer. This may come as a surprise to the younger generation of users, but they should be reminded that any information disclosed likely would be considered public information, even if it is only being shared with a few friends, because once the information is posted, there is no control over where and how the information is shared from that point forward.

And finally, businesses should consider developing procedures for capturing information used by the Web 2.0 applications. Many employers already use social networking sites in screening applicants for employment. They should consider obtaining discovery from third party providers of social networking services if the issues in a case – such as claims of harassment and discrimination or theft of trade secrets – suggest that key individuals may have been active on social networking sites.

This is particularly important since, unlike e-mail, information on social networking sites is under the control of third parties, which creates greater challenges in terms of obtaining and preserving relevant information. Although there have been few cases in which evidence issues relating to social networking sites have had to be resolved, it is only a matter of time before more of these issues are raised. Indeed, a federal court in Connecticut recently ruled in favor of full disclosure of information obtained from a social networking site in an action involving a student dispute with a prep school.

Buckle up and prepare for the challenges of Web 2.0 because they are surely coming. The failure to keep up with the spread of social networks and Web 2.0 applications can lead to the loss of employee productivity and possibly valuable business information. Now is the time to identify the holes and start plugging the leaks. ■