KAYE SCHOLER LLP

NOVEMBER 10, 2008

Employees Online: Protecting Company Interests in a Web 2.0 World

by Robert Barnes and Darya V. Pollak

Interactivity rules today's Internet. Generation "C" users — so-named because of their content-generating activities — interact via blogs and social networking sites, create and upload video, edit wikis, and provide up-to-the minute personal update "Twitters," all for the instant review and commentary of others. In on-line gaming worlds, avatars — virtual representations of participants — interact with individuals across the globe, often engaging in virtual, and sometimes real-world, commerce.

In this brave new interactive "Web 2.0" World, how should employers protect themselves as growing numbers of employees engage with outsiders, often independently of supervision, and sometimes in the company's name or as its apparent representative? How, and to what extent, can an employer control what an employee posts on the Internet during non-work hours from a non-work computer?

While many employers already have policies governing nondisclosure of trade secrets and use of company computers, few have taken the necessary next steps of letting employees know what interactive Internet activities are appropriate and what are unacceptable, whether or not on company time or property.

Take, for example, the termination of former CNN producer Chez Pazienzia who claims CNN fired him for unauthorized blogging. Responding, naturally, through his widely-read blog, Pazienzia took CNN to task for not giving him notice of any formal policy identifying what is allowed and what is impermissible for employees' Internet postings.

While cases like Pazienzia's may be relatively uncommon today, that is unlikely to be so for long. Employers should now be drawing their own bright lines for this new frontier before employees (and perhaps courts and juries too) draw it for them. Consider the following when developing your company policy:

1. Define Your Objectives, But Do Not Overreach. Web 2.0 is an excellent vehicle for growing brand awareness and reaching out to consumers and others, especially when targeting younger or more tech-savvy markets. Allowing your employees to engage online with consumers can generate excitement about upcoming products and initiatives, and increase your online presence. Blogs demonstrate your employees' expertise as they comment on posts or answer questions from consumers and industry colleagues. For any of these reasons, your company may decide to encourage employees to blog about non-confidential company matters.

Remember, however, that for your employees' comments to have impact in the "blogosphere" they must speak candidly, and not appear to be parroting the "company line." As always, there has to be a balance. You may not want to inhibit your employees unprompted expressions of enthusiasm for the company and its products. But, you need to be prepared to act against an employee making inappropriate and unprotected comments online.

Sun Microsystems and many other companies have created their own company-sponsored blogs and Sun's policy contains sensible advice: "[A] community site is a public place and you should avoid embarrassing the company and community members .... The best way to be interesting, stay out of trouble, and have fun is to write about what you know." If your employee Web 2.0 activities take place on company time or with company equipment you may have greater responsibility for the resulting content. If you create company-sponsored blogs or other Web 2.0 vehicles, consider seriously using filters, or implement other measures to moderate content before posting to prevent the uploading of improper material.

But, once you purport to exercise supervision, your defensive measures may, ironically, reduce your legal protections. For example, active oversight of employee-written blogs would likely preclude any Communications Decency Act immunity you might otherwise have had by remaining passive. The greater the tolerance for and facilitation of employee blogs' content, the greater the risk of liability for intellectual property infringement, defamation or other torts if the content crosses any legal lines. Blogging by high-level executives raises additional concerns.

If your instincts are defensive, and you want to maximize the protection of your company's proprietary information and image and minimize legal exposure, adopt a restrictive approach to employee Internet interactivity. You can prohibit Web 2.0 activity on company time and property. You can also largely forbid your employees from commenting on work-related matters entirely — even on their own private time. An unambiguous and broadly publicized written policy can meet those goals.

But, if you decide to impose tight controls, take care not to run afoul of your employees' rights. For example, the National Labor Relations Act protects certain union and pre-unionization activity, and insulates discussion of other matters of common concern such as wages and working conditions. A technology policy cannot mask unlawful efforts to stifle your employees' collective bargaining activities.

2. Company Policy Applies. Many employees do not realize that out-of-work Internet activities may expose them to adverse employment actions. Any Web 2.0 policy, whether lax or restrictive, must emphasize that all existing company policies apply fully to Internet conduct.

You should also be sure to integrate references to Internet usage and activities into your company's well-established policies on disclosure of intellectual property and proprietary information, non-harassment, and non-discrimination. A comprehensive Web 2.0 policy can even extend to the company dress code. IBM's "Virtual World Guidelines" remind employees that "You need to be especially sensitive to the appropriateness of your avatar or persona's appearance when you are meeting with IBM clients or conducting IBM business."

3. Disclose and Disclaim. In an extreme case, the company may be at risk of liability to a third-party because of an employee's posting. Clear directions to would-be employee bloggers will help the company manage the risk of exposure to liability for what is said on a private blog. Employees who comment on company or industry matters must identify themselves as employees of the company. An employee should never purport to speak on behalf of the company without express authorization. If the post is a personal comment related to the company or industry, it should include a disclaimer that the views expressed are the employee's alone, and not those of the company. The poster should provide contact information for the company representative authorized to speak on the matter.

4. Beware of the SEC. Securities law and regulations strictly limit the type of information public companies may share.

An employee's inadvertent posting on any corporate financial matter may have serious repercussions. Draw a line and warn your employees to stay away from any comments on financial matters. Comments on the company's share price, revenue, future plans, performance and forecasts, and undisclosed financial results should be absolutely forbidden.

5. It's Not Private! Blogging and Internet usage require the same restraint as other public behavior. Though it seems obvious, remind your employees that their Web 2.0 activities, even if posted under pseudonyms, are not private. Even after a decade of ubiquitous e-mail usage, people still can be oblivious to the permanency of pushing the 'Send' button. Once sent, inappropriate posts cannot easily be recalled.

Your basic computer usage policy should already retain your rights to monitor Internet usage on company time or equipment. Depending on your corporate culture, you may also want to remind employees that the company has the right to monitor public Internet postings made using personal time and property. Many employees will be surprised to learn that they do not have an expectation of privacy preventing their employers from viewing their Facebook or MySpace pages, YouTube videos, Twitters or blog postings, provided that such content is publicly accessible online. Forewarned is forearmed: employees may avoid being reckless in their online conduct if they know the boss could be watching.

6. Respect Intellectual Property Rights. In addition to protecting your own IP rights through a carefully-drafted policy applying to all employees, you should remind employees that copying and posting non-original content may render them personally liable for copyright or trademark infringement. Actual and/or statutory damages, plus attorneys' fees and costs, may result from infringement of a third party's rights.

The law of contributory and vicarious infringement is complicated and, in some respects, unsettled. However, in certain circumstances, the company may be held liable for an employee's infringing conduct, particularly if the content is on a company-sponsored site and acts as a draw for consumers.

7. Plan for Criticism. Like it or not, Web 2.0 provides a powerful tool for popularizing expressions of discontent. A Google search of your company name followed by the word "sucks" may yield some unpleasant surprises.

You should resist the temptation to take action against employees criticizing your company online without a careful investigation of the law and the facts. In some situations, the employee's conduct could involve protected speech or conduct. You may be liable for deterring or punishing the exercise of those rights. If you are a public agency, there may be First Amendment issues.

Depending on the accuracy, significance, effect and importance of the employee's comment and your corporate attitude towards criticism, you may decide to let the comment slip relatively unnoticed into the vast mass of information on the Internet. But take care to apply your tolerance consistently and fairly, or you may lose control of your ability to curtail truly undesirable content and conduct.

Some employers decide to embrace Web 2.0 and allow employees to share both positive and negative thoughts on the company and respond where appropriate. Such interactions may benefit the company by alerting it to ways to improve its product or better manage its human resources. Toleration of constructive dissent can boost employee morale, and create a public image of a company that is both technologically progressive and open to dialogue with its employees and/or consumers.

Some companies, such as Wal-Mart and Sun Microsystems, feature employee blogs on their webpages that allow consumers to post comments or responses. While these comments can sometimes be critical, they are invariably more civil and open to dialogue than those on third party anti-corporate webpages. Your employees can actually help manage negative PR and debunk public misconceptions by responding to critical consumer posts on your blog.

Ultimately, your company philosophy, culture and marketing strategy will determine the extent to which you wish to limit or encourage company and employee involvement in Web 2.0 and virtual worlds. Counsel can assist your company in tailoring an Interactive Internet Activities policy to your specific needs.

Employee Internet interconnectivity is here, and will grow. A sensible and thoughtful approach to what your employees can do, and the consequences of where you draw the lines, will help your company navigate this emerging wave.

* * *

Robert Barnes is a Partner in the Litigation department in the Los Angeles office of Kaye Scholer LLP and may be reached at 310.788.1180 or rbarnes@kayscholer.com. Darya Pollak is an Associate in the Litigation department in the Los Angeles office of Kaye Scholer LLP and may be reached at 310.788.1289 or dpollak@kayescholer.com.