Online Social Media and the Workplace

What's an Employer to Do?

By Daniel B. Klein, Esq., and Dana L. Fleming, Esq.

This scene may be familiar to you: word reaches the human resources department that an employee's Facebook page contains photographs of a sexually explicit nature. Or a manager learns that a job applicant has posted controversial religious commentary on a blogging site. Or an employee has "tweeted" about the upcoming layoffs.

Welcome to Web 2.0. Websites that incorporate user-generated content have burst into the workplace, and the resulting personal information overload has, in turn, inundated human resource offices everywhere. Web 2.0 includes social networking sites (Facebook, MySpace, LinkedIn), blogging sites (Blogger, Tumblr), microblogs (Twitter), and video sharing sites (YouTube, Flickr), among others.

The explosion in employee use of online social media creates substantial risks for employers. These risks range from lost productivity, as employees endlessly surf and update their status, to stress on the company's internal systems and networks. Employers may also find that their employees have started anti-employer sites or members-only groups where they can vent about their managers, their compensation, their parking spaces—you name it. The widespread use of social media by employees also increases the risk of exposure of an employer's confidential information and trade secrets as well as the potential for insider trading and other securities laws violations. Employees' use of social media encourages real-time, uncensored and occasionally anonymous postings about employers. This type of unfettered public commentary can create serious customer relations issues for companies as well as compromise employee morale. Think of it like the rumor mill—but on steroids.

In addition to productivity and business problems, employee social networking and blogging creates a host of legal risks. Some risks are fairly obvious: Companies could face potential liability for torts committed by employees, including invasion of privacy, negligence and defamation of the company's employees, customers or competitors ("cybersmearing"). Others are more nuanced: Employers could be held liable for failing to stop unlawful harassment of an employee through comments made on a social networking site if the site relates to the workplace in a direct manner and the employer has reason to know about the harassment. Even a manager's seemingly innocent decision to "friend" some employees, but not others, could give rise to a claim of discrimination or retaliation.

How do employers balance these risks? Should employers monitor Facebook, YouTube and Twitter to ensure that employees are not badmouthing the company? Should employers use these sites as resources to screen job applicants? Should businesses jump into the fray and use social media as part of their own employee morale-building and marketing strategies?

This article explores the many legal concerns that have arisen from social networking in the workplace and discusses a variety of best practices that employers can use to try to manage these risks.

EMPLOYER CONTROL AND RESTRICTIONS ON EMPLOYEE POSTING AND BLOGGING

As the popularity of social networking increases and becomes more mainstream, employers may feel inclined to regulate their employees' Web 2.0 activities more tightly. However, employers must balance this impulse against an array of legal risks associated with terminating or disciplining employees for their online activities. For example, employers need to be aware of whistleblower protections under various state and federal laws (e.g., Sarbanes Oxley) that may apply to employees who criticize certain business practices in a blog entry or post. Likewise, the National Labor Relations Act prohibits employers from interfering with or discriminating against employees who engage in concerted activities for the purpose of collective bargaining or other mutual aid or protection. This includes a broad array of activity, including discussions about the terms or conditions of employment, including wages, hours and workplace conditions. State privacy laws also may be implicated where an employer invades an employee's reasonable expectation of privacy. In an increasing number of states (not Massachusetts), state statutes further protect employees from being

disciplined for lawful off-duty activities (such as posting a video of their workplace to YouTube or commenting about a customer on Twitter). An employer taking action against an employee for such activities could create liability.

In addition to the legal limits on what actions an employer may take in the face of inappropriate social networking, there are other non-legal risks for employers to consider. Employers do not want to draw greater attention to an unfavorable post on a social media site, nor do they want to cause the same individual or others to post even more commentary. Companies also do not want to create a perception that they are unfair to employees or that they are turning into "Big Brother."

It is lawful and appropriate, however, for employers to regulate or prohibit their employees from using online social networking and blogging sites while on company time, property or business. Employees of private employers do not have a constitutional "free speech" right to disparage their employers, coworkers, customers or competitors. Employees of private employers also do not have a constitutional right to discuss their employer's internal business matters online. An increasing number of employers are attempting to limit employees' ability to post disparaging remarks about the company through carefully crafted policies that make it clear that such conduct is prohibited and may result in disciplinary action.

IMPLEMENTING AN EFFECTIVE ELECTRONIC COMMUNICATIONS AND SOCIAL NETWORKING/ BLOGGING POLICY

Employers should adopt a carefully crafted electronic communications, social networking and blogging policy. Such a policy should aim to protect the confidentiality of company information, prohibit any type of employment discrimination or harassment, and regulate the use of the company's communication and computer systems.

In order to minimize the exposure for potential invasion of privacy claims, employers should make clear that all company-issued equipment and data belong to the company, and that email and internet usage will be monitored. The policy should state that employees have no expectation of privacy in their emails and online communications made through company computers and other systems.

It is lawful and appropriate for employers to regulate or prohibit their employees from using online social networking and blogging sites while on company time, property or business.

Employers may want to prohibit altogether any non-work-related blogging or social networking during work hours. At a minimum, the policy should specify what activities are permitted during work hours and on company systems, by whom, and what time limits apply.

When employees engage in blogging and social networking on their personal time and with their own equipment, it becomes more difficult to monitor or control activities that create risk for the employer. A social networking policy should encourage employees to use common sense and sufficient privacy measures when using social networking and other Web 2.0 sites.

Employers should stress that all company policies apply equally to Web 2.0 communications, including anti-discrimination and anti-harassment policies, confidentiality and trade secret policies, and securities and other legal/regulatory policies. The policy should also make clear that the company may access at any time without prior notice any information created, transmitted, downloaded, exchanged or discussed on social networking sites or blogs. The policy should further prohibit employees from disclosing confidential or proprietary information, including but not limited to trade secrets and other copyrighted material.

In order to distance the company from employees' personal use of social media, an effective policy should prohibit employees from using—without specific authorization—the name, trademarks, logos, and other identifying graphics or copyright-protected material of the employer or its customers. Employers should also discourage employees from listing their company email address on their personal profiles unless the site is used purely for company business or professional purposes. The

policy should make clear that employees who choose to engage in social networking must refrain from posting material that is discriminatory, harassing or defamatory, or that reflects or may reflect negatively on the company or its interests. If such communications adversely affect work relationships in any manner, the policy should explain that the employee may be subject to discipline, up to and including termination.

A social networking and blogging policy should further require employees who identify themselves as an employee of the company to make clear in any online communications concerning work-related matters that their views and opinions are their own and that they do not represent the views of the company. The policy should state that any employee who self-identifies as a company employee in a social media setting is presenting himself or herself as a representative of the company, and should comport themselves according to the company's professional standards of conduct.

With respect to managers and supervisors, employers can regulate their online conduct more aggressively because they are company representatives. At a minimum, managers should understand that they should not make any statements to their co-workers online that they would not make in the workplace, and that postings made on these sites could lead to a harassment or discrimination claim even if the comment was posted to a "personal" page.

Employees should be required to sign an acknowledgment that they have received the policy, and employers should provide training, monitor compliance and enforce these policies consistently.

EMPLOYER'S USE OF SOCIAL NETWORKING AND BLOGGING SITES AS A BUSINESS TOOL

Screening job candidates. Many companies have decided to follow the old adage, "If you can't beat them, join them," and have dipped their corporate toes into the social networking or blogging waters. Employers have begun screening or "mining" job applicants by obtaining information from searches of social networking and blogging sites, including industry-specific blogs, discussion forums, and newsgroups. These sources, such as a candidate's Facebook or LinkedIn profile, can provide clues to a job candidate's analytical skills, communication skills and style, tact, personality traits, interests, and general maturity level. These sites can also provide insight into how others feel about the candidate. Obtaining such thorough information may even help an employer avoid a claim for negligent hiring.

If an employer is going to use Web 2.0 resources to screen applicants, it should develop guidelines for human resources personnel to follow concerning what type of information will be sought and how it should relate to the qualifications for the position.

Employers, however, need to be careful when using such screening measures. Before using social media to vet job applicants, employers should consider the varying definitions of "applicant" and "application" and the resulting statutory recordkeeping requirements that may apply to records produced during such searches. Employers also should consider restrictions on background checks and the use of information obtained from them. Searching these sites often reveals "protected" information about an applicant (age, religion, sexual orientation, marital status, etc.), which can give rise to a potential failure to hire claim.

If an employer is going to use Web 2.0 resources to screen applicants, it should develop guidelines for human resources personnel to follow concerning what type of information will be sought and how it should relate to the qualifications for the position. Companies should develop protocols identifying what Internet resources will be used and how the information will be verified. Company representatives should run searches consistently as to all candidates for a given position, regardless of protected class status. In order to minimize exposure for discrimination liability, non-decision-making personnel should conduct the search and filter out information related to protected characteristics before passing the information along to the hiring manager. Employers can avoid potential issues under the Fair Credit Reporting Act by running the searches themselves rather than using a third party vendor, but must also be aware of state statutes restricting the use of arrest and/or conviction records, as well as information appearing on sex offender registries.

If the search results are adverse or damaging to the candidate, employers should advise the candidate of those results and provide the candidate an opportunity to respond to and/or correct the information. If search results are used to disqualify a candidate, the company should record what results were used and why they were disqualifying. Employers should retain search results consistent with their customary record retention protocols.

EMPLOYER-SPONSORED BLOGS AND SOCIAL NETWORKS

A growing number of employers have begun their own blogs or social networking fan groups. Where the decision has been made to use social networks and/or blogging sites for business purposes, employers should establish clear policies to control the content that employees may post on these sites. The company will then need to monitor and control that content.

In sum, Web 2.0 presents a brave new world for employers, offering an array of benefits, but also a bevy of legal risks for the wary. Employers should devote proper attention and resources to decide how best to enter this new frontier while at the same time balancing the risks. Well-crafted policies and protocols can go a long way toward minimizing potential liabilities. Employers would be wise to consult with legal counsel during this process. ■

Daniel B. Klein, Esq., is a partner with Seyfarth Shaw, LLP, and NEHRA's legal advisor. Contact Dan at dklein@seyfarth.com. Dan's colleague, Dana L. Fleming, Esq., is an Associate with Seyfarth Shaw, LLP. Contact Dana at dfleming@seyfarth.com.