

For The Defense

DRI™

The magazine
for defense,
insurance and
corporate counsel

March 2010

Employment Law

- **Employing Members of the Armed Forces**
- **ADEA Litigation After *Gross***
- **Title VII's Opposition Clause Under *Crawford***
- **And more!**

page 26

ALSO

**Keeping Your Financial Damages
Expert in the Case** page 12

**Chinese Drywall Claims: Will
Contractors Be Covered?** page 18

Potential Pitfalls

By Michael J. Newman
and Faith C. Isenhath

Counsel must help employers recognize the legal issues that may arise when taking advantage of these useful tools.

Social Networking in the Workplace

In the past few years, there has been an explosion in the popularity of online social networking websites. While these sites can present a tremendous opportunity for employers, they can also present a series of legal pitfalls.

It is important for employers to understand the benefits of these useful tools, for instance, for recruiting, and also the disadvantages, such as loss of productivity, along with the legal issues that can arise with using these online tools. The article provides an overview of some commonly used social networking sites and their functions and discusses the potential legal issues that employers face when using these tools in the workplace to help counsel assist employers in drafting effective social networking policies.

Common Social Networking Sites

Facebook (www.facebook.com) is a social networking website where users can add friends, send messages to them, and update their profiles to notify friends about themselves. Users have the ability to join networks organized by city, workplace, school, and region, as well as groups for common interests. This social networking website was initially launched in 2004 by Harvard undergraduates, and it quickly

spread worldwide. Facebook currently has over 300 million active users. Notably, its usage is no longer unique to the young; use by the 35–49 year-old age group experienced the largest growth on Facebook last year, increasing by 24.1 million users from the previous year. See Facebook Factsheet, <http://www.facebook.com/press/info.php?factsheet>; see also *Global Faces and Networked Places: A Nielson Report on Social Networking's New Global Footprint* (2009) (Nielson Report), available at <http://scribd.com/doc/13112459/Global-Faces-And-Networked-Places-A-Nielson-Report-On-Social-Net-Workings-New-Global-Footprint>.

Myspace (www.myspace.com) is one of the world's largest online, social networks, with over 125 million users. Myspace is considered a music network, connecting millions of bands with millions of music lovers. Myspace is similar to Facebook. Its users can add friends, send them messages, and comment on their profiles. Users can customize their profiles and add music, and several independent websites even



■ Michael J. Newman is a partner with Dinsmore & Shohl LLP in its Cincinnati office, where he chairs the firm's labor and employment appellate practice group. He serves on DRI's Employment Law Committee and its Employers Practice Liability Insurance (EPLI) Subcommittee. Faith C. Isenhath is a labor and employment associate with Dinsmore & Shohl LLP, also in its Cincinnati office.



offer Myspace-customized layout designs for profiles. See Myspace Fact Sheet, <http://www.myspace.com/pressroom?url=/fact+sheet/>.

Twitter (www.twitter.com) is a social networking service that enables its users to send and read messages known as “tweets.” Tweets are posts of up to 140 characters displayed on an author’s profile page and delivered to the author’s subscribers, known as

A discrimination claim

might arise when an employer uses social networking websites to pre-screen candidates.

“followers.” Launched in 2006, Twitter asks one question: “What are you doing?” This service is recognized by celebrities and corporations for its self-promotion capabilities. Twitter grew 1,382 percent between February 2008 and February 2009. A February 2009 *compete.com* blog entry ranked Twitter the third most used social network based on its six million monthly visitors. See About Twitter, <http://twitter.com/about>.

LinkedIn (www.linkedin.com) is a social networking website focused on professional networking. This website allows registered users to maintain a list of contacts of people who they know and trust in business. The people in the list are called “connections,” and users can invite anyone to become a connection. Launched in 2004, LinkedIn currently has over 50 million members in over 200 countries worldwide. See About Us, LinkedIn, <http://press.linkedin.com/>. These connections can help members find jobs, list jobs, and also search for potential candidates, which is a useful resource for employers. *Id.*

In addition to LinkedIn, **MeettheBoss** (www.meettheboss.com) is a business networking tool for business executive around the world. Members of Meettheboss have individual profiles describing business interests. This site features weekly interviews with industry leaders heading large global companies. Discussion groups are set up

with question and answer sessions to provide opportunities for users to make contacts and gain insight from industry leaders. See MeettheBoss, <http://www.meettheboss.com/>. **Plaxo** (www.plaxo.com) is another social networking service and online address book that provides automatic updating of contact information. Users store their information on the servers, and when this information is edited by a user, the changes appear in the address books of all those listed as contacts. In 2008, Plaxo reported 20 million users. See Plaxo, <http://www.plaxo.com/>. **Blogs** are a type of interactive website, usually maintained by an individual, with regular commentary, descriptions of events, or other materials, such as graphics or video. A typical blog combines text, images, and links to other blogs, as well as links to other websites and other media related to the blog’s topic. Blogs also typically provide their readers with the ability to post comments, encouraging interactive dialogue. See *What Are Blogs, RSS Feeds, Podcasts, and Widgets?* TeacherVision, <http://www.teachervision.fen.com/educational-technology/resource/50508.html>.

Employers must have familiarity with these social networking websites, especially their prevalence. According to a Nielson Report, time spent on these social networking sites accounted for one in every 11 minutes spent on the Internet around the world in 2008. *Nielson Report, supra*. Additionally, 35 percent of hiring managers “google” applicants, while 23 percent check social networking sites, and approximately one-third of these searches results in job rejections. Karen Glickstein, *Social Networking and Employment Law*, (Oct. 6, 2008), <http://forthedefense.org/post/Social-Networking-and-Employment-Law.aspx>. Moreover, 79 percent of employees use social networking at work for “business reasons.” Chris Crum, *Is Social Media Good or Bad for Business?*, WebProNews (Oct. 28, 2008), <http://www.webpronews.com/topnews/2008/10/27/is-social-media-good-or-bad-for-business>.

These social networking tools are great marketing and advertising resources for employers. Additionally, social networking tools provide helpful resources for recruiting. Social networking websites can provide insight into whether a candidate will fit into a company’s culture. A list of justifications for screening applicants through

these tools is extensive, and the number of employers that take advantage of them continues to grow. Even the Obama administration required that candidates seeking positions in the administration disclose potentially damaging or embarrassing e-mails, blog postings, and text messages that they had produced, as well as provide links to their social networking sites so that the administration could inspect them. Jackie Calmes, *For a Washington Job, Be Prepared to Tell All*, *New York Times* (Nov. 12, 2008), available at <http://www.nytimes.com/2008/11/13/us/politics/13apply.html>.

A recent story reported on MSNBC.com provides a real world example of social networking in recruitment. The story concerned a corporate recruiter charged with hiring physicians. The recruiter would log into Facebook to view a candidate. In one particular incident, the recruiter found pictures of a candidate taking off her shirt at parties and called the candidate to request an explanation. Unimpressed, he did not offer the position to her, stating, “[H]ospitals want doctors with great skills to provide great services to communities. They also don’t want patients to say to each other, ‘Heard about Dr. Jones? You’ve got to see those pictures.’” Glickstein, *supra*.

Legal Issues That Arise with Social Networking Websites in the Workplace

Along with benefits, there are disadvantages to using social networking websites in the workplace. For one, productivity decreases due to the time that employees spend on these sites. As noted above, legal issues can arise when a business decides to use social networking websites in the workplace. Chiefly, employers must understand discrimination, privacy, confidentiality, and privilege issues.

For instance, a discrimination claim might arise when an employer uses social networking websites to pre-screen candidates. In pre-screening an applicant’s Facebook or Myspace page an employer might become aware of a candidate’s race, religion, gender, sexual preference, age, nationality, marital status, or disability. Through searching these sites, employers might obtain information about applicants that they otherwise would not have known by simply interviewing applicants—as well

as information that they cannot legally seek or use in hiring decisions. The issue then becomes proving that this information was not the basis for an employer's decision not to hire a candidate. This pre-screening issue potentially implicates a number of federal employment statutes, including the Americans with Disabilities Act (ADA), Title VII of the Civil Rights Act of 1964 (Title VII), the Age Discrimination in Employment Act (ADEA), and the Uniformed Services Employment and Reemployment Rights Act (USERRA), among other statutes that provide protection for employees and applicants.

Another issue that arises with social networking in the workplace is privacy. Employers must beware of invading employees' privacy through monitoring their use of these sites. Employees have privacy interests in information if they have taken reasonable efforts to keep information private and if they derive economic, personal, emotional, or other value from keeping the information private. An employer infringes upon employee privacy if the employee's interest in keeping the information private from an employer outweighs the employer's interest in obtaining the information, and the employer nevertheless requires that the employee provide the information to the employer. Restatement of Privacy §7.03 Privacy Interests in Content Information.

As mentioned, an employee must take reasonable efforts to keep the information private. If an employee has not restricted access to information, then the employee did not take reasonable steps to keep the information private from an employer. For example, if an employee has a webpage that is accessible and open to Internet users indiscriminately where he or she posts personal pictures and information, that employee has not taken reasonable steps to keep the information private. In contrast, if an employee has a personal webpage that is accessible only to those who enter a proper username and a password, and the employee only provides passwords to his or her friends and family, then the employee has taken reasonable steps to keep the information private. Therefore, in the second example, the employee has a privacy interest in the information on his or her webpage. Employers should know

about the particular common law privacy torts in their specific jurisdiction.

Along with common law privacy, the Stored Communications Act (SCA) also comes into play with employees' use of social networking sites. The SCA is a federal statute that prohibits third parties from accessing electronically stored communications—for example, e-mail or Facebook entries—without proper authorization. 18 U.S.C. §2701.

Under the SCA, an offense is committed by anyone who: "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided"; or "(2) intentionally exceeds an authorization to access that facility; and thereby obtains... [an] electronic communication while it is in electronic storage in such system." *Id.* The definitions in the Electronic Communications Protection Act (ECPA), known as the Wiretap Act, apply to the SCA, and "electronic storage" is defined as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. §2510(17), 2711(1). The SCA aims to prevent hackers from obtaining, altering, or destroying stored electronic communications. *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

Konop v. Hawaiian Airlines, Inc., provides an example of the applicability of this statute to this issue. *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002). *Konop*, a case from the United States Court of Appeals for the Ninth Circuit, concerned the denial of summary judgment to an employer on the employee's SCA claim. *Id.* In *Konop*, an airline pilot sued his employer, alleging that the airline viewed the pilot's secured website in violation of the SCA. The pilot maintained a website, in which he criticized the airline, the airline's officers, and the union. Certain eligible airline employees could access the site by logging in with a username and password created by the individual employees. They were deemed eligible according to a list of names maintained by the pilot; however, the pilot expressly excluded management employees. *Id.* at 872-73. The vice

president of the airline was concerned that the pilot was making untruthful allegations on the website, so he asked an eligible employee to assist him in accessing the website. Upset by the pilot's accusations on the website, the vice president contacted the union about the website. *Id.*

The court first dismissed the pilot's claim under the ECPA, or Wiretap Act,

Employers must beware
of invading employees'
privacy through monitoring
their use of these sites.

because the vice president's act of logging into the site did not constitute an "interception" of an electronic communication and was, therefore, not prohibited by the ECPA. *Id.* at 879. Regarding the pilot's SCA claim, the court found that it raised questions about whether the eligible employee constituted a "user" of the website—in other words, whether the eligible employee had the power to "authorize" the vice president, a third party, to access the website. However, the court noted that if that employee had that power, the vice president would have been authorized to access the website, and as such, exempt from liability under the SCA. *Konop*, 302 F.3d at 880; see also *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*, No. 06-5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. 2008) (upholding a jury verdict with punitive damages in which the company was held liable under the SCA for intentionally accessing a chat group on an employee's Myspace account without having received authorization from the Myspace member to join the group).

In addition to the SCA, employers also need to recognize potential issues under the National Labor Relations Act (NLRA). 29 U.S.C. §157. An employer monitoring employees' social networking sites may have a chilling effect on employees' communications regarding the terms and conditions of their employment. In *Endicott Interconnect Technologies, Inc.*, the National Labor Relations Board (NLRB)

found an employee's posting on a public-forum website—in favor of union representation at the company and criticizing recent management of the company—was protected conduct under the NLRA. The company was found to have violated 8(a)(1) by threatening, and then discharging, the employee for his statements on the website. 345 N.L.R.B. No. 28 (Aug. 27, 2005).

An effective social networking policy should establish guidelines about whether employees can use social networking sites during working hours.

In a similar case, the NLRB held that the company's policy prohibiting employee use of the company e-mail system for "non job-related solicitations" did not violate Section 8(a)(1) of the NLRA. In *The Guard Publishing Company d/b/a The Register-Guard*, the company implemented a policy that employees could not use company communications systems, including e-mail, for non-job-related solicitations. 351 N.L.R.B. No. 70 (Dec. 16, 2007). The company was aware that employees sent personal e-mails, such as baby announcements, party invitations, and sports tickets, but had no evidence that the employees used the e-mail system to solicit support for outside causes or organizations, other than the annual United Way fundraiser. An employee received two written warnings for sending e-mails to colleagues at their company soliciting union support.

The union filed a charge alleging that the company violated Section 8(a)(1) by maintaining its policy and discriminatorily applying it against union-related e-mails. The NLRB compared e-mail systems to other types of employer-owned property—such as bulletin boards, telephones, and televisions—and found that employees had no statutory right to use an employer's equipment or media, as long as the restrictions

were not discriminatory. The NLRB also found that the employee's e-mails soliciting union support differed from the occasional e-mails about baby announcements, in that they supported an outside group or organization. Ultimately, the NLRB found that employees had no statutory right to use the company e-mail system for Section 7 purposes under the NLRA, which gives employees the right to form, join, or assist labor organizations, and other concerted activities for other mutual aid or protection. 351 N.L.R.B. No. 70 (Dec. 16, 2007).

Finally, some courts have found that employers violate state professional conduct ethics rules by retaining and using e-mails protected under the attorney-client privilege doctrine. Sean Carnathan, *Attorney-client Privilege Trumps Workplace Regulations*, *Litigation News* (ABA Section of Litigation Sept. 2009), http://www.abanet.org/litigation/litigationnews/top_stories/attorney-client-computer-stengart.html. For example, in *Nat'l Econ. Research Assoc. v. Evans*, a Massachusetts Superior Court ruled that an employee did not waive the attorney-client privilege for personal e-mails sent to his attorney and later accessed by his employer. *Nat'l Econ. Research Assoc. v. Evans*, No. 04-2618-BLS2, 2006 Mass. Super. LEXIS 371 (Mass. Super. 2006). Many of these e-mails were sent through the employee's work computer using his personal e-mail account, not his company account. The court held that the employee did not waive the attorney-client privilege because he did not use the company intranet or e-mail, and he did not forward the communications to his company intranet or save them in a file on his company laptop. Therefore, the court found that the employee took adequate steps to protect the confidentiality of his privileged communications and denied the company's motion to compel disclosure of attorney-client communications between a past employee and his attorney. *Id.* at *11. The law on this issue depends on an employer's specific jurisdiction. However, the lesson for employers is to have a properly drafted e-mail policy that is clearly disseminated to employees and updated as appropriate. Carnathan, *supra*.

Creating a Social Networking Policy

In light of the potential legal issues, employers should develop a social network-

ing policy if they intend to use this media. An employer must consider the goals of this type of policy, which, include protecting a company's

- Trade secrets and confidential, proprietary, and privileged information
- Reputation; and
- The privacy of employees.

Additionally, an effective social networking policy should establish guidelines about whether employees can use social networking sites during working hours, and if so, under what circumstances.

Employers must also consider the elements of a social networking policy. An effective social networking policy will:

- Urge employees to go to Human Resources with work-related issues and complaints before blogging about them;
- Set forth potential discipline, up to and including termination, if an employee misuses social networking sites relating to employment;
- Establish a reporting procedure for suspected violations of the policy; reiterate that the company's policies, including harassment and discrimination policies, apply with equal force to employees' communications on social networking sites;
- Remind employees that the company's computers and e-mail system are company property intended for business use only, and that the company may monitor computer and e-mail usage;
- Require employees to sign a written acknowledgment that they have read, understand, and will abide by the policy; and
- Enforce this policy consistently and indiscriminately employees.

These guidelines should permit counsel to help employers develop a new policy that will cover these social networking tools. Both counsel and employers will want to remember that certain businesses raise additional business-specific issues.

Conclusion

Employers should embrace these social networking websites for their useful resources. Counsel must help employers recognize the legal issues that arise when taking advantage of these resources. Technology will continue to develop, as will the law regarding its use in the workplace. **FD**