We live in a world dominated by the Internet, and increasingly, social networking sites like Facebook, MySpace, LinkedIn and Twitter. According to its most recently published statistics, Facebook now has over 400 million active users, half of whom sign on daily to check their accounts. These users include many employees who communicate with Facebook “friends” and Twitter “followers” (and likely work colleagues) while sitting in their office, from their mobile devices while on the road, and from their homes. Now more than ever, employers, too, find themselves turning to these online resources as a tool to disseminate corporate information, attract and evaluate candidates for employment, and, in some instances, monitor employees’ behavior.

These actions are not without risk. Employees must be mindful of the significant dangers posed by accessing and participating in social networking sites. When used to engage in inappropriate conduct toward co-workers or reveal the company’s private and confidential information, employees may be to discipline and even legal liability. Likewise, employers must ensure they do not use these technologies in ways that unintentionally create exposure under state and federal laws.

As the law struggles to keep pace with the world of online social networking, and the potential legal issues it presents, employers face difficult questions about how to appropriately use the information available on the Internet, and to what extent they may regulate potentially damaging employee activity.

Social Networking Activities: The Risks

Few employers would have envisioned a few years ago that they would need to concern themselves with employees’ social networking activities. Now, however, employees may “friend” co-workers on Facebook and use the Internet to “tweet” the company’s confidential information to outsiders. Employers must be prepared to address these situations.

Disclosure of Confidential Information

For better or worse, social networking sites provide a platform for the instantaneous dissemination of information around the globe. Employees can easily reveal a company’s (or its client’s) confidential and proprietary information with the simple click of a mouse button.

Jilted ex-employees also may use these tools to release “secrets” to the Internet as way to “get back at” their former employers. Current employees may inadvertently divulge private information. For instance, a careless worker may unintentionally reveal a client’s forthcoming business acquisition by posting the particulars of her most recent “big deal.” For medical employers, the unauthorized release of patient information can result in serious violations of patient confidentiality laws. Recently, a group of San Diego nurses were dismissed from their jobs after posting confidential patient information to their social networking pages.

Discrimination/Harassment

Claims involving federal and state equal employment opportunity laws remain particularly troublesome for employers. Social media sites like Twitter, Facebook and YouTube make “policing” the workforce all the more difficult. Social networking sites effectively “extend the workplace” to create potential liability for conduct occurring over the Internet.

For example, a supervisor who uses social media to engage in lewd “chat” sessions with his subordinates may create liability for himself and his employer. This is true even if the supervisor performs such acts on his home computer, outside of his regular working hours. This is because, generally speaking, anti-harassment laws draw no distinction between acts that occur during official “working” and “non-working” times. Rather, employees may be considered “at work” for purposes of harassment liability whenever and wherever they
interact with their colleagues—whether during the day at the workplace or over the weekend at a co-worker's private wedding.

Even the seemingly benign act of “friending” a co-worker can have unintended implications. Imagine a situation where a supervisor attends a bachelorette party and posts updates about the event on her Facebook “wall.” If the supervisor has “friended” any of her subordinates, the updates could violate the employer’s harassment prevention policy and lead to legal liability.

Similarly, employers who use information found on social networks to make employment decisions may find themselves subject to discrimination claims. Employers commonly search the Internet for information about job applicants. This can include reviewing an applicant’s Facebook and MySpace pages. Those pages may reveal an applicant’s “protected classes,” such as race or marital status. Employers should appreciate that these Internet searches present the same risk as asking questions about an applicant’s religious beliefs or sexual preferences, for instance, during an interview.

Off-color Internet postings by management employees can also cast doubt on otherwise legitimate employment decisions. Assume an employee is fired for repeated tardiness. The employee later sues the employer claiming her termination was motivated not by her chronic tardiness, but by unlawful age discrimination. If the boss previously “tweeted” about the employee’s “lack of energy” as compared with the company’s “younger employees,” the employee can use the “tweets” to show the boss’s unlawful motivation for her termination.

Defamation and Other Tort Liability

Social networking sites likewise provide a vehicle for potential tort liability, including defamation, when employees use online resources to publish false statements about their colleagues. For instance, feuding coworkers may take their dispute to the Internet, engaging in back-and-forth “tweets” of made up, offensive statements about one another. Besides having a negative impact on office morale, employers can, in certain circumstances, be vicariously liable for such postings.

Likewise, employers should be wary of making online comments made about departing employees. An employer may be tempted to post unflattering statements about an employee who announces he is “jumping ship” to work for a competitor. However, if the competitor rescinds the job offer because of the post, the employee may have a claim for defamation, even if the statements are true. Truth is not necessarily a defense to certain tort claims asserting intentional interference with business relations. Particularly offensive comments about current or former employees posted to social media sites can likewise form the basis for another tort—intentional infliction of emotional distress.

Employee Discipline—A Sticky Proposition

Given the potential for liability, to mitigate risk, employers should monitor their employees’ work activities, and take action against those whose use social networking sites in a manner that may create legal problems. As a general matter, employers are well within their rights to discipline employees for using company equipment (computers, smart-phones) as a vehicle to engage in inappropriate conduct towards their colleagues. Likewise, employers may discipline employees who “steal time” by constantly checking their social networking page, posting to a blog, or surfing the Internet during work hours. However, employers may face liability in certain areas.

Employee Monitoring

Federal and state privacy laws limit how far employers may go to monitor their employees’ social networking activities. In weighing employee privacy concerns, courts generally seek to balance the employer’s interest in objecting to the employee’s conduct (i.e., the harm to employer) with the employee’s expectations of privacy. As such, employers can mitigate their risk by disabusing employees of any privacy expectations relating to their jobs. This includes implementing policies that inform employees their work activities may be monitored.

In addition, federal laws such as the Stored Communications Act may provide additional hurdles to monitoring employee’s use of social media. A New Jersey jury recently held an employer liable under the Act where it fired two employees after hacking into their MySpace accounts, and finding postings critical of the organization.

National Labor Relations Act Concerns

Employers also must avoid disciplining employees for activities that could be considered protected “concerted activity” under the National Labor Relations Act (“NLRA”). The NLRA generally protects employees’ rights to talk openly with one another and their employer about the terms and conditions of employment. This
includes engaging in group communications aimed at improving working conditions. Many employers do not realize that these protections apply to all employees, whether or not they belong to a union.

Whistleblower Protections

State and federal “whistleblower” laws safeguard employees’ rights to complain about certain workplace issues, including perceived equal employment opportunity violations and health and safety concerns. So, an employee who complains of a violation of the harassment prevention policy on a company-sponsored Facebook page may be protected from discipline for engaging in this conduct.

Employer Best Practices

Given the risks posed by employees’ use of social networking sites, and the potential pitfalls for employers, employers should take the following steps to minimize their potential liability:

- Educate all employees about the risks of using of social-networking sites. Make sure they understand how even comments made outside of work and on their “own time” can create liability.
- Develop and distribute comprehensive electronic communications policies that address social networking. These policies should be accompanied by appropriately drafted confidentiality and non-disclosure agreements that protect against public dissemination of company and third-party secrets.
- Monitor social media policies and practices to keep pace with changing technology and new legal interpretations.
- Inform employees that they should have no expectation of privacy in their workplace communications.
- Before disciplining employees for their electronic communications, consider the potential legal consequences of such actions. These issues can be tricky, and the potential consequences for missteps significant.

Reprinted by permission of The Daily Recorder.

Jennifer Brown Shaw is a partner at Shaw Valenza LLP. Her practice includes providing regular advice and counsel to private and public sector employers. She also develops and presents seminars on legal issues in the workplace for management and non-supervisory employees.

jshaw@shawvalenza.com