WEB MONITORING ADVICE TO EMPLOYERS—TREAD CAREFULLY

An employer who monitors employees’ personal Web postings on blogs or social networking sites such as Facebook and MySpace might be motivated by the reasonable goals of protecting its reputation or proprietary information; however, an employer that proceeds incautiously could create liability on several fronts, according to attorneys and a consultant who advise companies on social media policies.

The commentators warn that employers monitoring employee Web postings must consider how they attain access to employees’ social media sites; the public or private nature of employees’ Web accounts; whether the information in the postings is protected under federal labor law or reveals employees’ protected status under discrimination laws; and what steps it could take if it were to find defamatory content.

Although some legal issues are unclear, management-side commentators suggest that employers can minimize their potential liability by incorporating references to social media into existing policies on confidentiality and external communications and by making the rules on what employees may and may not post as specific as possible so that the employees are “on notice.”

Lon Safko, a New York-based consultant who advises companies on how best to use social media, says that more employers are developing social media policies that devise ways to protect the company’s reputation or proprietary information and that employers don’t need to develop entirely new policies. Rather, employers should add the language “social media” and “social networking sites” to existing policies, such as those limiting employees’ right to discuss proprietary company information outside of the workplace or those limiting employee contact with reporters. Instead of imposing an outright ban on blogging and social networking, companies should give workers guidelines on what they can and cannot blog about. Employers should have policies recommending that workers bring workplace-related issues and complaints to the attention of human resources departments before blogging about them, according to Safko.

What type of monitoring is permissible may depend on the type of social media involved, according to Lewis Maltby, president of the National Workrights Institute, a worker advocacy organization in Princeton, N.J. “If employees put something on the Internet for all the world to see, then they are taking a chance. That is the risk they took in posting on public sites. Password-protected and nonpublic sites such as [private pages on] Facebook are a different matter. If the employer did something improper such as use spyware to get an employee’s account access; then the employer could get into trouble.”

John “Lou” Michaels Jr., a management attorney and partner with Baker & McKenzie in Chicago, says it is clear that employers can terminate employees for publishing defamatory statements about the company or fellow employees on Web sites, but that they can still face liability if they accessed the defamatory content in an illegal manner.

Robert Lavitt, a partner at Schwerin Campbell Barnard Iglitzerin & Lavitt in Seattle, also urges caution that “Employers need to be very careful about accessing private password-protected social networking sites—and the SCA [Stored Communications Act] adds another layer of concern for employers.” “There may be legitimate reasons why employers might monitor an employee’s blog in order to protect its brand or image. The rub is where employers view working condition complaints as harming its image and try to tamp down on it. This can have a chilling effect on legitimate employee communication about workplace terms and conditions such as salaries and benefits that are protected under Section 7” of the National Labor Relations Act.