

by STACEY DEKALB and BRYAN FELDHAUS

Why employers must address networking sites

LAST YEAR, the city of Bozeman, Montana, implemented a policy that prospective employees must supply the usernames and passwords for any Web sites they belonged to, including Facebook, MySpace, Yahoo, Google and YouTube, so that they could make informed decisions about recruiting, hiring and firing.

When news of the Bozeman background check process was publicized, however, there was tremendous outrage and the city suspended the practice.

In other situations, employers have sought to review text messages sent by and to employees on employer-provided equipment. There has been litigation over whether one's Twitter messages constitute opinion or expose one to claims of libel and defamation.

Employers that engage in such monitoring face pitfalls and must be aware of potential employment claims, including invasion of privacy, and must avoid a public outcry like that in Bozeman.

Today's employers have been slow to adopt policies addressing the use of social networking sites like LinkedIn, Facebook or Twitter. While companies have the right to set such policies, their employees often need guidance about their own privacy expectations when accessing social networking sites through company equipment. Following are some areas to consider:

Legal landscape

Disparate impact and anti-discrimination claims: Businesses that use social networking sites for recruiting and hiring may subject themselves to disparate impact claims under state and federal laws that prohibit workplace harassment and discrimination.

If these sites are used to gain information about job applicants, an employer may be subject to scrutiny if an applicant is denied employment, especially where an applicant believes that employment was denied because the employer obtained information

about the applicant's protected class status such as race, religious affiliation, gender, age, national origin, sexual orientation or the like through personal online media.

Stored Communications Act: The SCA renders it an offense to "intentionally access without authorization a facility through which an electronic communication service is provided" or to "intentionally exceed an authorization to access that facility." This legislation means simply that employers are precluded from using illicit or coercive means to access an employee's private social networking accounts.

National Labor Relations Act: The NLRA protects an employee's right to form, join and assist a labor organization, engage in collective bargaining, and to conduct other concerted activities for mutual aid or protection. A social networking policy that curtails these rights of employees may subject an employer to liability under the NLRA.

Off-duty conduct statutes: A number of states — but not yet Minnesota — have recently enacted social media legislation prohibiting employers from disciplining employees for lawful off-duty conduct away from the employer's premises, unless that conduct creates a material conflict of interest for the employer or is reasonably related to the employee's job.

An employee who is discharged due to social networking posts may also

[tips]

- 1 | Adopting a social networking policy will reduce the idle time your employees spend surfing the Internet and will likely improve your employees' productivity.
- 2 | It may protect your company against unauthorized and/or unfavorable uses of company trademarks, logos, and other intellectual property by employees on social networking sites.
- 3 | It may protect your employees from digital harassment by other employees and may prevent defamatory or unfavorable comments from being made against employers on social networking sites.
- 4 | It may permit an employer to track Internet postings made by employees on social networking sites, whether private or public.

“Companies should strive to define the line where business use — and personal use — of social network sites begins and ends so that employees clearly understand what is private and what is not.”

— Stacey DeKalb and Bryan Feldhaus, Lommen Abdo

have various state law claims, including a claim for invasion of privacy. Under Minnesota law, such a claim requires an employee to establish an intentional interference with his or her private affairs, affairs for which the employee has a reasonable expectation of privacy, and the interference must be done in a manner that would be highly offensive to a reasonable person in a similar situation.

Typically, information on a Web site is not private because the public at large can access it — unless the user controls access by invitation, such as Facebook. If the employee can restrict access to the public, he or she may have a reasonable expectation of privacy and, therefore, claim an invasion of privacy if the employer discharges that employee based on private online communications.

Companies should strive to define the line where business use — and personal use — of social network sites begins and ends so that employees clearly understand what is private and what is not.

There are a number of reasons, outlined in the tips box above, why an employer should consider adopting a social networking policy to prohibit employees from accessing social networking sites during work hours.

A social networking policy may, how-

ever, have the following detrimental effects on your workforce:

- an aggressive policy may decrease employee morale or negatively affect your company culture;
- a policy that affects employment decisions may cause your company negative publicity;
- and a policy may also discourage employees from legitimate uses of social networking sites for professional marketing purposes, especially LinkedIn and other professional sites.

Policy model

An overly broad or unreasonable social networking policy, which prohibits employees from professional networking or creates other detrimental effects, will ultimately harm your company. Accordingly, employers should identify the specific goals of their policy and draft one that will ensure the policy goals are realized. It should include at least the following:

1. Prohibit employees from revealing confidential and/or proprietary information.
2. Prohibit employees from revealing personal information of clients, customers, employees or employers.
3. Prohibit employees from using the logos, trademarks or trade dress of the

employer except with express authorization.

4. Prohibit employees from using social media to violate federal, state or local law.

5. Prohibit employees from using social media for defamatory or discriminatory purposes, whether related to customers, clients, employees or the company.

6. Prohibit employees from engaging in any conduct that creates a conflict of interest or otherwise harms the employer's business interests.

7. Limit the type and extent of social networks at work to professional networking sites to avoid interference with work.

8. State the types of permissible online social networking at the workplace.

9. State that when using an employer's technology, an employee has no expectation of privacy.

10. State that the social networking policy is to be read in accord with any existing employment codes of conduct, disciplinary schemes, or other policies.

11. State that any questions concerning the social networking policy or the conduct permitted by the policy be directed to management.

12. State what disciplinary consequences an employee could face for violating the policy.

Business is becoming increasingly web-centric and adopting prudent legal guidelines about social networking has become a necessity. Today, even the city of Bozeman has its own Facebook page.

[contact]

Stacey DeKalb

(612.336.9310; stacey@lommen.com) is chair of the employment practice at **Lommen**

Abdo law firm in Minneapolis. **Bryan Feldhaus**

(612.336.4389, bryan@lommen.com) is a Lommen Abdo litigator who focuses on areas of professional liability and intellectual property: www.lommen.com

