



Productivity

May/June 2009

Social Networking Sites Pose Risk for Employers

Employers are increasingly turning to Google and social-networking sites such as Facebook and MySpace to conduct background checks on job applicants and employees. A recent survey by Vault of 350 employers found that 44% of employers use social-networking sites to examine the profiles of job candidates and 39% have looked up the profile of a current employee.

Some find this trend surprising and even troubling. But for employers who face liability for negligent hiring, reviewing the information available on social-networking sites and personal blogs is often seen as prudent, and even essential, to ensure they are satisfying their due diligence obligations.

However, use of social-networking technologies to screen applicants and employees poses its own potential legal risks for employers. For example, while most employers have stopped requiring applicants to submit photographs or inquiring about marital status or age to avoid accusations that they rejected a candidate for discriminatory reasons, social-networking profiles make this once off-limits information readily available, thus reopening the potential for liability. And discovering demographic data isn't the only concern for employers. Social-networking profiles also may include information about employees' political affiliations and/or off-duty political activities, factors that public employers and even private employers in several state and local jurisdictions (including the City of Seattle) are prohibited from considering.

Other potential risks include violations of federal and state fair credit reporting laws, the terms of service conditions on commercial social-networking sites, and federal laws governing access to electronic communications. And while using publicly available profiles and blogs to screen applicants and employees may not in most cases constitute a violation of their legal right to privacy, the practice may nevertheless violate "off-duty" conduct statutes.

Fair Credit Reporting Acts

The federal Fair Credit Reporting Act (FCRA) and its state law counterpart, the Washington Fair Credit Reporting Act (WFCRA), require an applicant's or employee's consent before an employer may engage a "consumer reporting agency" to conduct a background check and produce a "consumer report" on that individual. FCRA does not prohibit employers from receiving or using a consumer report that contains information derived from social-networking

sites or blogs, but it does require them to disclose to the individual that such information was the basis for an adverse employment decision.

Recent amendments to WFCRA, on the other hand, restrict the scope of employers' background checks to information that is reasonably related to the applicant's or employee's job duties. Accordingly, under WFCRA, an employer may not obtain or use information from an applicant's or employee's Facebook site or blog unless the information is reasonably related to work that the applicant or employee would be performing.

Discrimination

Employers who conduct their own background investigations using online social-networking sites and blogs are at potential risk of discrimination claims when they obtain information about non-obvious characteristics that are protected under non-discrimination laws. An applicant's or employee's MySpace page or blog, for example, might disclose that he or she suffers from a physical or mental condition (potentially protected under the Americans With Disabilities Act), is a gay man or a lesbian (sexual orientation is protected under Washington law) or is a member of the Green Party (political affiliation is protected under the Seattle Municipal Code).

Such disclosures provide disappointed applicants and employees with a basis for alleging that an employer's decision not to offer them a job or promotion was due to a protected characteristic. An employer's admission that it examined an applicant's or employee's social-network profile or blog prior to taking an adverse employment action thus makes it easier to ensnare the employer in costly and time-consuming litigation, while also making it more difficult to defend against discrimination claims. A successful defense requires that an employer "unring the bell" and prove that it didn't use the information it found as part of the adverse employment decision.

A related issue is whether the employer is treating all applicants and employees in a similar fashion. Employers that perform Internet searches on a hit-or-miss basis, with no written policy or standard approach, expose themselves to potential liability for unlawful discrimination if they use the results of such searches as a basis for taking an adverse action against applicants or employees.

Privacy

Some argue that social-networking pages are "private areas," like an applicant's or employee's home, where employers may not go without permission. However, establishing an invasion of privacy claim (or, as to public employers, a constitutional claim for unreasonable search and seizure) can be problematic for applicants and employees because of the difficulty in demonstrating they had a "reasonable expectation" of privacy. After all, how reasonable is their privacy expectation if thousands of people can access their MySpace page?

On the other hand, an employer may be subject to potential liability for invasion of privacy if: 1) the applicant or employee reasonably believes that the website is private, i.e., has instituted privacy controls; 2) the site promotes itself as private; and 3) in particular, the company used nefarious means, i.e., "pretexting," to gain access to the site.

Irrespective of an individual's reasonable privacy expectation in a website or blog, employers who use such resources to conduct background checks are subject to another source of potential liability. Some states, not including Washington, have established restrictions on an employer's ability to use lawful "off duty" behavior for employment decisions.

Employers in these states may thus be precluded from making use of an individual's off-duty social-networking site or blog in a hiring or promotion decision. Courts have afforded employers broader discretion — it is worth noting — where such behavior was shown to have damaged a company, hurt business interests or be inconsistent with business needs.

Pretexting

As noted, an employer would be flirting with particular trouble if it obtained information by manipulating social-networking sites. This could be done by creating multiple identities or by using "pretexting," which can include pretending to be someone else or another entity. Such conduct would not only constitute a potential violation of the "terms of use" conditions commonly established by commercial social-networking sites, but may subject an employer to liability under federal law, including the Stored Communications Act, which protects the privacy of stored Internet communications.

In light of these potential risks and pitfalls, employers should initially consider whether the benefits of information derived from social-networking sites and blogs are worth the potential liability. Employers that decide to make use of online information should exercise a high degree of discretion in determining what and how such information should be collected and considered before using it as a basis for employment decisions.

Excerpt from the King County Bar Association, www.kcba.org. Authors Vickie Wallen and Brian Flock practice labor and employment law at Perkins Coie, LLP. All rights reserved. This content is copyrighted and may be reproduced in any form including digital and print for any non-commercial purpose so long as this notice remains visible and attached hereto.