MILLER CANFIELD

Reviewing an Applicant's Social Media Site: Legal Right or Picking a Fight?

May 11, 2012

Gathering information from social media to use in the hiring process can help employers weed out potential problem employees, as well as reinforce a good applicant's potential for success. Recent studies suggest that nearly 70% of employers have rejected candidates based upon information found online. Such a practice, however, is not risk-free.

There are risks in checking and in not checking.

Social media often provides information that is not provided during the "traditional" application process, including allowing visitors to determine certain demographic statuses protected by local, state, and federal law. Consider an employer that learns an applicant is pregnant via her Facebook page after an interview where she was not "showing." Knowing that she is pregnant is not illegal, but by utilizing social media, the employer has likely lost any "lack of notice" argument it might have had but for a search of her Facebook page.

This does not mean, however, that employers should never review applicants' social media sites. It is not yet known whether employers have an *affirmative* obligation to review such sites. Recently, one Colorado court considered a plaintiff's argument that the employer should have reviewed social media as part of its background check process, and had it done so, it would have discovered the employee's checkered past and was therefore liable under the theory of negligent hiring. Though the court rejected such an argument, it is likely that similar suits will follow.

But the profile is private…

Garnering significant national attention recently, some employers have even taken the controversial step of requiring applicants to provide login and password information during the application process. Such practices, privacy advocates argue, violate common law and statutory privacy rights (and for public employees, constitutional rights). Facebook believes that requiring the login and password disclosure could not only "potentially expose the employer who seeks . . . access to unanticipated legal liability," it also is "a violation of Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password."

These practices have also attracted attention from Congress – two Senators recently asked the Department of Justice and EEOC to investigate whether such practices violate federal law and a bill is currently pending before the House of Representatives that would prohibit employers and educational institutions from gaining access to private email and social networking accounts – down to state legislatures. In April 2012, Maryland became the first state to pass legislation prohibiting employers from either requesting or requiring that an applicant or employee disclose a user name or password to the employer. The legislation also prevents employers from taking action against applicants or employees who refuse to disclose information. Exceptions to the legislation are limited to employers conducting investigations regarding securities or financial law and regulations and unauthorized downloading of the employer's proprietary information or financial data.

Several other states are also considering legislation governing such practices, including Michigan. Michigan's bill, for example, is broader than Maryland's law in many aspects: It would prohibit both employers *and* educational institutions from requesting access to the social networking accounts of applicants, employees, students, and prospective students. It also does not include any exceptions, including those for investigatory purposes.

Continued

Given the dearth of guidance on this issue, employers should tread carefully in this area and consider the business consequences of such practices. From a business perspective, while reviewing or requiring access to "private" social media sites might be justified by a legitimate business reason, it might also be viewed as "snooping" and could limit an applicant pool or lead to decreased employee morale if employees thought big brother was watching all the time.

Best Practices

· Define a process for why and how to evaluate an applicant's online presence. Account for such things as accuracy of information presented, verifiability, and how the information is obtained.

· Consider designating a neutral party, instead of the decision maker, to conduct the search and filter out protected status information. Note that retaining third-party vendors to review information likely triggers the procedural and notice requirements of the Fair Credit Reporting Act.

· Maintain a record of *how* information was gathered via the Internet or social media and *what* information was gathered.

· Train employees responsible for implementing this process.

Contact

David King
kingd@millercanfield.com

Adam S. Forman
forman@millercanfield.com