

Facebook in the Hiring Process

Risks and Rewards of Checking Social Networking Sites

February 25, 2010

Social networking sites, like Facebook and LinkedIn, are attempting new means for employers to conduct background checks on job applicants. At little or no charge, employers can quickly check applicant information and assess the applicant's judgment and discretion. Information from social networking sites can help the employer make good hiring decisions, avoid workplace violence, embezzlement, and fraud, and prevent negligent hiring claims.

But there is risk as well as reward in accessing social networking sites during the hiring process: the risk of getting false information and the risk of learning too much facts that an employer cannot legally consider in a hiring decision. An employer with access to those facts will have a harder time defending discrimination-in-hiring claims later.

If an employer decides to access social networking sites despite the risk, it should do so openly, not log on as someone else. "Pretexting" only exposes an employer to added risk and liability.

Lies, Damned Lies, and LinkedIn

An employer may use social networking sites such as LinkedIn to verify a job applicant's education, qualifications, job history and other information.

Doing so is risky, however. The information on LinkedIn may be just as false as a job application and resume. LinkedIn postings and reviews may be made by

friends or confederates, not prior managers or supervisors. Inaccurate information may be posted by anyone. No third-party verifies the entries. Other social networking sites operate the same way.

Knowing More than You Should

Another risk employers run in checking social networking sites is learning too much about job applicants. From text and pictures on a typical Facebook page, an employer can often deduce a job applicant's race, ethnicity, age, sex, marital status, and often religious affiliation and sexual preference.

This information cannot legally be used in reaching an employment decision. So employment applications usually avoid eliciting it. An employer that does not know the job applicant's ethnicity, for example, may more easily defend any claim it discriminated on that ground.

Accessing social-networking sites defeats this purpose because it exposes the employer to knowledge of facts it cannot legally use in choosing whom to hire. Looking at the job applicant's Facebook page is like using an employment application that asks the applicant to state his or her race, age and sexual orientation.

A rejected applicant may easily allege the employer discriminated against him or her based on facts, such as race or sexual orientation, that the employer learned from accessing the applicant's social networking site. It is much more difficult

for the employer to disprove that claim once it has viewed the site.

The applicant's claim is more likely to survive until trial based on an inference of discrimination arising from access to information about protected personal characteristics.

At trial, the jury is likely to presume the employer gained knowledge of facts that might be read or deduced from an accessed site. It may be hard to convince a jury that the employer ignored those facts in making an employment decision.

Pretending To Be Someone Else

An employer that decides to access social networking sites despite the risks should do so openly. Pretending to be someone else by using another company's name or other user's identity when logging onto a site will not shield the employer from the risks of false information or too much knowledge. Doing so will only make the employer less believable when it counts.

Worse, by "pretexting," the employer will likely breach site's terms of use conditions and risk liability for violating federal law, including the Stored Communications Act, which protects the privacy of stored Internet communications.

Sticking to the Tried and True

There is good reason for an employer to use only the traditional resources in conducting background checks on job applicants. Credit reporting agencies and investigative consumer reporting agencies are regulated by state and federal law.

Reputable, experienced agencies know how to comply with these laws but still obtain needed information. These

agencies are more likely to test the accuracy of information they provide and to avoid providing data the employer cannot lawfully use in reaching employment decisions.

If you have any questions about accessing social networking sites before, during and after employment, please direct them to Rhonda L. Nelson 415-677-5502, rln@severson.com or Danielle M. Ellis at 415-677-5504, dme@severson.com