



# Sharing Passwords With @MyBoss

Insights

5.01.12

(Labor Letter, May 2012)

Maryland has become the first state in the country to ban companies from asking employees and applicants for their social media passwords. The bill, which makes the practice entirely illegal, easily passed both houses of the legislature and is awaiting signature by Gov. Martin O'Malley. It will become effective October 1, 2012. Similar bills are being discussed in other states, including California, Illinois, New Jersey, New York, and Washington. In addition, U.S. Senators Charles Schumer (D-NY) and Richard Blumenthal (D-CT) have announced that they will seek investigations of the practice from the Justice Department and the U.S. Equal Employment Opportunity Commission (EEOC).

## Asking For Passwords Is Risky

Though it has received media and political attention, the practice of asking for employee passwords appears to be rare. Examples in news reports cite applicants for municipal jobs such as positions with police departments, where employee vetting is necessarily more stringent. No large, private company has been accused of the practice.

Still, Facebook Chief Privacy Officer Erin Egan reported in March that the site had experienced "a distressing increase in reports of employers or others seeking to gain inappropriate access to people's Facebook profiles or private information." Egan decried the practice because it was not the "right thing to do."

Most employers instinctively shy away from requesting personal passwords, with good reason. As an initial matter, it could create bad press and ill will for the company. As mentioned above, several states are in the process of creating laws to ban the practice and so such a policy, while lawful now, may soon become illegal. Furthermore, it is likely the EEOC will issue guidance that disfavors it. In addition, such policies may violate the federal Stored Communications Act, at least to the extent that a court would consider requiring employees to provide their passwords involuntarily. Finally, password sharing violates the terms of service of Facebook and other social media sites.

## Online Searches Are Less Risky

While asking for passwords is rare and risky, the practice of searching for employees on the Internet is commonplace. In fact, a Microsoft-sponsored survey from late 2009 found that 75% of managers were *required* to research candidates online before hiring.

In many ways, searching for applicants and employees online makes sense. A company should know if an employee has held something out to the public that would reflect poorly on its business. Online conduct can be indicative of poor judgment. In the extreme, a search could reveal that an applicant has committed a crime that makes his or her presence a danger to other employees. In that case, the failure to perform an online search could (theoretically) constitute negligent hiring.

But any use of online searches to vet or monitor employees is also risky. The biggest issue with online monitoring is that you could become aware of an employee's protected characteristic, subjecting your company to liability under Title VII. It is illegal under federal law for employers to ask candidates about their nationality, religion, age, race, sex, or disability during the interview process. Many states add still more protected categories.

While some of these characteristics will be apparent, others will not. To the extent that you are unaware of a protected characteristic, you cannot discriminate based on it. But as soon as the company runs an online search and discovers that an employee practices a certain religion or has a disability, it has opened itself to charges of discrimination under Title VII.

Moreover, the practice of online monitoring could suggest a company knew of a protected trait even where it didn't. Imagine, for example, that a company that requests employee passwords or regularly searches social media websites terminates an employee. The company is unaware that she is pregnant, but she has announced the news with a sonogram picture on Facebook. The act of online monitoring has put the company at risk for a claim of wrongful termination that will be harder to disprove.

### **The Bottom Line**

In light of these issues, newly-improved privacy options on social media sites are actually beneficial for employers. The fact is that employers are *allowed* to gather job-related information about applicants and employees. Beyond that, access to additional information creates liability.

Where information is readily available, an employer could face liability for ignoring it (such as negligence claims) or accessing it (such as discrimination claims). It is likely that your best course is to maintain a policy against online monitoring and hire a third-party firm to run background checks (in compliance with state laws) to avoid negligent hiring claims.. If you decide to monitor candidates or employees online, it's advisable to limit such searches to information readily available to the public at large.

*For more information contact the author at [tgeorge@laborlawyers.com](mailto:tgeorge@laborlawyers.com) or (504) 522-3303.*