GONZALEZ SAGGIO HARLAN

THE GSH 60 SECOND MEMO™

SPONSORED BY THE GSH EMPLOYMENT GROUP

August 29, 2012

Jerilyn Jacobs, Esq.

Questions on this topic? CLICK HERE

What's Your Password? Pending Password Protection Provisions

By Jerilyn Jacobs

When it comes to Facebook, if there is anything scarier than the thought of your grandparents joining and creating an account, it may be the idea that some employers reportedly have been asking job applicants for their Facebook and other social media passwords.

To understand how an employer might even get such an idea, one can look to the brief history of employer use of the Internet to screen applicants. One of the first (and continued) uses of the Internet by employers in this regard was when employers began conducting simple internet searches of applicants. Then, as Facebook became popular, many employers specifically checked for Facebook pages and the information they yielded. Some employers even asked applicants to identify their user names on social media sites. As applicants became savvier and began limiting what information from their accounts was available to the public, some employers decided to raise the stakes even higher by asking applicants to provide their user name passwords so that the employer could access the site and take a look around.

Employers requesting applicant passwords to social media sites had many questioning, "Can employers do that? Is that even legal?" Federal legislators wondered the same thing, as in March 2012 two United States Senators sent a request to the U.S. Attorney General asking the Department of Justice to investigate whether the practice violated current federal law. Apparently believing that the answer might be "No," federal legislators have also introduced two bills that would prohibit employers from requesting social media passwords.

The Social Networking Online Protection Act (SNOPA) was introduced in the House of Representatives on April 27, 2012. SNOPA

would prohibit an employer from asking its employees and applicants (and prohibit schools from asking its students) for Facebook and other social media passwords. Specifically, it provided that it would be unlawful for any employer to:

- Require or request any employee or applicant for employment to provide their user name, password, or other means for accessing a private email account or social networking website account; or
- Discharge, discipline, or discriminate against any employee or applicant because of the employee's refusal to provide such information or because the employee or applicant filed a complaint or testified in a proceeding related to SNOPA.

SNOPA includes a civil penalty provision up to $10,000 and gives the Secretary of Labor the authority to bring an action for injunctive relief. Unlike employment discrimination statutes that typically do not apply to very small businesses, SNOPA would apply to all employers, regardless of workforce size, as it expressly defined the term "employer" as meaning "any person acting directly or indirectly in the interest of an employer in relation to an employee or an applicant for employment."

Another proposed measure, the Password Protection Act of 2012 (PPA), was introduced in both houses of Congress on May 9, 2012. The PPA would amend the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, by adding the following provision among its prohibitions:

> [F]or the purposes of employing, promoting, or terminating employment, compel[ling] or coerc[ing] any person to authorize access, such as by providing a password or similar information through which a computer may be accessed, to a protected computer that is not the employer's protected computer, and thereby obtains information from such protected computer.

The PPA would, among other things, also prohibit employers from disciplining or discriminating against any person who fails to provide the employer with access to the employee's protected computer. The PPA carves out exemptions for the military and federal agencies, such as the National Security Agency and Defense Intelligence Agency, which deal with classified information. Also, PPA adopts the same definition of employer as found in the Genetic Information Nondiscrimination Act of 2008, which would make it applicable to most businesses with 15 or more employees.

Commentators have noted that the PPA, given its broad language, would apply to personal email accounts and smart phones, including iPhones. The belief is that the drafters tried to craft language that would be sufficiently flexible to remain relevant as new technologies are developed. Unlike SNOPA, the PPA does not extend protection for students by password-related requests by universities.

While both SNOPA and the PPA have been referred to committee, neither has made it far along in the process.

States also have taken action. In May 2012, Maryland became the first state to pass a password protection measure for employees and applicants. Illinois joined it earlier this month. Similar bills are reportedly pending in at least twelve other states, including California, Delaware, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, Pennsylvania, South Carolina, and Washington.

Illinois' provision, 820 ILCS § 55/10, not only makes it unlawful for an employer to request that any employee or applicant provide any password for a social media site, it prohibits an employer from demanding "access in any manner to an employee's or prospective employee's account or profile on a social networking website." Some commentators have interpreted this language to include a prohibition on "shoulder surfing," where an interviewer asks an applicant to log into his or her account while the interviewer looks on.

Employers considering using investigation of social media information as a screening tool should not only be wary of prohibitive legislation, but they should also consider the possible drawback that could expose them to liability under employment discrimination laws. While the potential upside of social media screening is the ability to obtain potentially valuable information showing the applicant to not be a desirable candidate for a position, one potential downside is that the employer may unwittingly gain knowledge of protected-class-status information, such as the religion, age, marital or pregnancy status, or sexual orientation of an applicant. For example, instead of being able to head off a disability claim on the grounds that the employer was unaware of any disabling medical condition, the applicant (or now employee) may argue that the employer may have seen postings, comments, or messages about an ongoing medical problem. Thus, it may be better to rely on objective qualifications and engaging in personal interaction and assessment rather than to cast a wide net in terms of information gathering in the hopes of unearthing a single, perhaps salacious, disqualifying trait.


Forward this issue

Arizona | California | Connecticut |Florida | Georgia | Illiniois | Indiana | Iowa
Massachusetts | New Jersey | New York | Ohio | Tennessee | Washington, D.C. | Wisconsin

www.gshllp.com