EPSTEIN BECKER GREEN

Act Now Advisory: Under Attack: Employer Access to Social Media Accounts of Employees and Applicants

April 19, 2012 | Publications

- Since 2006, the McLean County, Illinois, sheriff's office has asked applicants to sign into Facebook during interviews so that their accounts can be screened.
- In Spotsylvania County, Virginia, the sheriff's department asks applicants for law enforcement positions to "friend" its background investigators.
- The city of Bozeman, Montana, had a policy of asking job applicants for passwords to their email addresses, social networking websites, and other online accounts until, facing a public outcry, it rescinded the policy in June 2009.

These public sector employers had the public's safety and welfare in mind when they sought access to an applicant's social media accounts; the hiring of a dangerous or untruthful individual in a public safety position can have dire consequences. There are also valid, business-related reasons for private-sector employers to seek access to an applicant's online accounts, particularly social networking sites: verification of information, safeguarding or taking action against defamatory statements, and preventing conflicts of interest. These practices, however, have recently ignited a firestorm of criticism, particularly in the wake of a March 29, 2012, Associated Press story characterizing the practices as "common." Facebook's Chief Privacy Officer criticized such practices as violations of personal privacy, and also cautioned that they carry with them legal risk — including accessing information considered protected under federal and state equal employment opportunity laws. The issue has drawn attention in Washington, D.C., where two U.S. Senators have asked the Equal Employment Opportunity Commission to investigate the legality of employers' requests for access to social media sites, as well as

People

David W. Garland
Board of Directors / Member of the Firm
Employment Litigation
New York, Newark
212-351-4708
dgarland@ebglaw.com

in state legislatures across the country.

This month, Maryland became the first state to pass legislation prohibiting employers from asking current or prospective employees for their usernames or passwords to social media sites. Md. Labor & Employment Code § 3-712. Maryland legislators became aware of this issue as a result of publicity given to an incident involving an employee of the state's Department of Corrections, who was asked for his Facebook password in connection with a job recertification process. The interviewer wanted to establish that the employee did not have gang contacts that might compromise his ability to perform his job. Although reluctant to provide the information, the employee felt that he had no choice. He watched while the interviewer logged on to his Facebook account and reviewed his messages, wall posts, and photos. Immediately after the interview, the employee contacted the American Civil Liberties Union.

The Maryland legislation, which passed with overwhelming support, provides that an employer "may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device." Neither may an employer discharge, discipline, or penalize an employee (or threaten to do so), or decline to hire an applicant, as a result of the employee's or applicant's refusal to provide such information. The bill has gone to the governor, who is expected to sign it.

Maryland legislators tempered this prohibition with limited protections for employers. The legislation prohibits employees from downloading unauthorized employer proprietary information or financial data to a personal website or web-based account. It also permits an employer to conduct investigations for the purpose of ensuring compliance with applicable securities laws or regulatory requirements, if the employer learns that a personal website or web-based account is being used by the employee in a way that would violate such laws or regulations. The legislation is silent as to the permissible means of obtaining such information.

Similar bills have been introduced in the legislatures of California, Illinois, Michigan, Minnesota, Washington, and, most recently, New York. Michigan legislators introduced a bill after learning of a teacher's aide who was fired when she refused to divulge her Facebook password to school administrators. The latter had been notified by a parent — with whom the aide was Facebook "friends" — of a posted photograph that the parent considered inappropriate. The proposed Michigan legislation, House Bill No. 5523, prohibits the same conduct as the Maryland bill, and adds a section prohibiting educational institutions from accessing *student* social media accounts. Violation of the statute would be a misdemeanor, and would also expose the violator to a private right of action in the Michigan circuit courts.

Minnesota's proposed legislation, H.F. No. 2963, would prohibit employers from asking for "any password or other related account information" to gain access to an account or profile on a social networking site but provides that such a site "shall not include electronic mail." The bill underscores the employer's right to regulate workplace conduct: "This paragraph shall not limit an employer's right to develop and maintain lawful workplace policies governing the use of the employer's electronic equipment, including policies regarding internet use, social networking site use, and electronic mail use."

Legislation passed by the Illinois House takes a slightly different approach; it bans employers from accessing social media passwords but permits them to ask for usernames so that they can view publicly available information. Similar considerations motivated Washington State Senator Steve Hobbs, who introduced his "Facebook bill" on April 4, 2012. That bill would impose a fine of $500 and attorneys' fees for violation of the law.

New York's proposed legislation, S. 6938, was introduced on April 13, 2012. The legislation's prohibition against asking for "any log-in name, password, or other means for accessing a personal account or service" (or taking adverse action because of a refusal to provide such information) is tempered by a provision permitting employers to ask for such information for "non-personal accounts or services that provide access to the employer's internal computer or information systems" — for instance, a personal computer with Citrix or other software applications that allow an employee to access the company's electronic systems remotely. The bill establishes civil penalties in the amount of $300 for the first violation and $500 for each subsequent one, and also creates a private right of action by "aggrieved individuals" for equitable relief and damages.

California's legislation, AB 1844, attempts to balance employer and employee interests by prohibiting access to employee/applicant social media while shielding employers from negligent hiring claims that may be premised on a failure to investigate social media sites: "For purposes of a claim of negligent hiring, an employer does not fail to exercise reasonable care to discover whether a potential employee is unfit or incompetent by the employer's failure to search or monitor social media before hiring the employee." Although this legislation proposes to amend the California Labor Code, it is worth noting that California's Constitution guarantees citizens a right to privacy, making employer access to social media risky on constitutional grounds, as well.

Employer access to Facebook and other electronic accounts has also been successfully challenged under the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-11, which is Title II of the Electronics Communications Privacy Act. The SCA makes it an offense to intentionally access, without authorization, "a facility through which an electronic service is provided ?... and thereby obtain[] ?... access to a wire or electronic communication while it is in electronic storage in such a

system." 18 U.S.C. §2701 (a)(1). No liability exists, however, for one who accesses such information with the authorization of a user of that service. 18 U.S.C. §2701(c)(2).

In *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 (D.N.J. Sept. 25, 2009) (unpublished), the district court upheld a jury verdict against an employer that asked employees to provide their MySpace log-in information to supervisors. The employer argued that the employees authorized access when they acceded to the supervisors' requests, and, therefore, that access did not violate the SCA. However, the employees testified that they were, in effect, under duress; they did not want to disclose their passwords but believed if they did not do so they would be "in trouble." The jury decided that the supposed "authorization" was a sham, and, in fact, the employer had violated the SCA. The district court denied a motion for a new trial, stating that the jury was justified in finding a violation of the SCA and analogous state law.

The U.S. Court of Appeals for the Ninth Circuit reached the same conclusion with regard to a private website set up by a Hawaiian Airlines pilot, on which he posted bulletins critical of his employer, its officers, and the union representing the pilots. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002). The plaintiff controlled access to his website by creating a list of people eligible to access the website, each of whom had to create a password to enter the site. A company vice-president accessed the site using the names of two pilots on the "eligible" list, with their permission. In a technical decision parsing the language of the statute, the Ninth Circuit decided that, because the two "eligible" pilots had never actually accessed the website, they were not "users" of the service. Therefore, they were not authorized to grant access to the site, and the access in question did not fall within the exception to liability found in 18 U.S.C. §2701(c)(2). The Ninth Circuit also found that a Railway Labor Act claim, in which the plaintiff alleged that the airline had interfered with protected union activity when it accessed his website, could go to a jury.

What Employers Should Do Now

- If you are a Maryland employer, review your policies and procedures on accessing the social media sites of employees and/or job applicants. Once the new legislation is signed by the governor and goes into effect, you should bring any such policies into compliance with the state's new law. If you are an employer in one of the other states considering laws similar to Maryland's, stay apprised of the status of the pending bills and adjust your policies and

procedures accordingly.

- In light of the general public support for these laws, and the emphasis in our society on individual privacy rights, prudence dictates that you review and reevaluate all your social media access policies. If you maintain access-to-social-media policies in a jurisdiction in which they are not prohibited, make sure that you clearly define the business considerations underlying the policies. A policy that is narrowly applied to positions affecting human health, safety, and security, which clearly articulates these legitimate concerns, is more likely to withstand a legal challenge.
- Give due consideration to employee privacy concerns and, if social media is accessed, do so in the most considerate way possible, confining the information to as few people as possible. Remember the potential challenges posed by state constitutional and common law privacy claims.
- Develop a system to address the problem of "too much information." Use a person not involved in the hiring decision to check the site in question for relevant information so that the ultimate decision-makers are unaware of information pertaining to state and federally protected Equal Employment Opportunity categories, such as age, race, and sexual orientation.

*****

For more information about this Advisory, please contact:

David W. Garland
New York
212/351-4708
dgarland@ebglaw.com