PASSWORD PROTECTED?

An Employer's Ability to Access Facebook Passwords

Author: Tracy H. Stroud, Attorney at Law

Across the country, employers have begun asking prospective and current employees for their Facebook passwords. In March 2012, United States Senators Richard Blumenthal and Charles Schumer asked the Department of Justice (DOJ) and the Equal Employment Opportunity Commission (EEOC) to investigate whether this practice violates computer protection statutes, namely, the Stored Communication Act (SCA) (18 U.S.C. § 2701), and the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030). The SCA prohibits intentional access to electronic information without authorization or intentionally exceeding that authorization The CFAA prohibits intentional access to a computer without authorization to obtain information. Requiring applicants and employees to provide usernames and passwords to secure social media websites and then using those credentials to access their private information may violate both SCA and the CFAA.

Two courts have examined the issue and found that when supervisors request employee login credentials and access otherwise private information with those credentials, the supervisors may have civil liability under the SCA. In *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir., 2002), James Konop, a Hawaiian airlines pilot, maintained a website where he posted bulletins critical of his employer. He controlled access to his website by requiring visitors to log in with a username and password, and he created a list of people eligible to access the website. Konop's supervisor obtained user names and passwords for two employees on the eligible list. He then logged onto the website as many as twenty (20) times as Gene Wong and at least fourteen (14) times as James Gardner, the approved users. The court allowed the case to move forward on the grounds that the employer could be liable under the SCA. In *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 (D. N.J. 2009), the court found employer's managers violated SCA by knowingly accessing a chat group on a social networking website without authorization. The employee had provided her login information to the manager, but she did not authorize access to the chat group.

As a result of the DOJ and EEOC investigations, in May, Senators Blumenthal and Schumer introduced a bill called the Password Protection Act of 2012. The highlights of the bill include: (1) prohibiting an employer from forcing prospective or current employees to provide access to their own private account as a condition of employment; (2) prohibiting employers from discriminating or retaliating against a prospective or current employee because the employee refuses to provide access to a password protected account; and (3) prohibiting adverse employment consequences when an employee does not provide access to their own private accounts. Employers who violate the Act would face financial penalties. The bill does preserve

employers' rights to regulate social media use within the office as well as the ability to set policies for employer computer systems.

States are also joining the bandwagon. Maryland's governor signed a bill in May to take effect October 1, 2012, prohibiting Maryland employers from asking current and prospective employees for their usernames and passwords to all social media sites. Illinois and California are considering similar legislation. The genesis of the Maryland law came about when Robert Collins, a Maryland Department of Corrections Officer, contacted the ACLU after being asked for his Facebook password in a recertification interview. To keep his job, he felt that he had no choice but to provide his password, and he had to sit there while the interviewer logged onto his Facebook account and reviewed his messages, wall posts and photos. On the flip side, the Department of Corrections said the policy had been an effective factor in employment denial to seven individuals over the course of a year, some of whom had utilized social media applications to post pictures of them showing gang signs.

Facebook's Privacy Officer, Erin Egan, has weighed in on this controversy, "In recent months, we've seen a distressing increase in reports of employers or others seeking to gain inappropriate access to people's Facebook profiles or private information." Facebook and others believe that the practice potentially exposes employers to unanticipated legal liability. For example, in job interviews, employers cannot ask certain questions about a person's children, pregnancy, sexual orientation, medical status, or religion. Once an employer starts trolling through someone's Facebook life, he stumbles onto a wealth of information. The employer can obtain private information such as age, pregnancy or familial status, national origin, religion or race, and employment may be denied because the employee is in one of these protected classes. If the company subsequently does not hire that person, the company may open itself up to allegations of discrimination.

On the other hand, there can be valid uses for obtaining an employee's password information. Comprehensive background checks for individuals seeking employment in law enforcement, at highly sensitive government sites, and for employees with high level security clearances are valid reasons to obtain social media passwords.

At this point the legality of employers obtaining employee passwords remains murky. It is clear that employers can make affirmative policies against Facebook use in the workplace, the use of Smartphones in the workplace, or accessing social media sites on company computers. As well, employers have a right to obtain information from their own servers. In an employer's handbook, employees should be made aware of these policies. Outside of those protections for employers, obtaining passwords for private email accounts or obtaining social media passwords is probably unlawful and a hornet's nest to avoid.