A Timely Analysis of Legal Developments

ASAP®

March 2012

Though Not Yet Banned, Requiring Social Media Information Is a Bad Idea

By Chris Leh

Employers continue to wrestle with the issue of whether to require employees and prospective employees to divulge their social media passwords. A recent spike in interest by the media, by advocacy groups, legislators and the general public has refocused attention on the issue. Although it may not be unlawful to seek the information to conduct background checks, deter and investigate harassment of coworkers, and discourage employees from posting online content that disparages the employer's products or services, in most situations, it is inadvisable.

The efforts of law enforcement agencies to obtain social media log-in information to supplement background checks on prospective recruits have received the most notoriety:

- Since 2006, the sheriff's office of McLean County, Illinois (like several others in the state) has requested login information from applicants to weed out those who have posted inappropriate pictures, had inappropriate relationships with people who are underage or engaged in other illegal behavior.
- In 2009, the City of Bozeman, Montana decided to require all applicants for employment to provide full login information, including passwords, to all social networks and online sites of which they were members. One city official recently said the city sought the information to ensure that prospective police officers were who they said they were. Shortly after the practice came under fire in the media, Bozeman discontinued it.
- In 2010, the Maryland Department of Public Safety and Correctional Services required job candidates to submit user name and password information related to their social media websites so it could check for gang affiliations. DPSCS stated that it rejected seven applicants based on information it obtained but eventually decided to drop the requirement. That decision occurred just days after a video made by the American Civil Liberties Union about the requirement went viral, prompting a public outcry.
- Similarly, in November 2011, a photo surfaced showing an application for a police clerical position in North Carolina, which asked, "Do you have any web page accounts such as Facebook, Myspace [sic], etc.? If so, list your username and password." The requirement sparked similar outrage.

Although governmental entities have been the targets of most of the media reports of social media login requirements, some private entities have engaged in the practice as well. For example, a New

York statistician withdrew his application when an interviewer at the company to which he had applied asked for his social media password.

Some critics of the practice, including Orin Kerr of George Washington University Law School, have asserted that surrendering a Facebook password is like handing over a key to a home. But that's incorrect. One commentator recently explained why: "If I wanted to stay in my house forever – never to come out again – I could, and my privacy would be intact. And I could do whatever I want inside my house. That's my territory. I control what it looks like, how it functions and what I do inside it. Facebook is entirely different. [Facebook officials] call all the shots. They get to decide what the environment looks like in my Facebook world. They create the arena in which I chat with my friends, play with apps and like websites, companies and causes. They monitor and track everything I do inside their world -- and they make a lot of money because of the practice."

Nevertheless, social media vendors have expressed outrage over employers' requiring users to produce their login information. On March 23, Facebook issued a statement on its blog condemning the practice. The company now prohibits users from soliciting login information, accessing accounts belonging to someone else, sharing passwords, and otherwise jeopardizing the security of their accounts. Although Facebook initially stated that it would "take action to protect the privacy and security of our users . . . by initiating legal action . . . .," the company later clarified that it "[did] not have any immediate plans to take legal action against any specific employers . . . ." Apart from barring such employers from establishing "pages" on Facebook or advertising there, however, it seems unlikely that it could bring such a claim on behalf of its users in any case.

So far, few courts have issued decisions that provide any guidance about the legality of seeking social media login information from employees or prospective employees. In *Pietrylo v. Hillstone Restaurant Group*, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009), a federal trial court case in New Jersey, the plaintiffs were restaurant employees who belonged to a chat group. Access to that group required an invitation and then a member's MySpace account and password. One of the restaurant's managers asked another restaurant employee for her login information for the chat group, which the employee provided. The plaintiffs brought a civil suit against the restaurant, claiming (among other things) that the managers had violated the Stored Communications Act (SCA). To prevail on the SCA claim, the plaintiffs were required to prove that the managers "knowingly, intentionally or purposefully" accessed the chat group without authorization. SCA violations may lead to statutory damages, punitive damages, and attorneys' fees and costs.

The jury found in favor of the plaintiffs and awarded them, collectively, $3,403 in compensatory and punitive damages. On its motion to set aside the verdict, the restaurant argued that the login information used to access the chat group came from an employee who had authorized them to access the site. But the authorizing employee testified that if she had not provided access, she believed that she "probably would have gotten in trouble." The court held that it was reasonable for the jury to infer that the employee's "purported 'authorization' was coerced or provided under pressure." The restaurant also argued that the managers did not access the chat group "knowingly, intentionally or purposefully." But, the court held that the jury reasonably could have drawn the contrary conclusion that it reached, explaining that the managers had accessed the site even though "it was clear on the website that the chat group was intended to be private and only accessible to invited members."

As discussed in a prior Littler Workplace Privacy Counsel post, the *Pietrylo* case is significant for employers because it recognizes that even if an employee provides the employer with login information for a social media site, using that information still may be unauthorized and may create liability under the SCA. But the decision may have limited impact. First, it is not binding on any other state or federal courts. Second, the court did not address whether the law required it to apply an objective standard – whether or not a reasonable person would believe she had provided authorization to the employer to access the chat group frequented by the plaintiffs. Instead, the court's decision on the SCA hinges on a single, subjective statement by one employee-witness. A different court might well apply an objective test and reach a different result. Third, if, as in *Pietrylo*, a subjective belief that an adverse action by the employer might occur is enough to demonstrate coercion or duress by an employer, authorization requirements in other areas of law might come under fire as well. For example, an employee asked to sign a Fair Credit Reporting Act authorization to permit a third party to conduct a background investigation might later claim that he believed he would be fired if he did not sign the authorization and then assert that any information from the background check found after he signed the written authorization was unlawfully obtained through coercion or duress. Applied by analogy, *Pietrylo's* subjective test for establishing coercion may create similarly absurd results in other circumstances, such as drug testing.

Although the legal status of the *Pietrylo* decision is unclear, Congress and state legislatures appear likely to take actions to limit or prevent

employers from eliciting social media login information from prospective and current employees. Recently, U.S. Senator Richard Blumenthal (D-CT) has stated that he is planning to offer federal legislation to prohibit the practice. He and Charles Schumer (D-NY) have asked the U.S. Department of Justice and the Equal Employment Opportunity Commission to launch investigations as to whether employers asking for Facebook passwords during job interviews are violating federal law.

The states are further along in their legislative efforts to regulate employers' collection and use of login information regarding social media sites:

- In Maryland, several bills were introduced in the Maryland legislature, one of which is still pending. That bill would prohibit an employer from requesting or requiring an applicant or employee to disclose login information for any personal account or service and prohibit an employer from taking, or threatening to take, disciplinary action based on the refusal to provide that information.
- In Illinois, a pending bill would prohibit employers from asking current or prospective employees to provide login information to gain access to their accounts or profiles on a social media site. The bill would allow job-seekers to file lawsuits if asked for access to sites like Facebook, but bosses could still ask for usernames that would allow them to view public information on the sites. Critics are concerned that a provision allowing employers to maintain lawful workplace policies regarding electronic equipment and investigating suspected unlawful or improper activity may undercut the desired protections of worker privacy. The bill is now on hold pending revision.
- In California, a bill now pending in the Assembly would prohibit employers from requiring employees or prospective employees from disclosing a user name or account password to access social media used by the employee or prospective employee. The bill also provides that in a claim of negligent hiring, an employer does not fail to exercise due care by not searching or monitoring social media before hiring an employee. Other California legislators are planning to introduce similar legislation.
- In New Jersey, an Assemblyman plans to introduce legislation that would prohibit an employer from requiring a current or prospective employee to provide or disclose social media login information, requiring a prospective employee to waive or limit any protection granted under the bill as a condition of applying for or receiving an offer of employment, and prohibiting retaliation or discrimination against an individual who complains about or participates in any investigation about violations of the law.

Consequently, state and perhaps federal law may soon prohibit at least some employers around the country from requiring employees and prospective employees to provide their login information for the social media sites they use. In the meantime, however, the practice currently is not prohibited.

If it is not prohibited for an employer to require an employee or prospective employee to provide social media account login information as a term of employment or continued employment, should the employer refrain from doing so? In most cases, the answer is yes:

- A fundamental best practice of information-gathering about employees is that the information sought should be related to the job that is at issue and whether the employee or prospective employee involved is capable of doing the job, or doing it properly, or engaging in misconduct related to his or her work. In many circumstances, information gleaned from a social media account is not likely to be particularly job-related; traditional interviews, reference checks, employment testing, and background checks are sufficient.
- Information gleaned from employees' social media accounts may well put employers on notice of information about employees or prospective employees that employers would be better off not having before making hiring decisions, including race, sex, age, disability or sexual orientation. The same is true for all, or certain types of, lawful, off-duty conduct, which many states prohibit employers or prospective employers from considering when they make hiring, disciplinary or other employment decisions.
- The employer that engages in the practice of seeking or requiring prospective or current employees to provide social media login information may become the target of a public Internet shaming campaign, may see a reduction in worker morale, and would likely discourage promising candidates from applying or encourage them to back out, unnecessarily limiting the labor pool.

In light of the likelihood of new legislation and the internal and public backlash against employers that request or require social media login information, the best practice is simply not to ask unless the employer has a strong and legitimate business reason for doing so. Even then, the employer should carefully weigh the risks and implement measures to mitigate the risks.

Although requiring employees or prospective employees to provide social media log-in information may be problematic, it is not yet illegal. There are circumstances in which it may be important to do it. For example, an employer may determine that it needs the information to investigate properly a complaint that coworkers, supervisors, or vendors are using social media to harass an employee or to engage in some other work-related misconduct. Similarly, some employers, such as those who hire for positions that will involve sensitive security issues or require a formal security clearance, may decide that there are legitimate business reasons for reviewing an applicant's restricted social media pages as part of the hiring process. To reduce the risks of legal liability or unwanted publicity, such employers should consider taking the following steps:

- Narrowly tailor the use of the requirement to circumstances in which review of social media activity advances important, articulable business objectives.
- Establish and apply consistently a written protocol specifying the circumstances in which log-in information will be required, who will have access to it, for what purpose it will be used, and the steps that will be taken to ensure that the information will be disseminated only to those with a need to know.
- If the employer plans to involve a third party to conduct the review, comply with the requirements of the Fair Credit Reporting Act and require that third party to follow the protocol.
- Request written consent from the employee or prospective employees and specify the consequences for refusal to consent.
- When reviewing an applicant's restricted social media pages, screen decision makers from information upon which the employer cannot lawfully rely in making an employment decision.
- Document the steps in the review and the findings.
- Thoroughly train affected employees concerning the protocol and the consequences of violating it.

Chris Leh is Of Counsel in Littler Mendelson's Denver office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Leh at cleh@littler.com.