A Timely Analysis of Legal Developments

ASAP®

August 7, 2012

Illinois' New Social Media Password Protection Law Handicaps Employers' Legitimate Business Activities

By Philip Gordon and Kathryn Siegel

On August 1, 2012, Illinois Governor Pat Quinn signed into law a bill modifying Illinois' Right to Privacy in the Workplace Act to limit employers' access to applicants' and employees' restricted social media accounts. The Illinois bill applies to both public sector and private sector employers.

The bill's sponsor, State Representative La Shawn Ford, explained his intentions in introducing the Bill as follows in a May 23, 2012, news release:

> Social networking accounts are places where we document the personal and private aspects of our lives, and employers have realized they can get answers to questions they are already prohibited from asking by gaining unfettered access to our accounts. Who we are friends with and what organizations we choose to support outside of work have nothing to do with whether we can do the job. Responding to current changes in our society, this bill takes a reasonable approach to protect our personal privacy.

Representative Ford's comments, however, ignore the fact that employers may have a legitimate interest in accessing applicants' or employees' restricted social media profiles — for example, to determine whether an applicant for a child care position has a proclivity for pedophilia or to investigate a post suggesting an employee's intent to engage in workplace violence.

Representative Ford explained to the Chicago Tribune that his office had received letters from a "small amount" of constituents who had been asked to provide their social media passwords to employers, and that the practice was prevalent in law enforcement and banking industries. Contrary to this non-empirical data, however, Littler Mendelson's Executive Employer Survey Report, published in June 2012, found that private employers *rarely* request social media log-in credentials from applicants or employees. That survey asked nearly 1,000 C-suite executives, corporate counsel, and human resources professionals from corporations throughout the United States and ranging in market capitalization from less than $1 billion to more than $4 billion the following question: "Has your organization requested social media logins as part of the hiring or onboarding process?" The response: 99% of respondents answered the question in the negative.

In any event, the law makes Illinois the second state in recent months (after Maryland) to forbid employers from requesting or requiring log-in credentials for an applicant's or employee's social

networking sites. Similar bills currently are pending or proposed in 12 other states, including California, Delaware, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, Pennsylvania, South Carolina and Washington, and in both houses of Congress.

Illinois' new law makes it unlawful for an employer to:

- "request or require any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website[;]" or
- "demand access in any manner to an employee's or prospective employee's account or profile on a social networking website."

While the language in the first bullet point seems relatively straightforward, the scope of the second provision is ambiguous. At first glance, the second provision appears to be intended to prohibit "shoulder surfing." In other words, the second provision was drafted to respond to concerns that an employer might demand that an employee or applicant show the employer his or her social media profile or account, without revealing any log-in credentials, as a way of circumventing the first provision prohibiting the employer from directly asking for an employee's or applicant's log-in credentials.

The ambiguous language, however, could be read even more broadly. For instance, if an employee complained about a Facebook post made by a co-worker that appeared on the complaining employee's Facebook timeline, the employer arguably could not ask the complaining employee for a printout of his timeline, an email of the timeline showing the post, or to view the post on the complaining employee's timeline, even though the target of the investigation is not the complaining employee's own social media content. The provision also arguably would prohibit the employer from asking the complaining employee to print, email, or show the employer the accused employee's timeline.

It is also not clear what "demand[ing] access in any manner" means. Facebook privacy settings may be set up in such a way that friends and "friends of friends" can see a Facebook page. If a member of an employer's management "friends" an employee's Facebook friend and gains access to the employee's Facebook page in that way, has the employer demanded access? Turning to other social media sites, if a manager uses his or her personal Twitter account and requests to follow an employee's private personal Twitter account, has the manager demanded access?

Beyond its broad and imprecise language, Illinois' new law is also concerning because it does not include any exceptions. The law merely emphasizes that it is not intended to restrict an employer's right to promulgate policies regulating use of the employer's own electronic resources or from monitoring usage of the employer's own electronic resources, including e-mail. There is no exception for legitimate workplace investigations. Thus, as noted above, a death threat communicated to a co-worker via a restricted social media page appears to be off-limits to the employer unless provided voluntarily by an employee.

The law does expressly state that it does not apply to "information that is in the public domain," *i.e.*, social networking sites for which the account holder has not used privacy settings to restrict access. However, this limitation provides little aid to employers as applicants and employees increasingly activate privacy settings to restrict access to their social media accounts. Further, because Facebook settings can be modified to permit different people access to different information, it is not clear what information will be considered to be in the "public domain."

The Administration and Enforcement Section of the Right to Privacy in the Workplace Act, which was amended by this new law, provides that an employee or applicant for employment may file a complaint with the Illinois Department of Labor. The Department is instructed to investigate and attempt to resolve the complaint. If it finds a violation and is unable to resolve the complaint with the employer, the Department may sue the employer in Circuit Court to compel compliance. If the Department fails to file an action in civil court, the employee or applicant may commence an action in Circuit Court. A successful plaintiff may be awarded actual damages, plus costs, and a penalty may issue against the employer for $200, plus costs, attorney's fees and actual damages for a willful and knowing violation.

Given that most employers recognize that employees' lawful off-duty activities are the employees' own business if those activities do not affect the workplace, the Illinois law is unnecessarily overbroad. The law prevents employers from conducting legitimate investigations and does not take into account the intricacies of the different social media sites. The law will be particularly challenging for Illinois employers to apply because of its ambiguity. Until regulations or court decisions clarify the ambiguity, the safest course of action for an Illinois employer would be to avoid *any* access to employees' or applicants' social media site(s) that are not in the public domain.

Philip Gordon, Chair of Littler Mendelson's Privacy and Data Protection Practice Group, is a Shareholder in the Denver office, and Kathryn Siegel is an Associate in the Chicago office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, Mr. Gordon at pgordon@littler.com, or Ms. Siegel at ksiegel@littler.com.