A Timely Analysis of Legal Developments

ASAP®

September 4, 2013

New Jersey Becomes the Twelfth State to Enact Social Media Password Protection Legislation; Recent Amendment to Illinois' Law Benefits the Financial Services Sector

By Philip Gordon and Joon Hwang

On August 29, 2013, New Jersey became the twelfth state to enact social media password protection legislation, continuing the nationwide trend towards imposing some form of restriction on employer access to the restricted, personal social media content of applicants and employees.[1] The new law becomes effective on December 1, 2013. Two weeks earlier, Illinois amended its existing password protection law. The amendment narrows the law's prohibitions so that the law does not impede financial services firms from monitoring their employees' business-related communications in social media.[2]

The New Jersey Law

The new law was enacted after Governor Chris Christie vetoed an earlier bill, which he characterized as "well-intentioned" but "too broad[.]" According to Governor Christie, the earlier bill was so broad that "an employer interviewing a candidate for a marketing job would be prohibited from asking about the candidate's use of social networking [] to gauge the candidate's technological skills and media savvy." In addition, the bill would "subject an employer to protracted litigation, compensatory damages, and attorneys' fees—a result that could not have been the sponsors' intent."

To alleviate this overbreadth, Governor Christie proposed removing the prohibition against asking applicants or employees merely to *disclose* whether they have a personal social media account. The governor also proposed striking language allowing applicants and employees to sue employers for alleged violations and recommended several employer-friendly exceptions to the prohibitions.

---

1 *See* Philip Gordon and Joon Hwang, *Making Sense of the Complex Patchwork Created by Nearly One Dozen New Social Media Password Protection Laws*, Littler ASAP (Jul. 2, 2013); Philip Gordon, Amber Spataro and William Simmons, *Workplace Policy Institute: Social Media Password Protection and Privacy — The Patchwork of State Laws and How It Affects Employers*, Littler Report (May 31, 2013)

2 *See* Philip Gordon and Kathryn Siegel, *Illinois' New Social Media Password Protection Law Handicaps Employers' Legitimate Business Activities*, Littler ASAP (Aug. 7, 2012).

The New Law's Prohibitions

While the new law adopts all of Governor Christie's proposed changes, it still broadly restricts employer access to the social media content of applicants and employees. The new law prohibits employers from asking or requiring that job applicants or current employees "provide or disclose any user name or password, or in *any way provide the employer access to, a personal account through an electronic communications device*" (emphasis supplied). The italicized language appears to encompass several different means of accessing restricted social media content, such as: (a) "shoulder surfing" an applicant's or employee's restricted, personal social media account; (b) compelling an applicant or employee to accept an employer's "friend" request to permit access to a restricted account; and (c) requiring an applicant or employee to change the privacy settings on a restricted account to enable the employer to access it. By prohibiting far more than just a request for an applicant's or employee's social media log-in credentials, New Jersey's prohibition is among the broadest in the nation.

The New Jersey law also is particularly broad as compared to similar laws in another important respect. All such laws prohibit an employer from requesting or requiring that applicants or employees provide access to their own personal accounts. New Jersey's law, by contrast, prohibits employers from seeking access to "*a* personal account" (emphasis supplied). Consequently, it appears that the New Jersey law would, for example, prohibit an employer from asking an employee to access the "friends only" Facebook page of a co-worker, so the employer could view the co-worker's restricted, social media content as opposed to the employee's own social media content.

In addition to broadly prohibiting the types of access requests described above, New Jersey's password protection law prohibits an employer from retaliating or discriminating against any job applicant or current employee for any of the following conduct: (1) refusing to comply with an employer's request or demand for log-in information for a personal social media account; (2) reporting alleged violation of the law to New Jersey's Commissioner of Labor and Workforce Development; (3) testifying, assisting, or participating in an investigation concerning a violation of the law; and (4) otherwise opposing a violation of the law.

The law's definitions of "personal account" and "social networking website" narrow its otherwise broad prohibitions to some extent. Whereas some password protection laws extend their protections to all online accounts, the definition of "social networking website" limits the law's scope to social media accounts. Other online accounts, such as personal e-mail accounts, are not covered. In addition, an account is not "personal" if it is used "for business purposes of the employer or to engage in business-related communications." As a result, the law does not prohibit employers from requesting log-in credentials for, or any other means of access to, business-related accounts.

Exceptions to the General Prohibitions

In adopting Governor Christie's proposed changes, New Jersey's legislature built into the new law several important limitations on its otherwise broad scope. Of particular importance for employers, the new law provides that "[n]othing in this act shall prevent an employer from conducting an investigation:" (a) to "ensure compliance with applicable laws" or with "prohibitions against employee misconduct" if the employer receives "specific information about activity on a personal account by an employee;" or (b) of specific allegations that an employee is transferring proprietary, confidential, or financial information to a personal account. This exception appears to permit an employer to ask for log-in credentials if the circumstances described apply.

The new law also contains an important exception for financial services firms subject to FINRA regulations that require monitoring of employees' social media communications. This exception provides that the new law should not be construed to prohibit an employer from "complying with the requirements of [s]tate or federal statutes, rules or regulations, case law or rules of self-regulatory organizations."

The law contains two other exceptions. Consistent with the law's limitation on the definition of "personal account," it does not prevent an employer from "implementing and enforcing a policy pertaining to the use of an employer issued electronic communications device or any accounts or services provided by the employer or that the employee uses for business purposes." In addition, the law permits employers to access and use information about job applicants and current employees accessible in the public domain. In other words, any information publicly available is fair game. Employers should note that their use of publicly available social media to impose discipline or for other employment decisions may be limited by other laws, such as the National Labor Relations Act, anti-discrimination laws, and laws prohibiting adverse employment action based on lawful off-duty conduct.

No Private Lawsuits, Only Administrative Remedies

The new law provides no private right of action for an aggrieved job applicant or current employee. Instead, an employer who violates any provision of the law may be subject to a civil penalty in an amount not to exceed $1,000 for the first offense and $2,500 for each subsequent offense. New Jersey's Commissioner of Labor and Workforce Development is responsible for enforcing the law.

Amendment to the Illinois Law

Illinois' password protection law prohibits employers from requesting or requiring applicants or employees 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 to gain access in any manner to" such accounts.[3] As originally enacted, the law did not limit this prohibition to "personal" social media accounts and, therefore, the law effectively prohibited employers from monitoring, or even obtaining access to, social media accounts that employees used for business purposes.

The amendment to the Illinois law carves out an important exception for the financial services sector. As amended, the law will no longer apply when an employer requests access to a "professional account" to "monitor or retain employee communications as required under Illinois insurance laws or federal law or by a self-regulatory organization as defined in Section 3(A)(26) of the Securities Exchange Act of 1934, 15 U.S.C. 78(A)(26)." The amendment defines "professional account" as "an account, service, or profile created, maintained, used, or accessed by a current or prospective employee for business purposes of the employer." The amendment also permits Illinois employers to seek access to a professional account when the employer has "a duty to screen applicants or employees prior to hiring." The amendment goes into effect on January 1, 2014.

Illinois employers should note that, even with these new exceptions, Illinois' social media password protection law remains among the most restrictive in the country.

Recommendations for Employers

A recent survey of C-suite executives, human resources professionals, and in-house counsel from a wide variety of industries revealed that only 1% of these respondents requested social media log-in credentials as part of the hiring or onboarding process.[4] Employers in New Jersey and Illinois and in the other ten states that have enacted social media password protection laws—Arkansas, California, Colorado, Maryland, Michigan, New Mexico, Nevada, Oregon, Utah, and Washington—should follow that practice. Employers in these states also should note that these new laws impose no restriction on access to applicants' publicly available social media content. Employers in other states should carefully evaluate whether access to restricted social media content is even needed during the hiring process and, if so, keep apprised of new legislation that could make such requests unlawful. All employers that consider social media content in the hiring process should implement policies, procedures, and training to mitigate the risk that decision makers will be exposed to information on which they cannot lawfully rely for an employment decision.

The exceptions in the New Jersey and Illinois laws, and those in the other social media password protection laws, implicitly recognize that employers have a legitimate business need to access employees' restricted, personal social media accounts in certain circumstances. However, none of these exceptions has yet been tested in court proceedings, and many of them are somewhat unclear. As a result, their precise scope remains uncertain. Accordingly, employers should scrutinize these laws before implementing a monitoring program, or conducting an investigation, that calls for access to employees' restricted social media content.

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

3 820 ILCS 55/10(b)(1).

4 2013 Executive Employer Survey Report, Littler Mendelson (Jul. 9, 2013).