A Timely Analysis of Legal Developments

ASAP®

October 10, 2012

California's New Social Media "Password Protection" Law Takes a More Balanced Approach by Accounting for Employers' Legitimate Business Interests

By Philip Gordon and Lauren Woon

After a series of alleged incidents reported in the news media of employers (principally public employers) requesting or requiring access to employees' or applicants' personal social media accounts, legislators around the country rushed to introduce legislation in response to the public outcry. Maryland and then Illinois enacted the country's first two "password protection" laws. On September 27, 2012, California Governor Jerry Brown signed into law the nation's third such law that generally prohibits employers from requiring or requesting that an employee or applicant provide access to personal social media content. Unlike the Illinois and Maryland laws, however, California's law embodies a more balanced approach, taking into account employers' legitimate business interests. It is effective January 1, 2013.

The Illinois and Maryland laws broadly prohibit access by employers to applicants' and employees' personal social media content. Illinois' law is especially broad, prohibiting employers from "demand[ing] access *in any manner* to an employee's or prospective employee's account or profile on a social networking website." (emphasis supplied). This language prohibits not only direct requests for log-in credentials, but also "shoulder surfing," *i.e.*, viewing social media content over an applicant's or employee's shoulder without asking for log-in credentials, as well as requests that an employee print screen shots of a co-worker's social media posts. The Illinois law has no exceptions at all.

Maryland's prohibition is limited on its face to direct requests for log-in credentials, but includes two narrow exceptions that permit employers to access an employee's social media account: (1) when the request is related to investigations into suspected securities fraud; or (2) when related to misappropriation of trade secrets.

The upshot is that the laws that served as a model for California's legislation effectively stymy employers' legitimate need to investigate suspected misconduct related to work. While these laws impose no restriction on employers' access to publicly available social media content, Illinois and Maryland applicants and employees who choose to use privacy settings to restrict their social media content only to invitees, *e.g.*, Facebook "friends," could use those settings to thwart legitimate investigations. By way of illustration, when an Illinois or Maryland employee reports to HR that a co-worker posted on his "friends only" Facebook page that he "hates his co-workers"

and "wants to shoot them up," the employer would risk engaging in illegal conduct by asking either the reporting employee or the posting co-worker for access to this content so that the employer could view the context and evaluate the risk of a workplace violence incident.

California's new law, entitled "Employer Use of Social Media," also broadly prohibits employers' access to applicants' and employees' personal social media content. Employers cannot request or require that applicants or employees: (a) disclose social media log-in credentials; (b) access personal social media in the employer's presence, i.e., allow the employer to "shoulder surf;" or (c) "[d]ivulge any personal social media content." The third prohibition is particularly broad, apparently barring an employer from asking an employee to provide the personal social media content of a co-worker who is a Facebook friend. Under the law, "social media" includes social media services and accounts, as well as content such as videos, photos, blogs, podcasts, text messages, email, and website profiles and locations.

However, unlike the Illinois and Maryland laws – as well as bills pending in more than one dozen states – California's law contains a critical exception for employers. The exception permits employers to ask an employee to divulge personal social media content that the employer "reasonably believe[s] to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations."

California employers should take heed that, although this exception provides a modicum of balance that is absent from the Illinois and Maryland laws, the exception has important limits. First, the exception does not apply to investigations of job applicants. Second, the exception does not apply to requests for log-in credentials or requests to "shoulder surf;" the exception applies only to requests by an employer that an employee divulge personal social media content. Finally, an employer can use social media content obtained in an investigation pursuant to the exception "solely for purposes of that investigation or a related proceeding."

California's password protection law also prohibits an employer from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee or applicant for refusing to comply with an employer's request or demand for access to a personal social media account. At the same time, the law expressly states that California's Labor Commissioner is not required to investigate complaints that the law has been violated, and the law does not create a private right of action for an employee to prosecute violations of the law. Consequently, it remains to be seen what remedies an employee could pursue in the instances where the Labor Commissioner declines to investigate complaints of violations.

In light of the new "password protection" law, California employers should review their social media policies and procedures to ensure they are not requiring or requesting employees or applicants to: (a) disclose their social media log-in credentials; (b) permit "shoulder surfing;" or (c) divulge any personal social media content. However, when a California employer reasonably believes that personal social media content is necessary for an investigation into employee misconduct or violations of applicable laws and regulations, an employer may ask an employee to divulge that information by, for example, printing or e-mailing a screen shot to the employer.

Philip Gordon, Chair of Littler Mendelson's Privacy and Data Protection Practice Group, is a Shareholder in the Denver office, and Lauren Woon is an Associate in the San Diego 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. Woon at lwoon@littler.com.