A Timely Analysis of Legal Developments

ASAP®

July 2, 2013

Making Sense of the Complex Patchwork Created by Nearly One Dozen New Social Media Password Protection Laws

By Philip L. Gordon and Joon Hwang

The legislative torrent has been virtually unprecedented in the area of workplace privacy. In a single season, spring 2013, *seven* states enacted social media password protection legislation, bringing the total number of states to 11 since Maryland enacted the first such law in May 2012. Bills are pending in more than 20 other states. The current roster of states, dominated by the Rocky Mountain Region and the Far West, is as follows: Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Mexico, Oregon, Utah and Washington. New Jersey appears poised to join this group as the state's legislature amends a bill conditionally vetoed by Governor Christie in May.

The 11 states have created an unwieldy legislative patchwork that will leave many multi-state employers struggling to create a uniform policy. Nonetheless, a thorough review of the legislative hodgepodge does lead to several useful conclusions for employers. These conclusions will be described in detail below.

What conduct by employers do these laws generally prohibit?

One of the only points of uniformity is the basic prohibition: all of these laws prohibit employers from requesting or requiring that applicants or employees disclose their user name, password, or other information needed to access a personal social media account. The notable exception is New Mexico, which applies the prohibition only to applicants.

The states with the most expansive legislation — Illinois, Michigan and Washington — also prohibit employers from requiring that applicants or employees (a) accept a request, such as a Facebook "friend request," that would permit access to restricted content; (b) permit the employer to observe their restricted social media content after they have logged in, *i.e.*, "shoulder surfing"; and (c) change their privacy settings in a manner that would permit the employer to access their restricted social media content. Arkansas and Colorado do not expressly prohibit shoulder surfing. California, Michigan and Oregon do not expressly prohibit requiring an applicant or employee to change privacy settings to permit employer access to restricted social media content. It remains an open question whether state courts will read these slightly narrower statutes and those statutes that prohibit only compelled disclosure of log-in credentials to encompass other methods for circumventing user-created restrictions on access to personal social media.

©2013 Littler Mendelson, P.C. All rights reserved.

A majority of states expand on their access prohibition by applying it not only to social media but also to any personal online account. For example, the most recently enacted law (Nevada) defines "social media account" to mean "any electronic service or account or electronic content, including, without limitation, videos, photographs, blogs, video blogs, podcasts, instant and text messages, electronic mail programs or services, online services or Internet website profiles." The states that most broadly define social media are Arkansas, California, Colorado, Maryland, Michigan, Nevada and Utah. By contrast, Illinois, New Mexico, Oregon, and Washington appear to apply their password protection laws only to social media accounts, excluding other personal online services from their laws' purview.

The legislative patchwork also presents material differences regarding the target of an access request. In virtually all states, an employer is prohibited from seeking access to an applicant's or employee's own restricted social media content. California's law appears to go one step further by prohibiting employers from asking an employee to help obtain access to the restricted social media content of a co-worker.

What are the exceptions to the general prohibition?

The range of exceptions to the general prohibition is even more dizzying than the range of prohibitions. All states, except for Illinois, expressly provide that employers can demand that employees provide log-in credentials to non-personal accounts that are used for the employer's business purposes. The precise formulation of these exceptions varies, but the gist of most of them is that if the employer creates or pays for the account, the general prohibition does not apply. Utah's law takes the exception one step further by permitting employers to request the log-in credentials for a personal social media account that the employee uses to conduct the employer's business.

The uniformity of the "non-personal account" exception evaporates with respect to workplace investigations. On this topic, the states break down into three evenly divided camps. Three states — Illinois, Nevada and New Mexico — have no exception for workplace investigations. Four states — Arkansas, California, Michigan and Utah — have what could be characterized as a broad exception. California's exception, for example, reads as follows: "Nothing in this section shall affect an employer's existing rights and obligations to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding." The remaining four states — Colorado, Maryland, Oregon and Washington — have relatively narrow exceptions for workplace investigations. The Colorado and Maryland laws, for example, permit requests for access to employees' personal social media content only when necessary to investigate violations of securities laws or regulations or potential misappropriation of trade secrets. Notably, the states with a workplace investigation exception appear to permit the employer to require the disclosure only of social media content, not the employee's log-in credentials.

These password protection laws could interfere with the ability of broker-dealers and other employers to comply with statutory or regulatory requirements to monitor business-related posts by employees regardless of whether the account used to post is personal or employer-provided. Consequently, six states have adopted language championed by the securities industry that appears to allow employers to request log-in credentials when required to comply with legal obligations or the rules of a self-regulatory organization such as the Financial Industry Regulatory Authority's (FINRA) rules on the supervision of online communications. These states include Arkansas, Michigan, Nevada, Oregon, Utah and Washington. Washington law, for example, provides as follows: "This section does not prevent an employer from complying with the requirements of state or federal statutes, rules or regulations, case law, or rules of self-regulatory organizations." As noted above, two states — Colorado and Maryland — have adopted narrower exceptions that appear to permit requests for social media content to investigate compliance with securities laws or regulations.

These 11 password protection laws have several other variations. First, half of the states — Arkansas, Illinois, Michigan, New Mexico, Oregon and Utah — expressly state that it is not unlawful for employers to access publicly available social media content. While the remaining five states do not speak to this issue, there does not appear to be any viable basis for an applicant or employee to complain about an employer's access to publicly available social media content. Second, three states — Arkansas, Oregon and Washington — expressly state that employers do not engage in prohibited conduct if they inadvertently acquire social media log-in credentials while monitoring corporate electronic resources as long as the employer does not use the information to access an employee's personal social media. Finally, three states — Michigan, Oregon and Utah — confer on employers immunity from claims based on their failure to request or require that an applicant or employee provide access to restricted, personal social media content.

ASAP® is published by Littler Mendelson in order to review the latest developments in employment law. ASAP® is designed to provide accurate and informative information and should not be considered legal advice.
©2013 Littler Mendelson, P.C. All rights reserved.

What remedies are available under these laws?

The remedial schemes for violation of these laws vary even more substantially than the prohibitions and exceptions. In three states — Arkansas, Nevada and New Mexico — the statutes do not include a remedial provision and do not expressly incorporate one by reference. Two states — California and Colorado — provide no private right of action. The remaining states provide a private right of action with varying caps: Utah and Washington ($500); Michigan ($1,000); Illinois and Maryland (no cap); Oregon (unclear). Four states — California, Colorado, Illinois, and Oregon — expressly create administrative remedies; the other states do not.

What should employers do in response?

Given the prevalence of social media and the increased melding of work and personal life, employers unquestionably will need access to applicants' and employees' personal social media content for a range of legitimate business purposes, including evaluating applicants' job qualifications, conducting workplace investigations and complying with legal requirements. At the same time, as demonstrated above, employers (especially multi-state employers) seeking to establish a uniform policy on access to applicants' and employees' personal social media content are faced with a legislative patchwork that can leave them scratching their heads. The legislative framework will likely become only more variable with more than 20 additional states currently considering social media password protection laws.

Despite these challenges, several guidelines for employers are discernible:

1. **Publicly available social media content is fair game**. Nothing in the password protection laws purports to regulate an employer's access to publicly available social media content. Employers do need to consider other factors when relying on publicly available social media content, such as whether the content is true and whether the content contains information on which an employer cannot lawfully rely for employment purposes.

2. **Employers can use restricted social media content voluntarily provided to the employer**. Employees routinely report voluntarily to HR about troubling social media content posted by co-workers. Nothing in the social media password protection laws restricts an employer's ability to accept and act on this information, even if the employee has restricted access to his or her social media content.

3. **Document the source of all social media content that will be used to justify adverse employment action**. In the event an applicant or employee alleges that an employer obtained restricted social media content in violation of a password protection law, the employer should be in a position to prove that it did not compel the applicant or employee to permit access by prohibited means. The employer can best avoid a "he-said-she-said" battle by producing documents showing the lawful means by which the employer obtained the social media content.

4. **Establish in writing that all accounts used to conduct the employer's business are <u>not</u> personal accounts**. As businesses rely increasingly on social media to attract new business and interact with customers, their employees are creating social media content and making connections that add substantial value to the business. To preserve that value and avoid losing it to a competitor when the employee leaves, employers must take steps to ensure on-going access to these accounts, including the ability to access the accounts at any time by maintaining a record of the log-in credentials. To that end, employers should obtain an employee's agreement, in writing, that the account is not personal when the employee is first assigned responsibility for the account. In this way, the employer eliminates the risk of liability for requiring the employee to disclose his or her log-in credentials and for firing an employee who refuses to cooperate.

5. **Establish a policy that prohibits employees from storing the employer's confidential information in a personal online account**. Under some of the password protection laws, employers arguably could not gain access to the employer's own confidential information stored in an employee's personal, online account, such as a Dropbox account, so that the employer could delete the information or observe the employee deleting the information. Employers can mitigate this risk by establishing a policy which prohibits such storage of the employer's confidential information. In addition, such a policy would provide the basis for the employer to invoke the workplace investigation exception in any password protection law that has this exception when the employer has reason to believe the employee is storing the employer's confidential information in a personal online account in violation of the policy.

ASAP® is published by Littler Mendelson in order to review the latest developments in employment law. ASAP® is designed to provide accurate and informative information and should not be considered legal advice.
©2013 Littler Mendelson, P.C. All rights reserved.

6. **Do not ask applicants for their log-in credentials and consult legal counsel before using other means, such as shoulder surfing, to access applicants' restricted social media content**. While the password protection laws have a range of exceptions applicable to requests for an employee's log-in credentials, these exceptions, such as the exception for workplace investigations, do not apply in the context of the hiring process. Consequently, as a general rule, employers should not seek access to applicants' restricted social media content. Notably, very few private employers currently seek such access. In June 2012, Littler Mendelson's Executive Employer Survey Report found that *99%* of 1,000 C-suite executives, corporate counsel, and human resources professionals surveyed stated that their organization did *not* request social medial log-in credentials as part of the hiring process.

7. **Consult legal counsel before accessing an employee's restricted social media content**. State legislators have recognized that employers can have legitimate reasons to access an employee's restricted social media content — for example, to conduct a workplace investigation or to comply with applicable law, such as FINRA's rules on supervising the social media content of registered representatives. Unfortunately, the password protection laws contain so many variations, nuances and ambiguities that employers will likely need the assistance of legal counsel to reduce the risk of a violation when accessing an employee's restricted social media content for these purposes.

8. **Train supervisors and in-house investigators to be cautious about seeking access to restricted social media content**. Given the newness of the password protection laws, supervisors and in-house investigators may not even be aware that these laws exist. At a minimum, employers should inform supervisors and in-house investigators that (a) access to restricted social media content potentially raises a red flag, and (b) they should consult with the organization's legal department or outside counsel before seeking access to such information.

9. **Support federal password protection legislation that preempts state laws and get involved in the state legislative process**. At this point, the only cure for the tangle of state law restrictions on access to social media content would be a federal law that preempts all of the state laws. However, that solution is nowhere on the horizon. The one federal bill addressing restrictions on employers' access to employees' and applicants' restricted social media content does not mention preemption. Given that, and the fact that bills addressing password protection are pending in many more states, employers should try to influence the legislative debate in an effort to obtain more balanced and uniform legislation that takes employers' interests into account.

Philip L. Gordon chairs Littler Mendelson's Privacy and Data Protection Practice Group and is a Shareholder in the firm's Denver office. Joon Hwang is an Associate in Littler's Northern Virginia office. Littler's Workplace Policy Institute (WPI) has recently issued a report that proposes model state legislation. Employers seeking to influence the debate should contact the WPI at http://www.littler.com/practice-areas/workplace-policy-institute. 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.

© 2013 Bloomberg Finance L.P. Originally published in the July 2, 2013, issue of the Bloomberg BNA Social Media Law & Policy Report. Reprinted with permission. The opinions expressed are those of the author

ASAP® is published by Littler Mendelson in order to review the latest developments in employment law. ASAP® is designed to provide accurate and informative information and should not be considered legal advice.
©2013 Littler Mendelson, P.C. All rights reserved.