A Timely Analysis of Legal Developments

ASAP®

June 10, 2014

Oklahoma and Louisiana Become the Latest States to Enact Social Media Password Protection Laws

By Philip Gordon and Joon Hwang

Weeks after Wisconsin and Tennessee[1] enacted their own legislation aimed at restricting access by employers to applicants' and employees' personal online content, Oklahoma and Louisiana have followed suit, further complicating the patchwork of state password protection laws already in place.[2]

On May 21, 2014, Oklahoma Governor Mary Fallin signed H.B. 2372, making Oklahoma the fifteenth state to impose restrictions on employers' access to the personal social media content of applicants and employees. Two days later, Louisiana Governor Bobby Jindal signed the Personal Online Account Privacy Protection Act (H.B. 340), which prohibits employers and public and private educational institutions from requiring applicants, employees, and students to provide access to their personal online accounts.

Both laws have many of the same elements as laws previously enacted in other states, and are substantially similar to each other. At the same time, each law has some unique and noteworthy features. To ensure compliance, employers with operations in Oklahoma or Louisiana should understand the requirements of each law. Oklahoma's new law becomes effective on November 1, 2014. Louisiana's new law becomes effective on August 1, 2014.

The General Prohibitions

Both new laws prohibit employers from requesting or requiring that applicants or employees disclose a username, password, or other means of authentication for their online accounts. The Oklahoma law also prohibits an employer from observing the applicants' or employees' restricted online content after they have accessed the account (*i.e.*, "shoulder surfing"). Unlike many of the other password protection laws, neither law expressly prohibits employers from requesting or requiring that an applicant or employee accept a "friend" request, change privacy settings to permit access by the employer, or otherwise divulge personal online content. The absence of these express prohibitions makes these new laws among the narrowest in the country.

1 *See* Philip Gordon and Joon Hwang, *Tennessee Joins the Growing List of States Limiting Employers' Access to Personal Online Content*, Littler ASAP (May 13, 2014).

2 *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).

In line with the majority of similar laws, both new laws define "personal online social media account" far more broadly than just social media. Specifically, both laws apply to any online account, including e-mail, instant messaging and media-sharing accounts, but with a significant narrowing exception. In the words of the Oklahoma statute, the account must be used "exclusively for personal communications to be protected." The Louisiana law expands on this concept by stating that the law does not apply to any account used "for either business purposes of the employer . . . or to engage in business-related communications." This carve-out further narrows the scope of the Oklahoma and Louisiana laws.

Both laws prohibit employers from taking adverse action based on an applicant's or employee's rejection of a request for their user name, password or other authentication information. The Louisiana law is particularly broad in this regard, prohibiting not only discharge, discipline, and refusal to hire, but also "otherwise penaliz[ing] or threaten[ing] to penalize" an employee or applicant for failing to disclose log-in credentials. By contrast, the Oklahoma law prohibits only "retaliatory personnel action" that "materially and negatively affects the terms and conditions of employment" in addition to refusal to hire. In what appears to be a drafting error, the plain language of the Oklahoma law does not prevent employers from taking adverse action based on an employee's or applicant's refusal to disclose "other means of authentication" for accessing a personal online social media account or refusal to permit shoulder surfing.

Exceptions to the General Prohibitions

Both laws have similar and significant exceptions aimed at protecting employers' legitimate business interests. For instance, nothing in the new laws prevents employers from requesting or requiring that employees: (a) disclose log-in credentials for any employer-provided system or equipment; or (b) divulge content in any accounts or services provided by the employer or by virtue of the employee's employment relationship with the employer. The Oklahoma law goes one step further by expressly allowing employers to review or access personal online accounts that employees access while using the employer's computer system, information technology network, or electronic communication device. However, before doing so, Oklahoma employers should confer with legal counsel regarding the potential implications of such searches under federal law.

Both laws contain relatively broad exceptions for workplace investigations. For example, neither law prohibits employers from conducting an investigation into misappropriation of proprietary information, violations of the law or workplace policies where the investigation arises from the receipt of specific information about activity on the employee's personal account. Unlike most other password protection laws, these new laws expressly state that an investigation includes requiring an employee or applicant "to share the content that has been reported in order to make a factual determination," albeit the employer still may not obtain the employee's or applicant's log-in credentials.

Both laws contain a potpourri of other exceptions and express carve-outs that are helpful for employers. Both laws provide that an employer is not liable if it inadvertently obtains employees' or applicants' user names, passwords, or other authentication information when monitoring corporate electronic resources, provided employers do not use this information to access the individual's personal online account. Both laws expressly permit employers to comply with a duty to screen applicants before hiring, or to monitor or retain employee communications, where the duty arises out of state or federal statutes, rules or regulations, case law, or rules of self-regulatory organizations, such as FINRA. Furthermore, the Louisiana law explicitly states that employers are not prohibited from viewing, accessing, or utilizing information about employees or applicants that is publicly available. The Louisiana law also states that it does not prohibit or restrict employees or applicants from self-disclosing any username, password, or other authentication information to employers to allow access to their personal online accounts.

Enforcement

The two laws vary most significantly in their remedial schemes.

The Oklahoma law, like similar laws of other states, provides for a private cause of action for aggrieved employees or applicants. However, employees and applicants must file a civil action within six months after the alleged violation, a relatively short statute of limitations. Although employees and applicants may seek injunctive relief to restrain an employer from committing any further violations, such relief is available only on a showing of a violation by clear and convincing evidence, which is a heavy evidentiary burden. Further, aggrieved employees and applicants may recover only liquidated damages of $500 per violation. Punitive damages and emotional distress damages are not recoverable. Moreover, a violation may not serve as the basis for a claim under any of Oklahoma's public policy torts.

In stark contrast to Oklahoma's detailed remedial scheme, Louisiana's new law, on its face, does not provide for a private cause of action for aggrieved employees or applicants, nor does it provide any mechanism for administrative enforcement. Accordingly, it is unclear how the new law will be enforced.

Recommendations for Employers

A growing number of states are adopting legislation aimed at limiting employers' access to personal online content. As of the date of this article, 16 states—Arkansas, California, Colorado, Illinois, Louisiana, Maryland, Michigan, New Jersey, New Mexico, Nevada, Oklahoma, Oregon, Tennessee, Utah, Washington, and Wisconsin—have enacted password protections laws. The laws in each of these states have their own distinct features, which places the onus on employers, especially those with multistate operations, to implement sufficient protocols to ensure compliance. Because of the state-to-state variations, employers should consult with legal counsel before requesting or requiring access to non-public, personal online content. In general, the best practice is not to seek access to personal online content except where there is a strong business interest for doing so that is recognized in the applicable password protection law, such as the interest in conducting a workplace investigation or complying with another applicable law, such as FINRA regulations.

Phillip Gordon, Co-Chair of Littler's Privacy and Background Check Practice Group, is a Shareholder in the firm's Denver office, and Joon Hwang is an Associate in the Northern Virginia 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 Mr. Hwang at jhwang@littler.com.