A Timely Analysis of Legal Developments

ASAP®

May 13, 2014

Tennessee Joins the Growing List of States Limiting Employers' Access to Personal Online Content

By Philip Gordon and Joon Hwang

Legislation to restrict employers' access to applicants' and employees' personal online content continues its rapid expansion in 2014.[1] Three weeks after Wisconsin became the 13th state to adopt its own social media password protection law, on April 29, 2014, Tennessee Governor Bill Haslam signed his own state's password protection law. This new law goes into effect on January 1, 2015.

The Tennessee law, known as the Employee Online Privacy Act of 2014 (S.B. 1808), has many of the same prohibitions and exceptions found in similar state laws. There are, however, some key differences that render Tennessee's new law broader in certain aspects, while narrower in others. Employers with operations in Tennessee should understand the new law's basic requirements as well as its differences from similar laws, as described in more detail below. Because the new law applies to employers with one or more employees, even the smallest Tennessee employers must comply with these new restrictions.

General Prohibitions

Like the legislation enacted in all other states, Tennessee's new law prohibits an employer from requesting or requiring that applicants or employees disclose their passwords for personal internet accounts. Tennessee's law also prohibits employers from requiring that applicants or employees: (a) add the employer to the employee's or applicant's list of contacts associated with the personal internet account (*e.g.*, accept a request, such as a Facebook "friend request," that would permit access to restricted online content); or (b) permit the employer to observe their restricted online content after they have accessed an online account (*i.e.*, "shoulder surfing"). Notably, the prohibitions on access are limited to these three specific actions. The new law, on its face, does not prohibit other methods for circumventing user-created restrictions on access to personal online content, such as asking applicants to change their privacy settings in a manner that would permit the employer to access their restricted social media account.

The new law is in line with the majority of similar laws insofar as it defines "personal internet account" far more broadly than just social media. Specifically, Tennessee's new law applies to "any

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 (July 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).

electronic medium or service where users may create, share or view content, including, emails, messages, instant messages, text messages, blogs, podcasts, photographs, videos or user-created profiles." The new law carves out from this broad definition accounts created, maintained, used or accessed by an employee or applicant for business-related communications or for a business purpose of the employer.

In addition, the law broadly prohibits employers from taking any adverse action against employees, failing to hire applicants, or otherwise penalizing an employee or applicant for not permitting access to their personal online account in a manner prohibited by the statute. The Tennessee law very broadly defines "adverse action" to include "discharge, threaten, or otherwise discriminate against an employee in any manner that affects the employee's employment, including compensation, terms, or conditions, location, rights, immunities, promotions, or privileges." This definition, combined with the new law's prohibition against "otherwise penaliz[ing]" employees or applicants for engaging in protected conduct, means that Tennessee's law prohibits a broader range of adverse employment actions than is found in any similar law.

Despite this breadth, the 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. Consequently, it currently is unclear how the new law will be enforced.

Exceptions to the General Prohibitions

In line with the majority of states that have enacted password protection laws, Tennessee's law provides certain exceptions to protect employers' legitimate business interests. For instance, employers may implement and enforce policies pertaining to the use of (a) any electronic communication device, account or service provided, or paid for, by the employer; or (b) a personal account used for the employer's business purposes. The new law also recognizes an employer's right to control and monitor employees' use of corporate electronic resources.

Importantly, the new law contains a broad exception for workplace investigations. Under this exception, employers can require employees to disclose content contained in a personal online account if that content (a) bears on whether the employee has violated the law or company policy, or (b) constitutes confidential information of the employer that has been transferred to the employee's personal online account without authorization. In addition, financial services companies subject to NASDAQ rules and/or securities regulations may monitor employees' personal online accounts and screen applicants' personal online accounts as may be necessary to comply with applicable law and regulations.

Unlike some similar laws, the Tennessee law does not confer immunity on employers who inadvertently obtain passwords for a personal online account. However, the new law does not impose a duty on employers to search or monitor activity in an employee's personal internet account and specifically immunizes Tennessee employers from liability for "failure to request or require that an employee or applicant grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal Internet account."

The new law explicitly permits employers to access and use publicly available information about job applicants and current employees. However, employers should note that their use of publicly available social media content to impose discipline or make 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.

Recommendations for Employers

In general, employers should carefully evaluate whether access to restricted social media or other online content is needed during the hiring process. If an employer believes such information is valuable, it must keep apprised of new legislation, such as Tennessee's law, that could make such requests unlawful. Employers in Tennessee and in the other 13 states that have enacted password protection laws—Arkansas, California, Colorado, Illinois, Maryland, Michigan, New Jersey, New Mexico, Nevada, Oregon, Utah, Washington, and Wisconsin—generally should not seek access to personal online content except where there is a strong business interest that is recognized in the applicable password protection law, such as the interest in conducting a workplace investigation. In addition, because of the significant state-to-state variations in these laws, employees authorized to ask applicants or employees for access to personal online content should be trained to consult with in-house or outside counsel before making such requests.

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.