A Timely Analysis of Legal Developments

ASAP®

March 30, 2015

Virginia's Password Protection Law Continues the Trend Toward Increasing Legislative Protection of Personal Online Accounts

By Philip Gordon and Joon Hwang

As many state legislatures open their 2015 sessions, Virginia has become the first this year—and most likely not the last—to continue the legislative trend towards protecting applicants' and employees' personal online accounts. As the 19th state to enact password protection legislation, Virginia has added even more complexity to the patchwork of state law restrictions on such access.[1] Governor Terry McAuliffe signed H.B. 2081 into law on March 23, 2015, and the new law becomes effective on July 1, 2015.

In keeping with Virginia's reputation as an "employer-friendly" state, Virginia's new law, as a whole, is limited when compared to similar state laws. Nonetheless, the law still imposes substantial restrictions on access by Virginia employers to applicants' and employees' personal online accounts. Public employers in Virginia should note that the new law applies to them as well as to private employers.

General Prohibitions

Like the legislation enacted in all other states, Virginia's new law generally prohibits an employer from requesting or requiring that applicants or employees disclose the username and passwords for their social media accounts. The law also prohibits any employer from requiring that applicants or employees add the employer's employee, supervisor, or administrator to the list of contacts associated with their social media account (*e.g.*, accept a request, such as a Facebook "friend request," that would permit access to restricted online content).

Virginia's law, however, is noticeably silent on prohibitions against other methods for circumventing user-created restrictions on access to social media accounts present in most other such laws. For example, Virginia's law does not prohibit employers from observing applicants' or employees' restricted online content after they have accessed an online account (*i.e.*, "shoulder surfing"). The law also does not prohibit employers from asking applicants or employees to change their privacy settings in a manner that would permit the employer to access their personal online account.

---

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).

In line with most similar laws, the new law defines "social media account" broadly to include any "electronic medium or service where users may create, share, or view user-generated content, including, without limitation, videos, photographs, blogs, podcasts, messages, emails, or website profiles or locations." Thus, although the law on its face applies only to "social media" accounts, in reality, it applies to virtually all personal online accounts.

The law expressly excludes from its scope accounts that were opened for the employer's benefit or to impersonate the employer. More specifically, the law excludes online accounts that satisfy any of the following criteria: (a) were opened or set up by an employee for the employer; (b) were provided to an employee by an employer, including the employer's email account or other software program owned or operated exclusively by an employer; or (c) were set up by an employee to impersonate an employer through the use of the employer's name, logos, or trademarks. Unlike some password protection laws, Virginia's law does not exclude personal online accounts that an employee uses for work but were established independently of any involvement from the employer.

In addition to the prohibitions described above, the law broadly prohibits employers from taking action against or threatening to discharge, discipline, or "otherwise penalize" employees, or failing to hire applicants, for not permitting access to their personal online account in a manner prohibited by the statute. The "otherwise penalize" language is broad and appears to effectively prohibit almost any adverse action that affects the employee's employment, including compensation, terms or conditions of employment, location of work, promotions, or privileges.

On its face, Virginia's law does not provide for a private cause of action for aggrieved employees or applicants, nor does it provide any mechanism for administrative enforcement. As a result, it currently is unclear how the new law will be enforced.

Exceptions to the General Prohibitions

In line with the majority of password protection laws, Virginia's new law provides certain exceptions to protect employers' legitimate business interests. For instance, the new law contains an exception for workplace investigations. Under that exception, employers can require employees to disclose their usernames and passwords for their personal online accounts if the account activity bears on whether the employees have violated the law or company policy. Notably, most similar laws permit employers to request access to content in an employee's personal online account for investigative purposes, but unlike Virginia's law, those other laws do not permit requests for the user's log-in credentials. Virginia's law, however, prohibits employers from using log-in credentials for any purpose other than the investigation that justified the request.

Like some similar laws, Virginia's law also expressly permits 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 the Financial Industry Regulatory Authority (FINRA). The law also confers immunity on employers who inadvertently obtain usernames, passwords, or other log-in information for an employee's personal online account where that information is stored on employer-owned equipment or captured when the employer monitors its corporate electronic resources, provided the employer does not use the log-in information to access the employee's personal online account.

The new law explicitly permits employers to access and use publicly available information about applicants and 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

Virginia's new law is relatively narrow when compared to laws enacted in other states. However, the best practice would be 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. By the same token, an employer who suspects that content stored in a personal online account may be relevant to an investigation should consider the specific prohibitions and exceptions established by the jurisdiction's law before attempting to access the account.

As of this writing, the following states have enacted password protection laws: Arkansas, California, Colorado, Illinois, Louisiana, Maryland, Michigan, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Virginia, Washington, and Wisconsin. The laws in each of these states have their own distinct features, which places the burden on employers, especially those with operations nationwide, to implement sufficient protocols to ensure compliance. 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.