A Timely Analysis of Legal Developments

ASAP®

January 4, 2013

Michigan's New "Internet Privacy Protection Act" Sets Limitations for Employers and Employees

by William Balke and Philip Gordon

On December 28, 2012, Michigan joined California,[1] Illinois,[2] and Maryland[3] in enacting a social media password protection law when Governor Rick Snyder signed the "Internet Privacy Protection Act" (IPPA or the "Act"). In an accompanying statement, the governor declared that "cyber security is important to the reinvention of Michigan, and protecting the private internet accounts of residents is a part of that," and that "potential employees and students should be judged on their skills and abilities, not private online activity." To accomplish these objectives, the IPPA, like the other states' social media legislation, generally prohibits employers from gaining access to applicants' or employees' personal social media accounts. The Act, however, also permits employers to access employees' use of employer equipment and systems and allows for investigations, under certain circumstances, of employees' personal social media accounts. While relatively straightforward, the Act will require businesses operating in Michigan to grapple with a range of interpretive challenges.

Initially, the IPPA applies to Michigan public and private educational institutions and public and private sector employers. The emphasis of this ASAP is on the Act's application to Michigan employers, defined by the Act as a "person, including a unit of state or local government, engaged in a business, industry, profession, trade, or other enterprise in this state and includes an agent, representative, or designee of the employer." Thus, all employers, regardless of size, are subject to the Act.

The IPPA regulates employers' access to an applicant's or employee's "personal internet account," which is defined as "an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data." Accordingly, the Act applies not just to social media accounts but to all internet-based accounts, including e-mail and cloud storage accounts.

The Act identifies three straightforward prohibitions on employers with respect to such accounts. First, employers cannot request an applicant or employee to grant it "access information," *i.e.*,

1 See Philip Gordon and Lauren Woon, *California's New Social Media "Password Protection" Law Takes a More Balanced Approach by Accounting for Employers' Legitimate Business Interests*, Littler ASAP (Oct. 10, 2012).

2 See Philip Gordon and Kathryn Siegel, *Illinois' New Social Media Password Protection Law Handicaps Employers' Legitimate Business Activities*, Littler ASAP (Aug. 7, 2012).

3 See Philip Gordon, Steven Kaplan, and Ashley Sims, *Legislation Roundup: Maryland "Facebook Law" Raises New Obstacles for Employers and Other Significant Maryland Developments*, Littler ASAP (Apr. 17, 2012).

"user name, password, login information, or other security information that protects access to a personal internet account," in order to gain access to any of the applicant's or employee's personal internet-based accounts. Second, the Act bars employers from requesting an applicant or employee to "allow observation of" his or her personal internet account, a practice commonly called "shoulder surfing." Third, the Act prohibits employers from requesting an applicant or employee to "disclose" information that would allow access to or observation of his or her personal internet account, thereby barring employers from reviewing content without asking for log-in credentials and without shoulder surfing. Consistent with these prohibitions, an employer cannot discharge, discipline, fail to hire, or otherwise penalize an applicant or employee for failing to 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.

While the Act expressly addresses the personal internet accounts of applicants and employees, it does not prohibit an employer from asking an employee to help the employer view content in another employee's, or in an applicant's, personal account. The Act's prohibitions appear to reach only to requests made to, and the observations of, the applicant or employee regarding his or her personal internet account. Given that employees routinely report social media conduct of coworkers that may violate corporate policy or is suspected to be unlawful, this apparent limitation is critical for employers seeking to investigate an employee's internet misconduct or compromising internet postings by a job applicant. In addition, the IPPA also does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an applicant or employee that can be obtained without any required access information or that is available in the public domain.

The IPPA's express exceptions also create important gaps in the facially broad prohibitions regarding employees. In this regard, the Act carefully carves out the employer's own systems and equipment from the Act's purview. The IPPA permits an employer to request or require an employee to disclose access information to the employer to permit the employer to gain access to or operate an electronic communications device paid for in whole or in part by the employer, as well as to any account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes. An employee may also be disciplined or discharged for transferring the employer's proprietary or confidential information or financial data to an employee's personal internet account without the employer's authorization.

An employer may also conduct an investigation or require an employee to cooperate in an investigation under two circumstances. First, "if there is specific information about activity on the employee's personal internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct." This exception would, for example, permit an employer to ask an employee for log-in credentials where a coworker reports a social media post that threatens workplace violence or contains racially derogatory comments about the coworker. The second investigation exception applies if the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal internet account.

An employer also has the right to restrict or prohibit an employee's access to certain websites while he or she is using an electronic communications device paid for in whole or in part by the employer, or the employer's network or resources, in accordance with state and federal law. Finally, an employer may also monitor, review, or access electronic data stored on an electronic communications device paid for in whole or in part by the employer, or traveling through or stored on an employer's network, in accordance with state and federal law.

The IPPA's prohibitions do not apply when an employer has a duty under federal law, or to comply with a self-regulatory scheme established under the Securities and Exchange Act, to screen applicants or monitor or retain certain employee communications. Further, actions that are taken to comply with requirements of federal or Michigan state law are an affirmative defense to any claimed violation of the Act.

The Act does leave open the question of its effect on employers involved in litigation with applicants and current or former employees. While the Act does not appear to impose any restriction on an employer's requesting production of social media content during discovery, the discovery of "access information" from a current employee or applicant litigant likely would be precluded. However, the Act's failure to define the term "employee" leaves this question open regarding former employees. Michigan courts likely will be called on to resolve this issue given the importance of social media content in many employment-related lawsuits. Accordingly, employers engaged in employment litigation should carefully evaluate the Act's impact on information requests made during the course of discovery.

Importantly, the Act expressly "does not create a duty" for employers to search or monitor activity of an employee's personal internet account. The Act expressly eliminates an employer's liability for failing to request that an applicant or employee grant access to, allow observation of,

or disclose information that allows access to or observation of his or her personal internet account. In other words, the victims of workplace violence presaged by the perpetrator-employee's ranting social media content could not assert a negligence claim against the employer based on the employer's failure to ask the perpetrator for access to his or her personal social media account. While the exact contours of these provisions are not entirely clear, they provide important protections for employers.

The IPPA's remedial provisions, though limited, do have the potential to deter violations. Most importantly, the Act exposes individual employees to criminal prosecution for a misdemeanor offense, but the punishment is limited to a fine of not more than $1,000. Similarly, the Act's civil remedy provisions caps damages at $1,000 and an award of attorneys' fees and costs. Potential plaintiffs must serve a written demand on the employer at least 60 days before asserting the claim. This provision gives employers the opportunity to forestall a claim by offering $1,000 in response to a demand.

In sum, Michigan employers should be able to obtain information about employees' internet conduct in many circumstances where they need it. However, before investigating an employee's or applicant's personal internet activity, they should carefully scrutinize the precise contours of the IPAA's prohibitions to avoid exposing human resources professionals to a potential misdemeanor prosecution.

William Balke is a Shareholder in Littler Mendelson's Detroit office, and Philip Gordon, Chair of the firm's Privacy and Data Protection Practice Group, is a Shareholder in the Denver office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, Mr. Balke at wbalke@littler.com, or Mr. Gordon at pgordon@littler.com.