A Timely Analysis of Legal Developments

ASAP®

April 2012

Legislation Roundup: Maryland "Facebook Law" Raises New Obstacles for Employers and Other Significant Maryland Developments

By Philip Gordon, Steven Kaplan, and Ashley Sims

Maryland has become the first state to pass a bill, the User Name and Password Privacy Protection Act (SB 433/HB 964) (the "Act"), that bans employers from asking employees and applicants for social media passwords and login information. Specifically, the bill would prohibit an employer from taking or threatening any form of adverse action based on an employee's or applicant's refusal to provide a user name or password to a personal account accessed through a communications device. Governor Martin O'Malley likely will sign the bill into law in May 2012.

The impetus for the bill appears to have been a media frenzy, and a lawsuit filed by the American Civil Liberties Union, after public revelations that the Maryland Department of Corrections had asked an applicant, as part of the hiring process, to provide his username and password to his Facebook page. The Department made the request to check whether the applicant had any gang connections. Although the applicant acquiesced in the request, he claimed to have been "mortified" that his potential employer could violate his privacy rights without recourse. He later enlisted the ACLU, and other groups, who pressured the Maryland General Assembly to pass this bill.

Under the Act, which will take effect on October 1, 2012 if signed, Maryland businesses will be prohibited from requiring, or even asking, that applicants or employees disclose their user names or passwords for "any personal account or service" accessed through "computers, telephones, personal digital assistants, and other similar devices." In other words, the prohibition extends far beyond Facebook and other social media sites to include personal e-mail accounts, personal online banking accounts, and any other online communications or service account.

The business community opposed this bill principally because it potentially limits an employer's sources of information when investigating inappropriate employee behavior such as discrimination, harassment, defamation, and/or general negative comments about the employer, the employee's coworkers, or the employer's customers. The bill also prevents employers from using online social networking sites to verify an employee's or applicant's work or education history to the extent such information is available only on restricted access social media sites.

Significantly, the bill does not authorize applicants or employees to sue an employer that violates the Act. Nonetheless, it is possible that an employee terminated in violation of the law could have a claim for wrongful discharge in violation of public policy.

Littler
Employment & Labor Law Solutions Worldwide™

Littler Mendelson, P.C. • www.littler.com • 1.888.littler • info@littler.com

While the law seems overly broad at first blush, it is critical for employers to understand the types of conduct that the law does not prohibit. Some of these exceptions are expressed in the statute itself; others are implicit.

1. **Access to Employer's Internal Systems:** The Act expressly permits employers to require that employees disclose log-in credentials "for accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems." In other words, employees cannot rely on the law to prevent employers from gaining access to information stored on the employer's own information systems.
2. **Violations of Securities or Financial Laws, or Regulatory Requirements:** If an employer receives information that an employee is using a personal online account for business purposes, the law "does not prevent" an employer from conducting an investigation to ensure that the employee is complying with "securities or financial law, or regulatory requirements." This exception appears intended to apply in a situation where an employee of a financial services company uses a personal online account to trade securities or engage in other financial transactions on the employer's behalf using a personal online account. The exception, however, does not appear to permit employers to require that an employee disclose log-in credentials for investigations into other forms of suspected misconduct, such as harassment or discrimination.
3. **Protection of Trade Secrets:** If an employer receives information that an employee has downloaded the employer's proprietary information, without authorization, to a personal online account, the law "does not prevent" an employer from conducting an investigation into such suspected misconduct.
4. **Passwords to Devices:** While the Maryland law bars employers from requesting log-in credentials for "accessing a personal account or service," the law does not prohibit employers from requesting or requiring log-in credentials to access an employee's personal device, such as a smartphone or tablet. This distinction is critical as employers increasingly are implementing "Bring-Your-Own-Device" policies that permit an employee to use a personal device to conduct the employer's business.
5. **Nonpersonal Accounts:** The Act protects log-in credentials only for "personal" accounts. Maryland employers should clearly define which accounts are personal and which are nonpersonal. For example, if an employee uses a corporate e-mail address to establish a LinkedIn profile or Twitter account, the employer should ensure that employees know from the outset that such an account is "nonpersonal" for purposes of the Maryland law.
6. **Information Received from Cooperating Employees.** Employers may commonly receive employees' social media content from coworkers who have access to the employee's restricted social media site (as a Facebook "friend," for example) and who are offended by the post. The Act does not prevent an employer from accepting voluntary offers of such information. The Act also apparently would not prohibit an employer from asking a coworker with access to an employee's restricted site to provide information posted on the site. However, an employer should consult counsel before doing so because of possible risks under other laws.

Because the Act's restrictions on its face arguably apply only to the disclosure of log-in credentials, it remains to be seen through judicial interpretation whether the Act's restrictions bar an employer from, for example, asking an employee or applicant to log into a personal account without disclosing the log-in credentials to the employer so the employer can observe the content of the personal account or asking an employee or applicant to print the content of a personal account. Before an employer chooses this route, they should speak with their employment counsel to educate themselves about the legal risks of doing so. While Maryland is the first jurisdiction to enact this legislation, it is not likely to be the last. Indeed, bills proposing similar restrictions currently are pending in various states, including but not limited to California, Illinois, Minnesota, New York, and Washington. In addition, U.S. Senator Richard Blumenthal (D–CT) has stated his plan to introduce similar legislation "in the very near future."

Other Legislative Changes in this Session of the General Assembly

The Jury Service Act

On April 11, 2012, Governor O'Malley signed into law a bill (SB 16/HB 353) that prohibits employers from discharging, coercing, intimidating, or threatening to discharge an employee that loses work time because he or she responded to a jury service summons. In particular, the Act

protects employees that serve four or more hours of jury duty in any given day, including travel time, by expressly forbidding employers from requiring such employees to work that day.

This means that employers cannot require employees serving a half-day or more of jury duty to report to work when their service ends. However, the Act does not prevent employees from returning to work or picking up a shift on a day they serve jury duty if the employee wishes to do so. The Act also provides a penalty for employers that violate the statute (a fine of up to $1,000).

Employers in Maryland should review their handbooks and jury leave policies to ensure that they are compliant with this new law. Although an employee can voluntarily choose to return to work, employers should be careful about allowing employees to work on such days because the language of the Act also includes "coercing" employees to work.

Revisions to the Workplace Fraud Act

The Maryland General Assembly enacted the Workplace Fraud Act of 2009 to penalize employers that misclassify employees as independent contractors. Specifically, the law targeted the construction and landscaping industries where employers routinely kept employees "off their books" by classifying them as independent contractors. This common maneuver allowed employers in these industries to avoid payroll taxes and contributions to the state's unemployment and workers' compensation insurance funds. In essence, the Act created a statutory presumption that an employer/employee relationship exists anytime payment is made to an individual for work performed.

Based on concerns brought forth by the business community, the General Assembly created an exception to the statutory presumption that an employee/employer relationship existed. In particular, the presumption will not apply when:

- the employer and business entity have a written contract that:
  - describes the nature of the work to be performed;
  - describes the remuneration to be paid; and
  - includes an acknowledgement by the independent contractor that it will properly withhold, remit, and report payroll taxes, pay unemployment insurance, and maintain workers' compensation insurance for all of its employees;
- the business entity signs an affidavit indicating that it is an independent contractor who is available to work for other business entities;
- the business entity has a State Department of Assessment and Taxation certificate of good standing;
- the business entity holds all occupational licenses required by State and local authorities for the work performed; and
- the employer provided notice of the Act to each independent contractor it employs.

Employers in these affected industries should review their independent contractor agreements in order to take advantage of these amendments.

Maryland Creates a Union-Employee Privilege Under Limited Circumstances

Under Maryland law (SB 797), certain communications between an employee and a union agent will now be privileged. In other words, the new law will extend certain facets of the attorney-client privilege to the union-employee relationship.

Protected Communications

Any communication or information imparted in confidence by an employee to a labor union and/or its agent while the labor union or agent was acting in a representative capacity concerning an employee grievance is protected under the statute. However, the communication or information must be relevant to the employee's grievance proceeding.

Unprotected Communications

Despite the rather broad protections offered to employees, there are several important exceptions of which employers should be aware:

- Communications germane to a criminal proceeding are not protected.
- The union or agent may be compelled to disclose the facts underlying a communication, but not the communication itself.

- The union or agent must disclose the communication if disclosure is reasonably necessary to prevent death or bodily harm.
- The union or agent may disclose the communication if it reasonably believes:
  - the disclosure is necessary to prevent the employee from committing a crime, fraud, or violation of the collective bargaining agreement between the employer and the union. However, the union or agent may only disclose if the employee's expected action is reasonably certain to cause injury to the property (tangible and/or financial) of any person or entity;
  - disclosure is necessary to prevent, remedy, or mitigate injury to an entity's property (tangible and/or financial) resulting from a criminal act completed or intended by employee;
  - disclosure is necessary to secure legal advice regarding compliance with a court order or the CBA;
  - disclosure is necessary to establish a claim or defense in a legal action or dispute between the employee and the union;
  - disclosure is necessary to comply with a court order or the CBA;
  - the communication is an admission that the employee committed a crime;
  - disclosure is necessary in any court, arbitration, and/or agency proceeding against the union or the union's agent;
  - the union obtained written or oral consent from the employee to disclose the communication; or
  - the employee waived the communication's confidentiality.

In addition, the law includes a "savings clause," which means that, if a union is required to disclose the communication under the National Labor Relations Act or another federal statute, federal law controls.

What The New Law Means for Maryland Employers

Employers should educate themselves, or speak with their employment counsel, regarding what communications and information unions are required under federal and state law to disclose to employers in the context of a grievance proceeding. Until courts have had the opportunity to interpret the savings clause, it is likely that unions and agents will err on the side of claiming most employee communications as privileged.

Governor O'Malley is expected to sign the social media, workplace fraud, and protected communications bills into law in May 2012 and they will become effective on October 1, 2012.

Philip Gordon, Chair of Littler Mendelson's Privacy and Data Protection Practice Group, is a Shareholder in the Denver office; Steven Kaplan and Ashley Sims are Associates in the Washington, D.C. 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, Mr. Kaplan at skaplan@littler.com, or Ms. Sims at easims@littler.com.