A Timely Analysis of Legal Developments

ASAP®

April 14, 2014

Wisconsin Adopts Password Protection Law

By Jonathan Levine and Adam Tuzzo

Wisconsin has become the thirteenth state to enact a law limiting the circumstances under which employers may request or require access to the personal internet accounts of applicants and employees. The 2013 Wisconsin Act 208,[1] which amends the Wisconsin Fair Employment Act (WFEA) and will be enforced by the Department of Workforce Development (DWD), prohibits employers from "requesting or requiring" employees and applicants to provide "access information" for their "personal Internet account" or "to otherwise grant access to or allow observation of that account." A "personal Internet account" is any "Internet-based account that is created and used by [an employee or applicant] ***exclusively for purposes of personal communications***." "Access information" means the "password or any other security information" that protects access to a personal Internet account. Access information does not include an employee's personal e-mail address; the Act expressly permits employers to require employees to disclose that information. In addition to prohibiting these requests for access information and access, the new law, as a general rule, prohibits employers from discriminating or retaliating against (*e.g.*, discharging or refusing to hire) an employee or applicant who exercises their rights under the law.

While the law primarily protects the privacy of employees and applicants, it also offers employers a limited degree of protection. For example, employers may require employees to disclose access information in order for the employer to gain access to or operate any "electronic communications device supplied or paid for in whole or in part by the employer" or to gain access 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." In addition, employers may require an employee to grant access to or allow observation of the employee's personal Internet account (but may not require the employee to disclose access information for that account) when conducting an investigation or requiring an employee to cooperate in an investigation of:

- "[A]ny alleged unauthorized transfer of the employer's proprietary or confidential information or financial data to the employee's personal Internet account, if the employer has reasonable cause to believe that such a transfer has occurred."
- "[A]ny other alleged employment-related misconduct, violation of the law, or violation of the employer's work rules as specified in an employee handbook, if the employer has reasonable cause to believe that activity on the employee's personal Internet account relating to that misconduct or violation has occurred."

1 The full text of the law may be viewed by clicking here.

Finally, employers are not prohibited from doing, among other things, any of the following:

- "Complying with a duty to screen applicants for employment prior to hiring or a duty to monitor or retain employee communications that is established under state or federal laws, rules, or regulations or the rules of a self-regulatory organization . . ."
- "Viewing, accessing, or using information about an employee or applicant for employment that can be obtained without access information or that is available in the public domain."
- "Requesting or requiring an employee to disclose the employee's personal electronic mail address."

The law does not apply to an employee's personal Internet account or an electronic communications device of employees who provide "financial services" and use the account or device to conduct business if their employer is subject to certain "content, supervision, and retention requirements" imposed by federal securities laws and regulations or by the rules of certain self-regulatory organizations.

The law also recognizes that employers may inadvertently obtain access information through devices or programs that monitor the employer's network or through devices supplied or paid for in whole or in part by the employer. In such cases, employers will avoid liability as long as the access information is not used to access the employee's personal Internet account.

Union employers with collective bargaining agreements that contain provisions inconsistent with the law may continue to enforce those provisions until the date those agreements expire or are extended, modified, or renewed, whichever occurs first.

Because the meaning and impact of the law's requirements and exceptions will evolve over time, employers should approach access issues with care and on a case-by-case basis. For example, there may be litigation over whether the phrase "***exclusively for purposes of personal communication***" in the definition of "personal Internet account" means that mixed-use Internet-based accounts (*e.g.*, those used by an employee for both personal and business communications) are not covered by the law at all. Employers should also keep in mind other risks associated with monitoring the social media activity of employees and applicants. Increasingly, employers are being accused of using such information to discriminate on any variety of bases—*e.g.*, age, race, disability, sexual orientation, use of lawful products—prohibited by state, federal and local laws.

Jonathan Levine is a Shareholder, and Adam Tuzzo is an Associate, in Littler's Milwaukee office. If you would like further information, please contact your Littler attorney at 1.888.LITTLER, info@littler.com, Mr. Levine at jlevine@littler.com, or Mr. Tuzzo at atuzzo@littler.com.