Washington Enacts Social Media Privacy Law

By Bryan P. O'Connor

June 4, 2013

Washington Governor Jay Inslee on May 21, 2013, signed Washington's social media privacy bill, banning employers from requesting user names and passwords of current or prospective employees' personal social media accounts. The bill (SB 5211) was passed unanimously by the Washington State Legislature in April 2013. Other states to have enacted such legislation include Arkansas, California, Colorado, Illinois, Maryland, Michigan, New Mexico, Oregon, and Utah. The new Washington law is effective on July 28, 2013.

The new law broadly defines "employers" to include any person, firm, corporation, partnership, business trust, legal representative or other business entity that engages in any business, industry, profession or other activity in Washington and employs one or more employees. The law covers the state, state agencies and political subdivisions.

The new law provides that employers may *not*:

(1) ask for login information (including user name and password) for an employee's or applicant's personal social networking account;

(2) engage in "shoulder-surfing" (meaning employers are prohibited from requesting, requiring, or otherwise coercing an employee or applicant to access his or her personal social networking account in the employer's presence in a manner that enables the employer to observe the contents of the account);

(3) compel or coerce an employee or applicant to add a person, including the employer, as a friend or contact associated with the employee's or applicant's social networking account; or

(4) request, require or cause an employee or applicant to alter his or her settings, which may affect a third party's ability to view the contents of the account.

Further, the law prohibits employers from taking adverse action against an employee or applicant because of the individual's refusal to provide the information or engage in any of prohibited conduct. "Adverse action" means: discharging, disciplining, or otherwise penalizing an employee; threatening to discharge, discipline, or otherwise penalize an employee; and failing or refusing to hire an applicant.

Exceptions

The statute provides an exception for employer investigations in certain circumstances. The law does *not* apply to an employer's request or requirement that an employee share the content to his or her personal social networking account if all of the following conditions are met:

(1) the employer requests or requires the content to make a factual determination in the course of conducting an investigation,

(2) the employer undertakes the investigation in response to receipt of information about the employee's activity on his or her personal social networking account,

(3) the purpose of the investigation is to

(i) ensure compliance with applicable laws or prohibitions against work-related employee misconduct *or*

(ii) investigate an allegation of unauthorized transfer of an employer's proprietary information, confidential information, or financial data to the employee's personal social

Meet the Author

Bryan P. O'Connor

Office Managing Principal
Seattle 206-626-6423
Email

Practices

Privacy, Data and Cybersecurity

networking account, and

(4) the employer does not request or require the employee to provide his or her login information.

The law does not apply to social networks, intranets and other technology platforms "that [are] intended primarily to facilitate work-related information exchange, collaboration, or communication by employees or other workers." Further, it does not prohibit an employer from requesting or requiring an employee to disclose login information for access to an account or service provided by virtue of the employee's employment relationship with the employer, or to an electronic communication device or online account paid for or supplied by the employer.

If, through the use of an employer-provided electronic communications device or an electronic device or program that monitors an employer's network, an employer inadvertently receives an employee's login information, the employer is not liable for simply possessing such information. However, the employer may not use this information to access the employee's personal social networking account.

Remedies

This law contains meaningful remedies and penalties. An employee or applicant may bring a civil action alleging a violation of this law. A court may award statutory damages of $500, injunctive or other equitable relief, actual damages, and reasonable attorneys' fees and costs to a prevailing employee or applicant. If a court finds the action was frivolous and advanced without reasonable cause, it may award reasonable expenses and attorneys' fees to any prevailing party, including employers.

Jackson Lewis attorneys are available to answer inquiries regarding this and other workplace developments.