A Timely Analysis of Legal Developments

ASAP®

June 6, 2013

Oregon Passes Social Media in the Workplace Law

By Howard Rubin and Don Stait

On May 22, 2013, Oregon Governor John Kitzhaber signed into law House Bill 2654, making Oregon the tenth state to enact a law prohibiting employers from accessing employees' private social media sites. The new law, which becomes effective January 1, 2014, makes it an unlawful employment practice for employers to compel employees or applicants for employment to provide access to their personal protected social media accounts.

"Social media" is broadly defined under the law as any "electronic medium that allows users to create, share and view user-generated content, including, but not limited to, uploading or downloading videos, still photographs, blogs, video blogs, podcasts, instant messages, electronic mail or Internet website profiles or locations." The definition includes such standard social media venues as Facebook, Twitter and LinkedIn, as well as the newer bulletin board-type sites like Pinterest and Instagram. According to the plain text of this definition, email accounts are also included.

Under the new law, which will become part of Oregon Revised Statutes (ORS) - Chapter 659A, employers, including employment agencies, are prohibited from "requir[ing] or request[ing] an employee or an applicant for employment to disclose or to provide access through the employee's or applicant's user name and password, password or other means of authentication that provides access to a personal social media account." Passwords and other forms of identification used to provide access to employees' social media sites are now beyond the reach of employers or prospective employers.

Nor can an employer "compel an employee or applicant . . . to add the employer . . . to the employee's . . . list of contacts associated with a social media website." In other words, employers cannot gain access to social media sites by requiring employees and/or applicants to "friend" them or to make them a contact on their social media accounts.

Moreover, an employer cannot "compel an employee . . . to access a personal social media account in the presence of the employer," thus preventing the employer from viewing an employee's content by having the employee log on to the site for the employer.

The law also prevents employers from retaliating or threatening to retaliate against employees or otherwise penalizing employees or applicants with any adverse employment action, including failure to hire, because the employee or applicant failed to provide the employer with access to the site by any of the means prohibited by the statute.

As inclusive as the law appears, it does provide limited exceptions. If the employer provided the social media account, or if the account was provided on behalf of the employer to be used for the employer, then the employee must disclose the user name and password he or she uses to access the account.

Moreover, nothing in the statute prohibits an employer from complying with state and federal laws, rules and regulations, or conducting a legitimate employment investigation "for the purpose of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct," if the employer has reason to believe, based on specific information, that content of an employee's personal online account or service is implicated or otherwise involved. The investigating employer may also require an employee to share social media content reported to the employer if it is necessary for the employer to make a factual determination about alleged unlawful work-related misconduct.

Even in concert with a legitimate investigation, the employer is prohibited from requiring an employee to disclose a username, password or other form of access to his or her social media accounts.

Employers may access information and content posted by or about an employee or applicant that is publicly available—for example, the public information on a Facebook account and any content not designated as private by the account holder.

Finally, if an employer inadvertently gains knowledge of an employee's access information by monitoring usage of the employer's network or employer-provided devices, the employer is not liable for having the information if the employer does not *use* the information to access the employee's personal social media accounts.

The bill that the Governor signed indicates only that it will become part of ORS chapter 659A, so it remains to be seen exactly what remedies will be available against employers who violate the statute. Most likely, available remedies will include injunctive relief and any other equitable relief that may be appropriate, including but not limited to back pay, reinstatement, and attorney's fees. Like some other violations of ORS 659A, general damages and punitive damages may also be available for violations of the new law.

Legislation regarding social media monitoring by employers is high on the agendas of many state legislatures. Washington passed a law similar to Oregon's statute earlier in May. At the federal level, Rep. Ed Perlmutter (D-CO) introduced the Password Protection Act of 2013 in the U.S. House of Representatives just days before Oregon's bill was signed into law. The federal House bill would amend the Computer Fraud and Abuse Act and make it unlawful for employers to require employees to authorize access to a computer that the employer does not own or operate. Further, the federal House bill provides no exception allowing employers to obtain password-protected social media content that reasonably relates to a workplace investigation into allegations of harassment.

What Steps Should Employers Take?

Employers with employees working in Oregon should review their social media policies to ensure they conform with the statute. Managers, supervisors and others involved in the hiring process should be trained to ensure they do not violate the statute.

Employers need not be concerned that their actions in complying with the statute will expose them to liability for negligent hiring. The statute confers immunity for negligent hire actions based on the employer's failure to obtain password-protected access to an employee's social media account.

The bottom line is that momentum is gathering for social media privacy. A watchful eye is warranted.

Howard Rubin is the Office Managing Shareholder of, and Don H. Stait is a Special Counsel in, Littler Mendelson's Portland office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, Mr. Rubin at hrubin@littler.com, or Mr. Stait at dstait@littler.com.