HRHero.com

UTAH EMPLOYMENT LAW LETTER

Part of your Utah Employment Law Service

Darryl J. Lee, Editor — Kirton McConkie

May 2013

LEGISLATION

Utah's new privacy law: Don't ask employees for their passwords

by Darryl J. Lee

Utah lawmakers recently passed the Internet Employment Privacy Act (IEPA), joining at least six other states in prohibiting employers from requiring employees or job applicants to disclose their passwords or user names for personal social media accounts. (California, Delaware, Illinois, Maryland, Michigan, and New Jersey have enacted similar legislation.) The new law is clearly a measured response to the increasing curiosity of employers and their desire to uncover any and all personal information about employees and applicants, in some instances going too far in that endeavor.

What does the law require?

The IEPA, which will become effective on May 14, 2013, specifically provides that employers may not:

- Request that employees or applicants disclose user names and passwords that allow access to their personal Internet accounts; or
- Take adverse action, fail to hire, or otherwise penalize employees or applicants for failing to disclose user names and passwords.

Under the new law, "adverse action" includes discharging, threatening, or otherwise discriminating against an employee in any manner that affects his employment, including his compensation, terms of employment, location, immunities, promotions, or privileges. A "personal Internet account" is an online account that is used by the employee or applicant exclusively for personal communications unrelated to any business purpose of the employer. It does not include an account created, maintained, used, or accessed by an employee or applicant for business-related communications or for a business purpose of the employer.

What are the exceptions?

The IEPA also makes clear, however, that employers are not prohibited from:

- Requesting or requiring employees to disclose user names or passwords needed only to gain access to (1) an electronic communications device supplied by or paid for in whole or in part by the employer or (2) an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, and used for the employer's business purposes;
- Disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to a personal Internet account without the employer's consent;
- Conducting an investigation or requiring employees to cooperate in an investigation to ensure compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct if (1) there is specific information about activity on an employee's personal Internet account or (2) the employer has specific information about an unauthorized transfer of its proprietary information, confidential information, or financial data to an employee's personal Internet account;
- Restricting or prohibiting employees' access to certain websites while they are using electronic communications devices supplied by or paid for in whole or in part by the employer or while using the employer's network or resources in accordance with state and federal law; and
- Monitoring, reviewing, accessing, or blocking electronic data stored on electronic communications devices supplied by or paid for in whole or in part by

the employer or stored on the employer's network in accordance with state and federal law.

Is all Internet screening prohibited?

Although the law places significant restrictions on employers, it does make it clear that employers are not prohibited or restricted from viewing, accessing, or using information about an employee or applicant that can be obtained without a username or password and is available in the public domain. Accordingly, employers may still perform due diligence investigations into potential employees by reviewing publicly available information on the Internet. Further, the IEPA makes it clear that an employer will not be held liable for *not* monitoring an employee's or applicant's personal Internet accounts.

What happens if violations occur?

Under the new law, if an employer violates the terms of the legislation, an employee is permitted to file a private right of action against the company. That means the employee could sue the employer in court for damages. However, the law states that a court cannot award the employee damages in excess of $500.

Where do we go from here?

While the new law does place significant restrictions on employers' efforts to obtain access to Internet information protected by passwords and user names, it isn't all bad for employers. As we noted above, the IEPA does recognize some exceptions, especially for electronic communication devices supplied or paid for by an employer and accounts or services provided by an employer and used for its business purposes. Also, in line with many Utah companies' current personnel policies, the IEPA expressly allows employers to monitor, review, access, or block electronic data stored on company servers, networks, or devices in circumstances in which employees have no reasonable expectation of privacy.

It would be prudent for all Utah employers to review their social media policies as well as their recruiting and hiring practices to ensure compliance with the ever-changing face of the electronic workplace.

➥ *You can research laws governing employer use of passwords and user names or any other employment law topic in the subscribers' area of www.HRHero.com, the website for Utah Employment Law Letter. Access to this online library is included in your newsletter subscription at no additional charge.* ✤