Utah's Internet Employment Privacy Act Restricts Access to Personal Social Media for Employment Purposes

Publication — 4/24/2013

Effective May 14, 2013, Utah employers may not request employees or applicants to disclose information related to their personal Internet accounts. The Internet Employment Privacy Act (IEPA), recently signed into law by Governor Gary R. Herbert, prohibits employers from asking an employee or applicant to reveal a username or password that allows access to the individual's personal Internet account. In addition, employers may not penalize or discriminate against an employee or applicant for failing to disclose a username or password. A similar restriction applies to higher educational institutions through passage of the Internet Postsecondary Institution Privacy Act.

With enactment of the IEPA, Utah becomes the fifth state to pass legislation that limits an employer's access to social media accounts, joining California, Illinois, Maryland and Michigan. New Mexico passed a similar law shortly after Utah and New Jersey's law passed the legislature and is awaiting the governor's signature. A bill introduced in February in the U.S. House of Representatives called the Social Networking Online Protection Act (H.R. 537) is stuck in committee.

Public Online Accounts Are Fair Game under the IEPA

The IEPA does not restrict or prohibit employers from viewing or using online information about employees and applicants that the employer can obtain without the employee's username or password. Any online information that is available to the public may be accessed and viewed by employers without violating the IEPA. Consequently, individuals who set privacy settings on their online accounts to allow "public" access effectively opt themselves out of any protections offered by this new law.

Utah Restriction Applies to Accounts Used Exclusively for Personal Communication

In prohibiting employers from requiring disclosure of online usernames and passwords, the IEPA draws a distinction between personal Internet accounts and those used for business related communications. The law only restricts employer access to personal online accounts that are used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer. It does not, however, restrict access to accounts created, maintained, used or accessed by an employee or applicant for business related communications or for a business purpose of the employer.

In practice, the line between personal and business related accounts may

be blurred as many employees use their personal online presence to network and communicate for business reasons. Consider the sales person who uses his or her LinkedIn account to communicate with potential buyers within a particular industry, or the CPA who posts tax reminders on his or her Facebook page. Are those accounts accessible under the IEPA since they are not used "exclusively" for personal communications? A plain reading of the law suggests that may be the case, thereby watering down the potential protections offered by the IEPA to applicants and employees.

Permitted Actions by an Employer under the IEPA

The IEPA clarifies that certain employer activities related to online accounts are permissible, including:

- Requesting or requiring an employee to disclose a username or password to gain access to an electronic device supplied or paid for by the employer or to access an account or service provided by the employer, obtained through the employment relationship and used for the employer's business purposes;
- Conducting an investigation or requiring an employee to cooperate in an investigation (a) to ensure compliance with the law or workplace conduct rules when there is specific information about what is on the employee's personal Internet account related to such compliance, or (b) regarding an unauthorized transfer of the employer's proprietary, confidential or financial data to an employee's personal Internet account when the employer has specific information about the employee's personal Internet account related to such transfer;
- Disciplining or discharging an employee for transferring the employer's proprietary, confidential or financial data to an employee's personal Internet account without the employer's authorization;
- Restricting or prohibiting an employee's access to certain websites while using employer-provided electronic devices, networks or resources; and
- Monitoring, reviewing, accessing or blocking electronic data stored on an employer-provided device or network.

Damages for Violation Capped at $500

A person alleging an employer's violation of the IEPA may file a civil lawsuit against the employer. If the court finds a violation occurred, the court may award up to $500 in damages to the aggrieved employee or applicant.

Steps for Complying with the IEPA

Utah employers should review their HR forms, policies and practices to ensure that they do not ask applicants and/or employees to provide a username or password to their personal Internet accounts. Train supervisors and managers not to ask for this information as well. In fact,

take the opportunity to remind supervisors and managers not to "friend" subordinates on personal online platforms, such as Facebook. In addition, reinforce that employees and applicants may not be penalized or treated adversely for failing to provide a username or password for personal online accounts.

Remember, too, that even though the IEPA does not prohibit accessing an employee's or applicant's public social media accounts, viewing such information gives rise to other risks. Employers may view information regarding the individual's religion, race, national origin, disability, age, or other protected group status that could give rise to a discrimination claim. Furthermore, online information is unreliable and ever-changing, meaning that employers should not rely on what they see online when making employment decisions. To stay out of trouble, consult with legal counsel before viewing or using social media in the employment context.