Proskauer

Utah’s New Internet Employment Privacy Law Continues a Growing Trend

April 2, 2013

On March 26, 2013, Utah joined Maryland, Illinois, California, and Michigan as the fifth state to prohibit employers from requesting that job applicants or employees disclose passwords protecting their personal internet accounts. Given that the U.S. Congress and many other state legislatures have advanced similar proposals, employers across the country should consider reviewing Utah's Internet Employment Privacy Act ("IEPA"). To assist employers in that endeavor, this alert details the scope of the IEPA's coverage, the breadth of its prohibitions and exceptions, and the remedies afforded therein.

Coverage

The IEPA defines a "personal Internet account" as one used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer. The IEPA explicitly excludes from its coverage any account created, maintained, used, or accessed by an employee or applicant for a business purpose.

Prohibitions

As noted above, the IEPA forbids an employer from requesting that an employee or applicant disclose a username and/or password allowing access to his or her personal Internet account. The IEPA also prohibits an employer from taking adverse action against an employee or applicant for failing to disclose such information.

Exceptions

The IEPA provides several exceptions. Among them, employers may request or require an employee to disclose a username or password for an

- employer-issued (or paid for) electronic communications device, or
- employer-provided account or service used for business purposes.

Further, in accordance with state and federal law, the employer may restrict or prohibit an employee's access to certain websites while using employer-issued (or paid for) electronic communications devices, or the employer's network or resources. The employer also may monitor, review, access, or block electronic data stored on an employer-issued (or paid for) electronic communications device or the employer's network, in accordance with state and federal law.

In addition, the employer may discipline an employee for transferring proprietary or confidential information or financial data to an employee's personal Internet account without the employer's authorization. Moreover, the employer has the right to conduct an investigation or require that the employee participate in such an investigation, if there is specific information about

- activity on the employee's personal Internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct, or

- the unauthorized transfer of proprietary or confidential information or financial data to an employee's personal Internet account.

The IEPA also states that nothing therein restricts employers from complying with a legal duty to screen employers or applicants, or to monitor or retain employee communications. So as not to create a Catch-22, the IEPA also makes clear that an employer will not be held liable for *not* monitoring the employee's or applicant's personal Internet account. Finally, employers may view, access, and use publicly available information on the internet regarding an applicant or employee consistent with existing law.

Remedy

Although the IEPA allows for a private right of action in a court of competent jurisdiction, damages may not exceed $500.

Takeaway

In addition to monitoring recent legislative developments across the nation, employers should (1) make sure that their searches and use of information found on the Internet and social media sites do not violate relevant privacy and antidiscrimination laws; (2) stay up to date with decisions rendered by courts and the National Labor Relations Board on these issues; and (3) ensure their general social media policies and any rules regarding company-sponsored social media activities are current with the developing law.

If you have any questions or concerns regarding these new laws or related developments, please contact your Proskauer lawyer or any co-chair of the Employment Law Counseling & Training Group.

Authors for this alert:

Katharine H. Parker, Daniel L. Saperstein and Noa M. Baddish.

Related Professionals

- **Noa M. Baddish**
  Partner