Nebraska Adopts Workplace Privacy Act

Mark A. Fahleson
Rembolt Ludtke LLP

During its recent session, the Nebraska Unicameral adopted the Workplace Privacy Act (LB 821). The legislation, introduced by Sen. Tyson Larson and adopted by the Legislature on a 46-0 vote, was signed into law by Governor Pete Ricketts on April 19, 2016, and goes into effect on or about July 19, 2016.

The stated purpose of the Workplace Privacy Act ("Act") is to "restrict employers from requesting or requiring that employees or applicants provide an employer with account information so that the employer can access their private social networking site profile or account."

The specifics of the Act, which is patterned off similar legislation adopted by other states, are as follows:

- Coverage. Covers "employers," which is broadly defined as "a public or nonpublic entity or an individual engaged in a business, an industry, a profession, a trade, or other enterprise in the state, including any agent, representative, or designee acting directly or indirectly in the interest of such an employer." Unlike other employment laws, the definition of a covered "employer" is not limited to those that employ a certain number of employees or have a threshold amount of revenue. Essentially, it's all employers, public and private, regardless of size.
- What it prevents. The Act prohibits "employers" from:

    - Requiring or requesting that an employee or applicant provide or disclose any username or password or any other related account information in order to gain access to the employee's or applicant's personal Internet account by way of an electronic communication device;
    - Requiring or requesting that an employee or applicant log into a personal Internet account by way of an electronic communication device in the presence of the employer in a manner that enables the employer to observe the contents of the employee's or applicant's personal Internet account or provides the employer access to the employee's or applicant's personal Internet account;
    - Requiring an employee or applicant to add anyone, including the employer, to the list of contacts associated with the employee's or applicant's personal Internet account or require or otherwise coerce an employee or applicant to change the settings on the employee's or applicant's personal Internet account which affects the ability of others to view the content of such account; and

    - Taking any adverse action against an employee or applicant for failure to provide or disclose any of the information or to take any of the actions specified above.
- Discrimination/Retaliation. The Act mandates that employers cannot discriminate or retaliate against employees or applicants for filing a complaint under the Act or participating in an investigation, proceeding or action concerning alleged violations of the Act.
- How it is enforced. The Act provides that an aggrieved employee or applicant may, in addition to any other available remedy institute a civil action in state district court within one (1) year after the date of the alleged violation or the discovery of the alleged violation, whichever is later. If successful, the employee or applicant shall be entitled to appropriate relief, including temporary or permanent injunctive relief, general and special damages, reasonable attorney's fees, and costs.
- What employers may still do. The Act makes clear that employers may still maintain workplace policies regarding Internet use and obtain access to devices and accounts provided by the employer. In addition, employers may still, if done properly, monitor employee Internet use on employer-provided devices/service as well as access information that is otherwise publicly available.
- No duty to investigate. The Act expressly provides that it does not create a duty for employers to request, gain access to or investigate information on an employee's or applicant's personnel Internet account.
- Pro-employer provisions. The Act potentially provides a new avenue for relief for employers whose employees pilfer the employer's confidential proprietary information, perhaps to compete with the employer. The Act states that "an employee shall not download or transfer an employer's private proprietary information or private financial data to a personal Internet account without authorization from the employer." However, as drafted, it is unclear whether employers may file a claim under the Act and seek the specified damages and attorneys' fees for such violations.

TAKEAWAYS: Most employers do not require applicants or employees to provide unfettered access to personal Internet and social media accounts and, thus, the Act will have nominal effect. However, the Act does create a new avenue for legal liability for employers, which means plaintiffs' attorneys will be looking for potential violations and the attorneys' fees that come with it. All employers--regardless of size—would be well advised to review their practices and policies to ensure compliance with the Act and to limit potential legal exposure for requesting or reviewing nonpublic personal information about an applicant or employee.

Fahleson is an attorney with the Lincoln-based law firm of Rembolt Ludtke LLP and may be reached at (402) 475-5100 or mfahleson@remboltlawfirm.com. ***This article is provided for general information purposes only and should not be construed as legal advice. Those requiring legal advice are encouraged to consult with their attorney.***

4844-2484-7664, v. 1