Illinois Now Restricts Employers' Access To Employees' Social Networking Sites

Insights
8.01.12

On March 22, 2012, Illinois legislature passed an amendment to the Illinois Right to Privacy in the Workplace Act. This bill was signed on August 1, 2012, by Gov. Pat Quinn, and takes effect January 1, 2013. This makes Illinois only the second state (Maryland was the first) to ban employers from requiring access to employee and applicant social networking sites.

In addition to Maryland, at least ten other states and the federal government are evaluating similar legislation. Additionally, U.S. Senators Richard Blumenthal (D-CT) and Charles E. Schumer (D-NY) have requested that both the EEOC and the U.S. Justice Department investigate the legality of demanding social networking passwords from employees and applicants.

Illinois employers should be aware of the scope of the statute, and, in particular, the manner in which the Act will limit your ability to access social media pages maintained by your employees.

What's In The New Amendment?

In General
The Act now prohibits employers from requesting or requiring any current employees or applicants to: 1) provide their passwords, or related account information, to any social networking site for the purpose of accessing the site, or 2) provide access to their social networking site in any manner. Such social networking sites would include Facebook, Twitter, Google+, MySpace, LinkedIn, and other similar sites.

The law does not prohibit you from establishing and maintaining workplace policies which restrict the use of the company's technology, such as computers, internet, or social networking sites while at work. The law also does not prohibit you from monitoring employee usage of company technology. Finally, the bill does allow you to search the public domain for information regarding employees or applicants (which would likely include accessing information on social networking sites which have not been restricted as "private" by the user).

Applicant Screening
One aspect of the Act is fairly non-controversial â€“ the Act prohibits employers from requiring that job applicants hand over their passwords so that the employer could explore their social networking sites as part of the hiring process. Employment lawyers have frequently noted that this practice

creates a potential risk under state and federal anti-discrimination statutes. Access to social media sites may likely reveal information regarding applicants such as religion, age, race, color, sex, disability, and other categories which are protected by Title VII, the Americans with Disabilities Act, and equivalent state laws.

For instance, many social network users upload photos and disclose their birthdays on their personalized social networking sites. Such information would allow a prospective employer to learn an applicant's age, color, and sex, even if the employer deliberately avoided collecting such information on its job application forms. And even if this information did not play a role in a hiring decision, accessing such information could lead to allegations that the employer took into account prohibited characteristics, resulting in a charge of discrimination. For these reasons, some commentators have questioned whether additional legislation barring employers from asking for social media passwords was even necessary.

But you are still allowed to use publically-available information to screen job applicants. The bill specifically allows employers to obtain information which is in the public domain. While you may still face certain risks under anti-discrimination laws by relying on public content relating to job applicants, the Federal Trade Commission has approved the use of third-party vendors to screen applicants based on publicly-available social media information and other Internet websites as part of an authorized background check.

These services are intended to alert employers when job applicants have been found to have engaged in anti-social or inappropriate behavior on public Internet sites as a way of keeping such conduct out of the workplace. Employers who rely on such a screening process may be insulated from access to information about job applicants that would be protected by anti-discrimination laws, while also reducing the risk of a possible future negligent-hiring type of claim.

Current Employees

The Act prohibits you from asking for employee passwords or circumventing the need for a password by requiring that employees or applicants access their social networking sites in the presence of the employer (even without turning over their passwords) so that you can review the contents of the social networking site.

These restrictions could affect a fair number of seemingly innocuous practices. For example, if an employee maintains a Twitter account that is primarily used to promote your business, you cannot ask that the employee share the account password, even to allow the company to update the account while the employee is absent.

Similarly, if an employee created a "fan page" on Facebook and is the only employee with administrative rights to the Facebook fan page, you may not ask the employee for the password that would enable the company to update its Facebook presence. For these reasons, employers that maintain profiles on social media sites should confirm the manner in which their business profiles

are maintained to ensure that they can continue to access these sites even if an employee departs unexpectedly.

In addition, consider how the Act might affect your ability to investigate workplace misconduct. For example, if you suspect that an employee is using a LinkedIn account to solicit customers for a rival business, the Act may prevent you from accessing the employee's account on LinkedIn, even if only for the purpose of confirming whether such communications have occurred. Similarly, if you receive a complaint of harassment involving comments posted on a social media account, take care when investigating such allegations to make sure not to get tripped up by the Act, while trying to assist the employee who is being harassed.

In fact, if an employee complains that a co-worker posted offensive content on his or her social media profile, you could violate the Act by simply asking the complaining employee to access a social media account for the purpose of showing you the offensive content at issue.

Going Forward

In order to comply with the Act that takes effect January 1, and the many other similar laws that may be on the horizon, you should evaluate your technology policies and practices that relate to employee social media accounts. For example, the Act expressly states that companies can monitor and restrict use of company-provided technology at work. Thus, the Act is not intended to protect employees who fritter away all of their time updating their social media profiles or playing on-line games.

Presumably, employers that use key-stroke monitoring or other electronic monitoring for the purpose of reviewing employee usage of Internet websites would be permitted to continue with these practices, even if the content of employee social media sites may be collected through these monitoring tools. On the other hand, password sharing among employees, even for the convenience of the employees, may be prohibited under the Act.

For more information contact any of the lawyers in our Chicago office at (312) 346-8061.

This Legal Alert provides an overview of a specific new state law. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.