

insights

Illinois takes the lead on employee privacy: What employers need to know

When it comes to employee privacy protection, employees in the United States generally do not have a right to privacy in their workplace. By contrast, members of the European Union recognize employee rights to privacy and specifically outline various protections that must be afforded employees. In the United States, the concept of employee privacy is largely left to the states. Not surprisingly, this means that employee privacy protections can vary widely from state to state as some enact laws designed to protect employee privacy rights while others are silent on the issue.

Illinois is one of the states that has enacted a number of laws designed to protect the privacy of employee information. And for businesses in Illinois or looking to move to Illinois that wish to avoid fines and other sanctions, it is important to be aware of the protections afforded to employees under these laws.

So what do you need to know about employee privacy in Illinois?

Guidelines for employer use of bio-identifiers in Illinois

As technological advances continue, more resources are becoming available that are designed to expedite certain employee-employer processes, such as time clocks. The age-old concept of “punching the clock” has received an upgrade. Employees can now “punch the clock” by using their fingerprint to “clock-in.” This reduces the amount of paper and helps expedite the payroll process. But employers beware: There are specific laws that apply to the collection, usage, sharing, and storage of such bio-identifiers, such as retina and iris scans, fingerprints, voiceprints, hand scans or facial geometry scans).

More resources that use bio-identifiers or biometric information (“biometric information” means any information based on bio-identifiers that can be used to identify an individual) are entering the workplace. While these resources can benefit employers and employees alike, concern regarding the collection, use, storage and potential misuse of this information led to the Illinois Biometric Privacy Act (740 ILCS 14). The Act was passed back in 2008, but only recently has technology caught up with the employment policies associated with the Act.

Under the Act, before you can use biometric identifiers for any purpose, you must have a written policy describing the company’s collection, storage, use, and destruction of that information. In that policy, you must:

- Inform the employee in writing of the collection of bio-identifiers, the purpose for the collection and for how long the information will be stored;
- Obtain written consent from the employee for the collection;
- Inform the employee of how you plan on destroying the information on the earlier of when the purpose it was collected for is satisfied or within three (3) years of the employee’s last contact with the employer.

Companies are prohibited from selling, leasing, trading, or in any way profiting from someone’s biometric information. And you cannot disclose biometric information unless the employee consents to the disclosure, if the disclosure completes a financial transaction authorized by the employee, or if the disclosure is required by law enforcement or a subpoena.

In addition, you must use reasonable measures to protect any biometric information you collect and store from unauthorized access. These measures must meet industry standards and must be equal to or more protective than other confidential or sensitive information stored by the employer.

If these regulations are not followed, employees may sue their employer for an unauthorized disclosure or failure to protect the biometric data. In addition to attorneys’ and expert fees and litigation costs, wronged employees can

choose between the greater of actual damages or a \$1,000 penalty per negligent violation, or the greater of a \$5,000 penalty per intentional or reckless violation.

Limits on the use of certain employee information

With the availability of information about employees through a host of public, semi-private, and private sources (including social media accounts, credit reports, and employment applications), employers have access to more information about their employees than ever before. Concern over the access to and use of such information has led Illinois to pass several laws protecting an employee's privacy in certain situations.

Under the Illinois Right to Privacy in the Workplace Act (820 ILCS 55), for instance, employers are prohibited from discriminating against employees in the workplace who engage in lawful activity outside of the workplace. This prohibition encompasses not only political activity but also an employee who takes advantage of Illinois' medical marijuana law for an allowed medical condition. (Our Tracking Cannabis blog has covered [some of the same issues that come up](#) for employers in California, another state that has legalized cannabis use.)

The Illinois Act prohibits employers from doing any of the following:

- Acquiring or requiring disclosure of username and passwords for personal online accounts;
- Requiring an applicant to access a personal online account in the employer's presence;
- Requiring an employee or applicant to invite the employer to join a group affiliated with the employee's or applicant's personal online account;
- Requiring an employee or applicant to join an online account established by the employer or add the employer or an employment agency to the employee's or applicant's contacts to allow employer access to the employee's or applicant's personal online accounts;
- Discriminating or refusing to hire an employee or applicant for refusing to do anything prohibited by the Act.

The Illinois Department of Labor enforces this Act and can impose fines (\$200 per employee for negligent violations and \$500 per employee for knowing violations) and assess attorneys' fees and costs to companies who fail to abide by these regulations.

A company's use of Social Security numbers (SSNs) has also been regulated under Illinois law 815 ILCS 505/2RR. This Act applies to any SSNs, not just those collected as a result of an employer-employee relationship.

Under the Act, an employer is not permitted to:

- Publicly post or display SSNs;
- Print SSNs on an ID card;
- Require an individual to transmit their SSN over the internet unless secure or encrypted;
- Require the use of a SSN to access a website, unless some other unique password or authentication is also required; and
- Print SSNs on any materials that are mailed to the individual (unless required by State or Federal Law).

Violations of any of these prohibitions are considered an "unlawful act" under the Illinois Consumer Fraud and Deceptive Business Practices Act and are subject to enforcement proceedings by the Illinois Attorney General's office.

For more information, please contact one of the attorneys in the Firm's [Cybersecurity](#) group.

authorsTest