HINSHAW

BIPA: Employer Obligations, the Risks of Noncompliance, and What Comes Next

Labor & Employment Newsletter - February 2018

Hinshaw Newsletter | 5 min read
Feb 15, 2018

BIPA: Employer Obligations, the Risks of Noncompliance, and What Comes Next

There is no denying that technology—hardware and software—has greatly enhanced the workplace. But with this digital technology revolution come new risks of improper disclosure, lost data, exposure of trade secrets, potential overtime claims when non-exempt personnel access electronic systems off-the-clock, among others. The Illinois Biometric Information Privacy Act (BIPA) seeks to manage those risks as they relate to biometric technology, by requiring employers (and any other entities) that collect biometric information to set up formal policies for handling, storing and destroying such information.

BIPA applies to employers that collect "biometric identifier" information. As defined by the statute, this "means a retina or iris scan, finger print, voice print, or scan of hand or face geometry." 740 ILCS 14/10. The statute also protects "biometric information" which is a derivation of biometric information (i.e., taking that biometric identifier and converting it into another form). See 740 ILCS 14/10. For instance, a finger print that is converted into a mathematical calculation for purposes of generating time entry is considered biometric information subject to protection.

Employer Obligations under BIPA

Written Policy Requirement: An employer must develop a written policy that specifies what information is collected and why. The policy must address how long the information is going to be retained and guidelines for permanently destroying the biometric identifiers and biometric information. 740 ILSC 14/5(a). The statute also provides that the destruction must be completed within three (3) years of the individual's last interaction with a private entity whichever occurs first. 740 ILCS 14/15(a). In other words, once that individual has left employment, the biometric information or biometric identifier must be permanently destroyed as promptly as possible.

Biometric information must be closely guarded, including the disclosure of such data with others. There are limitations on the sale, lease, trade or otherwise, profiting of this information. If the employer uses a third-party

vendor for purposes of timekeeping, security or other business reason, it should detail in writing the steps it will take to protect this information and ensure that the vendor follows the same or similar steps. Notice to employees of this disclosure should also be part of the acknowledgement that they will sign, as addressed in the section below.

Written Consent Requirement: An employee must be informed of the nature of the biometric information that is stored, its purpose, and how it is stored. It is referred to as "informed consent" in the statute, consent that must be received before an employer can collect and use such information. As noted, it should include a reference to any disclosure of the info to a third-party vendor. The employee's consent can be a term of employment.

The Risks of Noncompliance

Violations of the statute can be substantial. A prevailing party is entitled to liquidated damages of $1,000 or actual damages, whichever is greater. 740 ILCS 14/20(1). In a case of intentional or reckless violations of the law, the liquidated damages are set at $5,000 or actual damages, whichever is greater. 740 ILCS 14/20(2). Just as importantly, the prevailing party is entitled to reasonable attorney's fees and costs associated with the litigation. 740 ILCS 14/20(3).

Biometric Technology Checklist

1) Ask yourself, do you really need biometrics technology? Just because the technology is "the latest thing" does not mean every employer needs it. If a proper functioning time clock is all you need to record employee time, then consider staying with that system if biometric time systems offer nothing better or more secure.

2) If a biometric system is adopted for any purpose, immediately comply with the statute. Develop a formal written policy that addresses collection, use, disclosure, retention and destruction in keeping with the requirements of the statute.

3) Roll out the new biometric system through education, distribution of policies, and receipt of assigned acknowledgement form that becomes an employee's "written consent" to the collection and use of their biometric data.

4) Design a security protocol for the storage and back up of this information. Treat biometric information as any other confidential business information. Control access of this data and ensure a plan is in place should there be a breach. For instance, consider how a breach will be handled, what steps will be taken to address it, and the scope of notice to those affected.

5) Develop destruction guidelines & schedules. For example, perhaps part of the exit process includes notification to IT, Payroll, a third party and other appropriate personnel that an employee has terminated and his or her biometric information must be destroyed. Destruction must be targeted at the biometric identifier and the mathematical conversion from it. Obviously, the underlying time records that come from the biometric time clock must be maintained for to be compliant with wage and hour statutes. We recommend ten years for those

employers subject to the Illinois Wage Payment & Collection Act. Consider adding "biometric info destruction" to an exit interview checklist. This should be as commonplace as sending a COBRA letter.

For employers that retain that information in-house, work with your IT and/or Payroll department to ensure prompt destruction and proof of same. If the biometric information has been shared with vendors, such as for payroll purposes, develop a formal communication system in which the vendor is notified in writing of the employee's separation and need to destroy biometric information. Require proof of destruction from the vendor.

6) Build in BIPA into your third-party contracts so that contractors acknowledge their obligations under BIPA and agree in writing to them.

After BIPA, What's Next?

Litigation over the BIPA statute is just beginning. For example, there is a split in the courts as to whether a plaintiff needs to show actual injury or damages for purposes of bringing suit under BIPA. Failing to have a formal policy, failing to follow it, and failing to have an employee sign off on a written consent may be sufficient violations of the statute which may subject an employer to liability. Don't be one of those employers! Even if you are unsure if the information is really biometrics as that term is defined under the statute, take precautions and adopt a compliant policy. For example, the technology you use may involve a temporary scan of a fingertip that is not a stored "finger print". Is it covered under BIPA? The statutory damages and risk of paying opposing counsel to find out may not be worth the risk. An ounce of prevention is worth a pound of cure.

Employment Law Observer Blog

Following release of the January newsletter, Hinshaw also blogged about employment law developments. Examples include:

- Hinshaw Employment Webinar Series: Employer-Assisted Student Loan Repayment Programs
- DOL Says Hello to Primary Beneficiary Intern Test, Goodbye to 6-Factor Test
- CEO Does Not Get Whistle Blower Protections for His Opinions
- Hinshaw E-alert on a New Employer Tax Credit for Paid FMLA

Related People

Linda K. Horras

Of Counsel

312-704-3022

Related Capabilities

Consumer & Class Action Defense

Labor & Employment