

An Employer's Guide to the Illinois Biometric Information Privacy Act

Insights for Employers Alert | 7 min read

Jan 17, 2019

The Illinois state legislature passed the [Biometric Information Privacy Act in 2008](#). The law, known as BIPA, covers and regulates private employer use of biometric identifiers and biometric information of Illinois employees. Local and state governmental employers are specifically exempted.

This guide reviews BIPA's scope, BIPA employer compliance requirements, and BIPA penalties for noncompliance. We have taken the time to review this legislation from 2008 because the use of employee biometric data is increasing. *Rosenbach v. Six Flags Entertainment Corp.*, is a BIPA case currently before the Illinois Supreme Court and we have provided a review of that case as well.

BIPA: Overview and Compliance Obligations

BIPA covers and regulates employer use of biometric identifiers and biometric information of Illinois employees. While Illinois private employers have little room to avoid compliance, governmental employers are excluded and BIPA does not apply to a contractor, subcontractor or agent of a State agency or local governmental unit when performing work on behalf of such governmental unit.

Examples of BIPA-covered employer interactions with employees' biometric identifiers include (but are not limited to) using any of the following for security scanning, time entry, and paying wages or salaries:

- retina or iris scans
- fingerprints
- voiceprints
- scan of hand or face geometry

Employers must take care with any biometric information which is defined in BIPA as any type of data from any source that is based on an individual's biometric identifier and that is used to identify an individual, subject to certain exclusions. The signals for the potential broad construction of BIPA appear in its provision which states that the full range of potential consequences of using biometric technology "are not fully known." For example,

when BIPA was passed, the legislators did not specifically anticipate the increasing use of biometric identifiers or biometric information by hourly employees to record when they start and end their work shifts.

Illinois employers **must** take several steps **before** obtaining or transferring biometric identifiers or biometric information on their employees:

- Inform an employee in writing that you are collecting or storing their biometric identifier and biometric information
- Inform the employee of the applicable time span and specific purpose for collecting, storing, and using the employee's biometric identifier or biometric information
- Receive a written release from the employee [BIPA defines a "written release" as meaning "informed consent, or, in the context of employment, a release executed by an employee as a condition of employment."]

Illinois employers must have a public written policy that states a schedule for retaining biometric identifiers and biometric information, and guidelines for destroying such data when the purposes for collecting such data have been satisfied or within 3 years of the employee's last interaction with the employer, whichever happens first. An employer is only excused from compliance with its retention policy and destruction guidelines by the issuance of a valid warrant or subpoena.

Illinois employers may not sell, lease, trade or profit from an employee's biometric identifier or biometric information. In addition, they may not disclose or distribute the employee's biometric identifier or biometric information unless the employee consents or production of such data is required under state or federal law or a valid warrant or subpoena.

BIPA also requires Illinois employers to store, transmit, and protect from disclosure an employee's biometric identifiers and biometric information in a manner that meets two standards:

- The first standard is the reasonable standard of care within the employer's industry, and
- the second standard is what the employer uses for storing, transmitting, and protecting confidential and sensitive information.

The law also references "confidential and sensitive information" which is personal data that can be used to uniquely identify individuals or their accounts or property. This means that under BIPA, confidential and sensitive information includes biometric identifiers such as fingerprints and other types of biometric data, and non-biometric data, including, but not limited to, genetic testing data and pass codes which are covered by other laws.

Potential BIPA Liabilities

BIPA gives every Illinois employee a right to sue a private employer who breaches its requirements. The employee must qualify as a person "aggrieved" by the employer's violation of the law. If qualified, the employee may file suit in an Illinois circuit court or add an action under BIPA as a supplemental claim in federal court. An employee who wins a BIPA claim has a variety of possible remedies. If the private employer is shown to have negligently

violated BIPA, the employee can recover liquidated damages of \$1,000 for each violation or actual damages, whichever is greater. For proven reckless or intentional violations, an employee can obtain liquidated damages of \$5,000 for each violation or actual damages, whichever sum is more. In addition, a successful employee can recover attorneys' fees, costs, expert witness fees and other litigation expenses from an Illinois employer. Finally, an employee may obtain an injunction against the employer or other relief that a court finds appropriate.

BIPA allows for a few specific exemptions. For example, an Illinois employer who can show that compliance with the X-Ray Retention Act or the federal Health Insurance Portability and Accountability Act of 1996 and their rules would conflict with BIPA may avoid liability. In addition, BIPA is not to be read as applying to a financial institution or its affiliate that is subject to Title V of the federal Gramm-Leach-Bailey Act of 1999 and its rules. Moreover, BIPA is not to be read as conflicting with requirements imposed by the Private Detective, Private Alarm, Private Security, Fingerprint Vendor and Locksmith Act of 2004 and its rules.

The many private Illinois employers who fall outside the referenced specific boundaries or limitations remain subject to the full scope of obligations and potential liabilities in BIPA.

Illinois Supreme Court Set to Interpret BIPA

The Illinois Supreme Court recently heard oral arguments on an appeal of a ruling by the Second District of the Illinois Appellate Court that dismissed a claim as lacking the required pleading of an injury or negative effect beyond asserting a technical BIPA violation. *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317, ¶128, *leave to appeal granted*, 98 N.E.3d 36 (2018).

In *Rosenbach*, the plaintiff mother purchased a season pass to an amusement park for her son. When the child picked up the season pass, he was fingerprinted without any of the required BIPA disclosures or consents being provided or obtained. The BIPA suit did not allege an actual injury but asserted that the season pass purchase would not have occurred with foreknowledge of the BIPA violations. The *Rosenbach* court read the BIPA term "aggrieved" as requiring an injury in fact, even if non-pecuniary in nature, so as to establish more than a technical violation of the law. The court cited the Mortgage Act as a guide, where a cloud on title is considered a tangible harm. In the absence of a similar tangible harm, the Second District affirmed the dismissal of the complaint.

The Illinois Supreme Court accepted an appeal and has held oral arguments. During those arguments, some comments by the Court indicated it had concerns over the fingerprinting of a minor and the legislative history that references persons made vulnerable by having their biometric identifiers or biometric information compromised. Until the Court rules, however, the extent and type of harm required to plead an action under BIPA remains in question.

In comparison, the First District of the Appellate Court ruled in *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175, ¶¶85-86, that alleged disclosure to an out-of state vendor and mental anguish each constitute a sufficient injury or adverse act to state a BIPA claim. Therefore, the Illinois Supreme Court will seek to resolve the differing interpretations.

While neither *Rosenbach* nor *Sekura* dealt with disputes between an employer and its employees, the disagreement appears in several actions filed in federal court. Like the pending Illinois Appellate Court analyses under review by the Illinois Supreme Court, the federal court rulings disagree over what qualifies an “aggrieved” party to proceed with a BIPA claim. Compare *Dixon v. Washington & Jane Smith Cmty.-Beverly*, 2018 BL 191825, **15-16, 2018 WL 2445292 (N.D. Ill. May 31, 2018) (finding pled claim by employee of actual and concrete injury to right of privacy in and control over biometric data allegations meets “aggrieved” standard for pleading BIPA claim); with *Aguilar v. Rexnord LLC*, 2018 BL 236417, **3-4, 2018 WL 3239715 (N.D. Ill. July 3, 2018) (finding lack of standing due to absence of concrete harm where employee knew his biometric information was being collected to clock in and out without formal notice or consent and where no disclosure was alleged); *Goings v. UGN, Inc.*, 2018 BL 209897, 2018 WL 2966970 (N.D. Ill. June 13, 2018) (same analysis applied to collection of employee fingerprints and hand prints with remand order); *Howe v. Speedway LLC*, 2018 BL 191892, 2018 WL 2445541 (N.D. Ill. May 31, 2018) (granting motion to remand and discussing lack of injury-in-fact analysis).

The sum effect is that all Illinois employers need to monitor and review their policy and consent procedures that they use for obtaining, storing, using, or transferring biometric identifiers and biometric information on their employees. In addition, Illinois employers will need to review with counsel their potential exposure under BIPA after the Illinois Supreme Court decides to read the term “aggrieved” so as to require an injury in fact or something less in order for an employee to proceed with a BIPA claim.

Predicting the outcome of that ruling is difficult. What is reasonable to expect is that if the Illinois Supreme Court uses an English teacher sensibility when reading the term “aggrieved,” the scope of BIPA may be defined within the traditional requirement of pleading an injury-in-fact. If, however, the Illinois Supreme Court relies on the legislative history behind BIPA that specifically references the lack of a remedy for acts that violate BIPA and that increase the risk of identity theft, then a broader reading of BIPA is likely in store for all Illinois employers. For now, the battle between the textual analysis and historical analysis is unresolved and is supportive of Illinois employers who use and follow policies and procedures that comply with BIPA.

If you’re interested in hearing more on BIPA and the *Rosenbach* case, [listen in on a discussion on The Greg & Dan Show](#), 1470 WMBD with Hinshaw Partner Ambrose McCall.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm’s national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People



Aimee E. Delaney

Partner

📞 312-704-3258



Ambrose V. McCall

Partner

📞 309-674-1025

Related Capabilities

Consumer & Class Action Defense

Labor & Employment