Bloomberg Law

Biometric Battles: Rising AI & Employment Litigation Trends

Introduction

2023 saw the second-highest volume of federal lawsuits citing violations of Illinois' Biometric Information Privacy Act (BIPA) in the statute's 15-year history– with artificial intelligence at issue in more than a third (35%) of them.

This report provides a holistic view of 2023's employment-related litigation arising from alleged violations of BIPA.

- A quarterly statistical analysis of the year's employment related federal court cases with BIPA claims
- Statistics on the use of artificial intelligence and biometric surveillance in the workplace
- A BIPA-compliant sample notice for the collection of employee biometrics
- A timeline of important Biometric Information Protection Act Developments

Table of Contents

ANALYSIS

PRACTICAL GUIDANCE

Q1 2023

Why Illinois BIPA Cases Will Spur Big-Damage Lawsuits

by Bridget Roddy
Legal Analyst, Bloomberg Law
Nov. 5, 2023

Two surprising decisions from the Illinois Supreme Court in February are broadening the scope of the state's landmark biometric privacy law, exposing noncompliant employers to the threat of more potential class actions—with larger damage awards—than ever before.

The court clarified that claims filed under the state's **Biometric Information Privacy Act** (BIPA) have a **five-year statute of limitations** and determined that claims **accrue every time** a violation occurs, not just on the first unlawful collection or use.

These holdings likely signal a new era of BIPA litigation by answering questions that have plagued courts for years—and raising a host of additional issues for privacy attorneys. Knowing what these issues are ahead of time can help prevent costly mistakes.

More Plaintiffs, More Problems

When BIPA took effect in 2008, it did so without a statute of limitations, leaving an open question for the courts to decide. Ever since, plaintiffs have argued that BIPA claims have a five-year statute of limitations, based on the state's **"catch-all" provision**, while defendants have argued that the narrower one-year time limit that governs **state defamation-based privacy claims** should apply.

In February, the state supreme court upheld a 2021 Seventh Circuit decision, ***Tim v. Black Horse Carriers*** , which **solidified** a five-year statute of limitations for all BIPA-related claims.

Now that arguments regarding the statute of limitations have been put to rest, aggrieved employees will likely feel more confident about bringing claims against employers who fail to meet the act's exacting standards.

This means that if an employer has been collecting **biometric data** from its employees without proper consent within the past five years, those employees

could have viable claims. While this may seem discouraging to employers who had avoided the statute's requirements in the past, attorneys should encourage their clients not to become apathetic about implementing the necessary policies moving forward.

Any employer—of any size—operating in Illinois and collecting biometric information should have a policy and notice procedure in place. Although any biometric information collected pre-notice and consent is fair game for a claim, once an employee is properly notified and consents to the collection of their information, they have no grounds to bring claims based on any future collection. At least employers will know that if proper policies are implemented now, the threat of BIPA violation claims will be extinguished after five years.

$17 Billion Worth of Fingerprints?

More concerning for employers who fail to comply with BIPA is the Illinois Supreme Court's decision in ***Cothron v. White Castle*** , which found that **claims accrue** every time there is a violation of the statute. A successful class action could now result in damage awards in the billions.

That's the reality White Castle Inc. is facing, following the court's holding that the fast-food chain violated the statute every time an employee was required to use the company's fingerprint-scanning time clock without the mandatory BIPA safeguards in place.

BIPA provides $1,000 in statutory **damages** and $5,000 for willful or reckless violations, as well as the recovery of **actual damages**. It also gives the courts almost unlimited discretion about how to award these damages, although discretion could, in theory, favor the defendant, depending on the deciding judge.

Assuming an employee scans their fingerprint four times a shift (clocking in and out and at break times) five days a week, for 50 weeks per year, a noncompliant employer could be liable for at least $1 million in statutory BIPA penalties in just one year for just that one employee.

With a class size of approximately 9,500 current and former White Castle employees, the court estimated that the damages in *Cothron* may exceed **$17 billion**.

What Comes Next?

Since about 2018, BIPA class actions have followed a general trajectory of being **removed to federal court**, and then being settled. The *Cothron* ruling might change that.

While BIPA settlement amounts have been high, none have come close to the potential billions in damages that White Castle may have to pay. Plaintiffs will be far less likely to settle if a seven-figure damage award is possible.

While it's unlikely the damages in *Cothron* will be quite that high—the state supreme court said that no damage award should **threaten to bankrupt a company**—we will likely see a spike in both damage and settlement award amounts in future BIPA cases.

These higher payouts will likely also create issues between employers and their insurers, through either higher premiums or costly litigation to determine if BIPA-related claims are even covered by their existing policy. The rise in BIPA litigation in the past few years has insurance companies scrambling to **exclude coverage for BIPA-related claims** altogether. While Illinois courts have leaned pro-policyholder in the past, employers **shouldn't count on indemnification** moving forward.

As Illinois employees begin to grasp the impact of these two rulings on their power as plaintiffs, employers will increasingly call upon legal counsel to insulate them before such claims arise by helping them develop robust BIPA-compliant internal policies and notice procedures.

Counsel with employer clients should discuss best practices regarding internal notice and consent policies to ensure BIPA compliance as well as review relevant insurance policies to confirm that BIPA-related payouts are covered.

Bloomberg Law subscribers can find related content on our **Privacy & Data Security** *practice page and our* **In Focus: Biometrics** *page.*

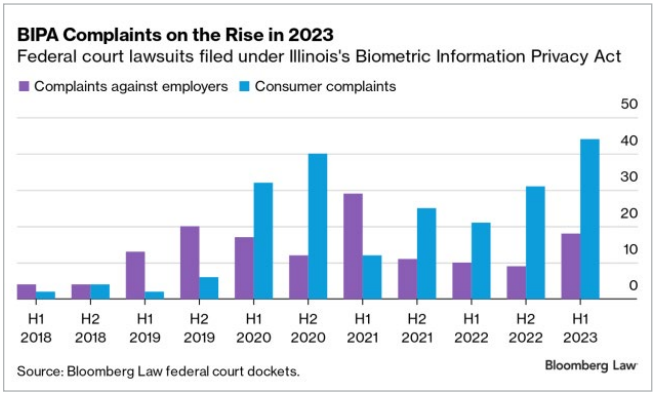
Q2 2023

AI Becomes New Focus of Employer Biometric Lawsuits

by Bridget Roddy
Legal Analyst, Bloomberg Law
Jul. 27, 2023

It's been four months since the Illinois Supreme Court broadened the scope of the Biometric Information Privacy Act (BIPA) with two key rulings, and courts have already seen an increase in BIPA-related complaints. But it also seems that plaintiffs are empowered by BIPA's newfound clarity to take on an increasingly imposing workplace specter: employers' use of artificial intelligence.

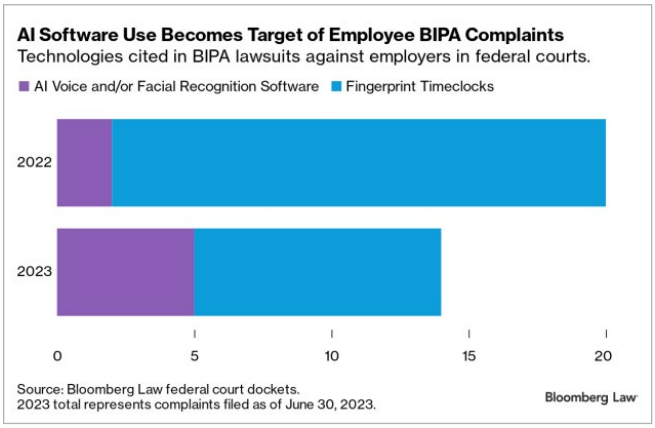
2023 has been a busy year for BIPA litigation, with an increase both in consumer and employment related complaints in federal court. State courts have seen a case increase as well. This rise is likely in part due to February's precedent-setting cases on long-standing questions regarding the act's statute of limitations and claim accrual.



For employers, this increase is accompanied by an emergence of new biometric-related issues in the workplace—largely due to their use of AI in the form of software that recognizes voice patterns and facial geometry.

It is common for consumer complaints to involve facial recognition software used by social media companies, dating apps, and luxury brands. This month, for example, a California-based law firm filed a class action against OpenAI and their primary financial backer, Microsoft. One of the allegations is that the company violated BIPA by illegally collecting the facial geometry of Illinois consumers and using it to train OpenAI's generative AI image creator, DALL-E.

Complaints of this nature have rarely been seen in the employment context. A survey of Bloomberg Law Dockets' employment-related federal court filings from 2018 through 2022 found only two employment related BIPA complaints involving any technology other than fingerprint-scanning time clocks—both filed in 2022. But in the first half of 2023 alone, 36% of all employment-related complaints singled out the use of AI voice or facial recognition software. (The remainder involved fingerprint-scanning time clocks).



This shift suggests two things: Employers are broadening the scope of the biometrics that they collect; and BIPA is being tested as a tool to combat the rise in workplace surveillance seen over the past few years, especially when it comes to employers implementing emerging AI technology.

Plaintiffs Use BIPA to Push Back on AI at Work

With the February rulings leaving fewer uncertainties about how BIPA will be interpreted by the courts, it appears that plaintiffs are more confident in using the law to address emerging concerns about employee privacy. And it's already proving to be expensive for allegedly non-compliant companies.

This year, **Whole Foods Market Group Inc**. was **ordered to pay** $297,000 and **PetSmart** was **ordered to pay** $424,000 to settle class actions brought by warehouse workers who allege their employers required them to utilize the voice recognition product Honeywell Voice without first implementing statutorily required knowledge and consent policies.

Three more **cases** have been brought by warehouse employees—including one **filed Tuesday** against **PepsiCo Inc.**—alleging their employers did not have BIPA-compliant policies in place before requiring employees to utilize the same **Honeywell** product.

Other cases, which are still in the early stages of litigation, show the variety of workplace AI tools that plaintiffs say violate their biometric privacy rights.

One complaint brought by sales associates alleges that, without their knowledge and consent, their employer contracted with a third-party company to use AI to collect the associates' voiceprints during their client calls. ***Cervantes v. Going.io Ltd*** is ongoing in the Northern District of California.

Another was brought by a plaintiff working as a shopper for the on-demand delivery app, Instacart. The complaint alleges the company violated BIPA by improperly collecting, storing, using, and profiting from selfies the shopper was required to upload while working with **Instacart**. These photos were used to verify her identity via third-party facial recognition software. ***Young v. Maplebear Inc.*** is ongoing in the Northern District of Illinois.

Similar complaints were filed against **Amazon Logistics Inc.**, alleging that its Amazon Flex app collected image data from delivery drivers without the company providing a publicly available biometrics policy or obtaining the driver's written consent to the collection, and also profited from this collection. The complaint alleges that this data was used both to verify the identity of the drivers and to "enhance" the company's proprietary AI software, Amazon Rekognition. ***Perry v. Amazon Logistics, Inc.*** and **Young v. Amazon Logistics, Inc.**, are both ongoing in the Northern District of Illinois.

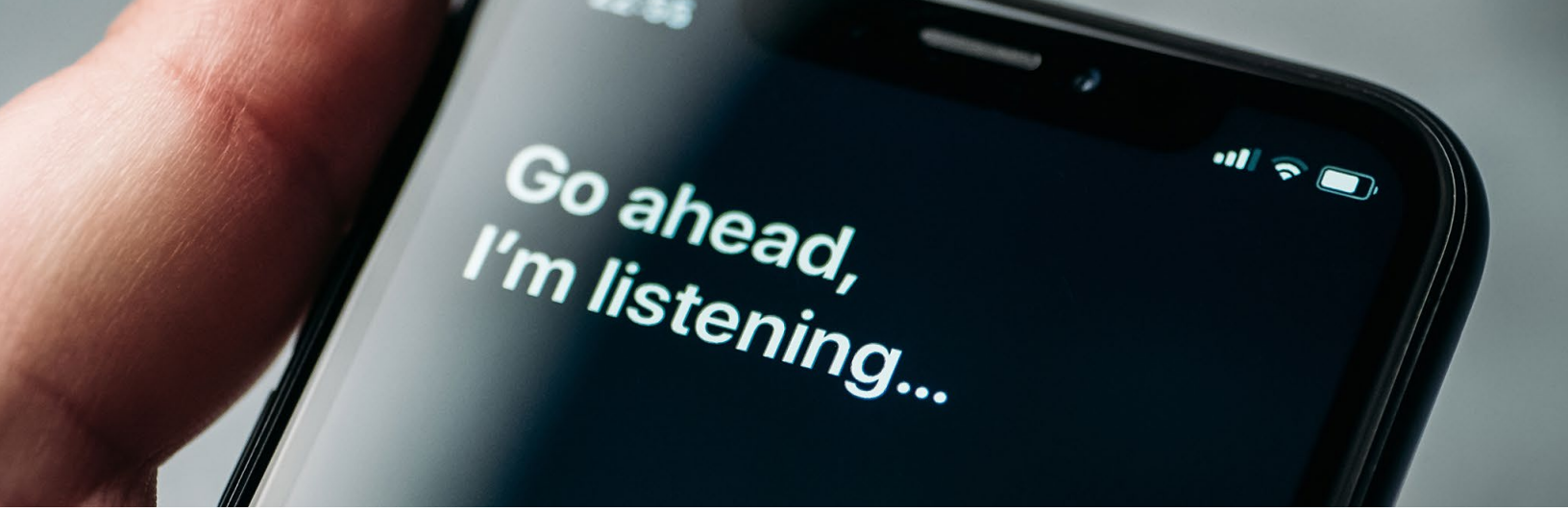
The future of these cases is uncertain, as all previous claims regarding facial geometry and voiceprints have either settled, been dismissed for lack of standing, or are ongoing. BIPA also does not define "**voiceprints**," and companies will likely argue the voice recordings collected don't rise to the threshold of "biometric information."

However, at least in the instances involving Honeywell Voice, the product seems to provide a match for what the court has interpreted "voiceprints" to be. In ***Carpenter v. McDonalds***, the court summarized that, at minimum, voiceprints are unique from simple voice recordings because, unlike "mere recordings," they can be used by AI to detect and analyze human speech by analyzing unique speech characteristics like the pitch, volume, duration, accent, gender, age, and geographic region of the speaker.

Given the settlement amounts to be paid by Whole Foods and PetSmart, it is possible these cases will settle and we won't see a court opinion defining "voiceprints" or "facial geometry" any time soon. However, following the success of the plaintiffs in ***Cothron v. White Castle***, we may see at least one group of plaintiffs risk a **jury trial** with hopes of a **large damage award**.

Now that the courts have clarified the murkier areas regarding BIPA's scope, plaintiffs have begun testing its application to address new issues. As workplace surveillance expands and adapts, it is likely that we will continue to see BIPA applied in more cases where employee biometrics are collected and used by AI.

Bloomberg Law subscribers can find related content on our **Privacy & Data Security** *practice page and our* **In Focus: Biometrics** *page.*



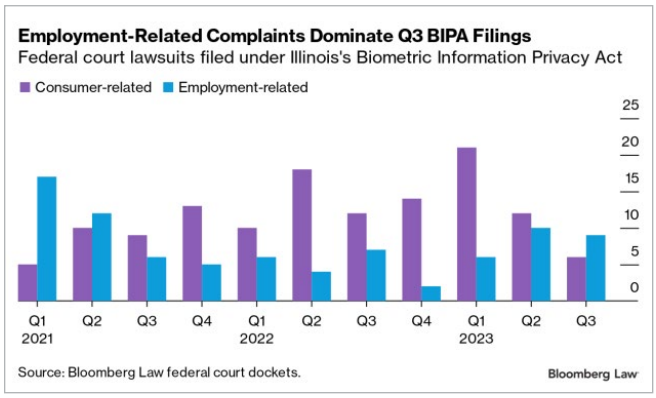
Q3 2023

AI Surveillance Gains Ground in Employees' BIPA Suits

by Bridget Roddy
Legal Analyst, Bloomberg Law
Oct. 26, 2023

Employers are facing a growing number of allegations of illegal collection and use of employee biometrics using AI technology, even though federal court lawsuits citing violations of the Illinois Biometric Information Privacy Act (BIPA) decreased overall in Q3. For the first time in nine quarters, employment-related BIPA filings—driven increasingly by concerns about workplace AI-powered voice and facial recognition software—outnumbered consumer-related filings, according to an analysis of Bloomberg Law dockets.

In the third quarter of 2023, only 15 initial complaints citing BIPA violations were filed in federal court, the lowest level of activity in two years. However, nine of those 15 lawsuits targeted employment-related policies and practices, which is the second-highest quarterly total since Q2 2021 (Ten employment-related complaints were initiated in Q2 of this year.)

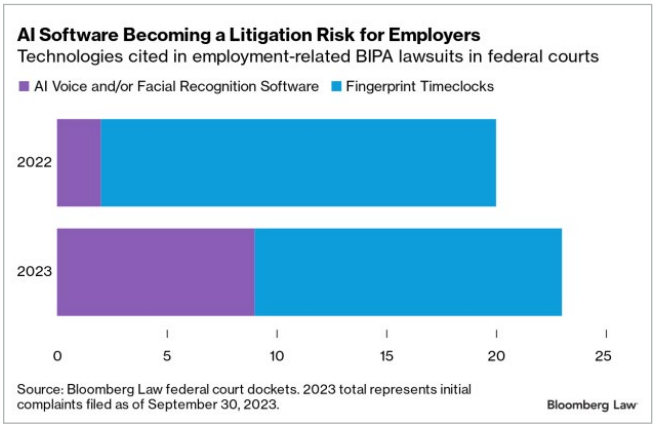


EIPA is one of only two laws in the US that allows employees to bring a private right of action for violations of their privacy. (California recently amended its law to allow a private right of action in limited circumstances). Although its scope is limited to biometric data and to complainants from Illinois, BIPA is regularly cited in privacy-related class actions and federal diversity cases against companies nationwide that involve alleged violations of Illinois employees' biometric privacy.

Mounting Complaints About Voice, Facial Recognition

Within employment-related BIPA complaints, employer use of AI voice and facial recognition software is looming as an emerging threat.

AI was cited in more employment-related BIPA complaints in the first nine months of 2023 than in all of BIPA's 15-year-history. The first two AI-related complaints emerged in 2022, and 2023's count of nine has already more than quadrupled that total. (The majority of employment-related lawsuits continue to involve fingerprint scanning timeclocks, which is not AI technology.)



Pending Litigation Confronts Unclear Definitions

BIPA explicitly governs the collection of biometrics, including voiceprints and facial geometry, but it actually defines neither.

But because BIPA cases settle or are dismissed for lack of standing before they make it to trial, courts haven't really had an opportunity to clarify what the act means when it says "voiceprints" and "facial geometry."

This lack of clarity opens the door for defendants to argue that the voice recordings or facial scans at issue in these complaints don't qualify as biometric information at all. Therefore, they claim, they are not required to make any disclosures or implement any of the safeguards mandated by BIPA before this data is collected.

Courts may get the chance to interpret "voiceprints" in the next year, however. A **class action** against **PepsiCo Inc.** for their alleged illegal implementation of **Honeywell** Voice filed on behalf of warehouse workers will likely to go to trial. Another proposed class action **filed** by workers of Lakes Venture, which does business as Fresh Thyme Market, **survived** a motion to dismiss in late September and is ongoing.

Two cases filed in Q3 also present the courts with an opportunity to define "facial geometry." Both suits involve technology novel to employment-related BIPA complaints: **facial recognition** timeclocks, and facial recognition **dash cam** monitors used to track the performance of drivers.

Another lawsuit, **filed** just this week against Instacart's parent company, **Maplebear**, alleges the company violated BIPA by improperly collecting, storing, using, and profiting from selfies that the shopper was required to upload while working with Instacart. This suit is nearly identical to **one filed** against the company in Q2, which was voluntarily dismissed Sept. 1.

Given historic BIPA litigation trends, it is not unlikely that all of these will settle before a final judgment is handed down discussing the meaning of either term. However, employers should still monitor these types of cases, as one will inevitably make it to trial.

BIPA Litigation Down But Not Out

The third quarter's lull in overall filings shouldn't be taken as a harbinger of diminished BIPA litigation in the future. Historically, fewer filings are made in summer months, making a slowing in Q3 not atypical.

Further, potential plaintiffs may have been holding off on filing lawsuits in Q3 while they waited to see how the **BNSF saga**, involving an unprecedented $228 million judgment for an employer's violation of the act, would shake out. Instead, the parties reached an out-of-court settlement on Oct. 2, leaving several legal questions about BIPA damages still unresolved. So there's no guarantee that employees who have been in wait-and-see mode will suddenly storm the courts with complaints in the fourth quarter.

Regardless of ups and downs in overall litigation patters, this is only the beginning for AI-driven employment-related BIPA lawsuits. Plaintiffs will continue to file claims regarding novel biometric capturing technologies at a faster pace, as they glean more insights from pending AI-related BIPA cases.

–With assistance from Bloomberg Law associate legal analyst Travis Yuille and Bloomberg Law associate content specialist Meghan Thompson.

Bloomberg Law subscribers can find related content on our **Privacy & Data Security** *practice page and our* **In Focus: Biometrics** *page.*

Q4 2023

Employees Fought for Biometric Privacy From AI in 2023

by Bridget Roddy
Legal Analyst, Bloomberg Law
Jan. 16, 2024

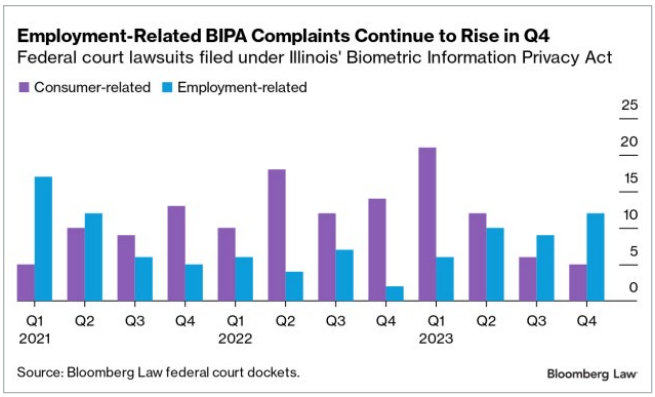
Federal lawsuits citing violations of Illinois' Biometric Information Privacy Act (BIPA) in 2023 reached their second-highest volume in the statute's 15-year history. And for the first time since 2021, employment-related complaints outnumbered consumer-related complaints for two consecutive quarters—with artificial intelligence at issue in most of them.

This flip suggests that businesses may be quick to adopt AI technology to monitor their employees, but they are slow to implement the required data privacy measures that go along with these tools.

Suits Against Employers Continue to Rise

Allegations of BIPA violations in federal court increased in 2023 to 81—up from 2022's 73 and 2021's 77 filings—making it the second most active year since the law was passed in 2008. Federal courts saw the most BIPA filings in 2020, with 106 initial complaints.

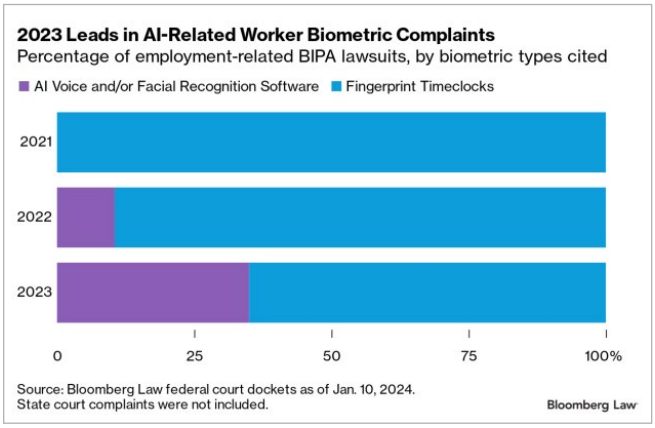
In the fourth quarter, 17 initial complaints involving BIPA violations were filed in federal court, slightly up from 15 in Q3. The number of employment-related complaints was also up from Q3 2023, with a total of 12 compared to Q3's nine. Meanwhile, the volume of consumer-related complaints, which had dominated filings in Q1 2023, has decreased over the year. For the first time since Q1 and Q2 2021, employment-related complaints were in the majority, outnumbering consumer-related complaints in both Q3 and Q4 2023.



Of the 12 employment-related complaints filed in Q4, nine named employers as defendants. The remaining three were filed against companies that develop biometric-collecting technology, which employees are exposed to while doing their jobs.

AI Is a Growing Issue for Employers

In 2021, no employment-related BIPA filings cited AI voice or facial recognition software. The following year, two (10%) of the BIPA filings cited these technologies, and in 2023, 13 (35%) of these complaints alleged the improper use of various facial- or voice-recognition technology powered by AI.



Employees' Unavoidable Exposure to AI

Today's workforce has very **little agency** over its personal data, a concern that's illustrated by the scope of last year's **biometric lawsuits**.

The complaints paint a picture of **increased** biometric surveillance of employees at nearly every stage of their workday: **Fingerprints** are scanned when clocking in and out, and again before and after lunch breaks; voiceprints are collected as call center workers assist customers and **warehouse workers** package orders; the facial geometry of delivery drivers is collected by both employer-controlled devices and recipients' front porch **security cameras**—with nearly all of this data being collected and analyzed by AI.

The complaints also underscore the anxiety this surveillance causes employees who have little control over **or knowledge** of where that personal information is stored and how it's used. Many employees likely aren't even aware that this information is being collected.

BIPA is a remedial statute that is intended to prevent the compromise of biometrics. The law does this by giving individuals control over sharing their personal data after being advised as to how and when it will be collected, stored, and potentially disclosed, the Illinois Supreme Court said in its 2023 decision in **Cothorn v. White Castle System, Inc**.

However, for many employees, the consent to provide their data has become less of a choice and more of a condition of employment.

The law has been in effect since 2008, yet businesses in Illinois continue to implement biometric-capturing technology without either crafting the written collection policies or obtaining the written, informed consent that the law requires.

The number of lawsuits filed each year suggests that many companies have failed to adequately comply with these preventive measures. Instead, businesses appear more willing to employ more cutting-edge technology to survey and collect data on employees and consumers than they are to implement privacy-protecting policies.

Bloomberg Law subscribers can find related content in our **In Focus: Artificial Intelligence (AI)** *page,* **In Focus: Biometrics** *page,* **Practical Guidance: AI in the Workplace**, *and the* **Workplace Privacy Toolkit**.

PRACTICAL GUIDANCE

Employment, Overview - Biometric Information Protection Act Developments

This timeline of Illinois Biometric Information Protection Act (BIPA) litigation features cases and holdings that shape the scope and applicability of the law. Understanding these developments is important for attorneys litigating BIPA violations, privacy professionals working to create compliance programs, and those following the development of other state biometric privacy laws.

BIPA has been used as a template for many state bill proposals governing this issue, though few have passed. Legislators are likely waiting to see what issues will come up during BIPA litigation before they advance these bills.

Establishment of BIPA

The Illinois Biometric Information Privacy Act was enacted on October 3, 2008. It was the first state law that specifically addressed the privacy concerns associated with the use of biometric identifiers.

The text of the law is sometimes perceived as broad or vague, and it is the only US law of its kind, as of July 2023, that allows for a private right of action for any violation of the act. The law has never been amended, and a long string of court opinions are necessary to understand how the law applies to covered entities.

The law allows aggrieved individuals to bring a claim against a private entity for any of the following violations:

- 15(a) violation—failure to develop a written policy, make that policy available to the public, or meet the statutory requirements for retention and destruction of the collected biometric identifiers.
- 15(b) violation—obtaining biometric identifiers without informing the individual of the collection, disclosing the specific purpose of the collection and the length of time it will be held by the collecting party, or obtaining a release in writing.
- 15(c) violation—selling, leasing, trading, or otherwise profiting from the use of an individual's biometric identifier.
- 15(d) violation—disclosing a person's biometric identifier without their consent, unless required to by law.
- 15(e) violation—failing to exercise a reasonable standard of care, pursuant to the collector's industry standard, when handling biometric identifiers.

First Cases Arise Under BIPA

Though the law was enacted in 2008, the first lawsuit was not brought until 2015 when several plaintiffs used it to challenge Facebook's photo scanning technology. It took nearly six years to resolve.

This section includes the first claims brought under BIPA, organized by consumer claims and employment related claims. These first cases allege violations of 15(a) and 15(b), which continue to be the litigated issues.

Consumer Cases

The first cases to claim the biometric privacy rights of consumers under BIPA were filed in state court in April 2015. In three individual lawsuits, plaintiffs alleged Facebook violated 15(b) by failing to notify them that their facial geometry was being collected and used in the website's photo tagging technology, and 15(a) by failing to provide a public policy related to the collection.

The suits were consolidated and transferred to the Northern District of California in San Francisco. *In re Facebook Biometric Information Privacy Litigation*, No. 3:15-cv-03747 (N.D. Cal. Aug 17, 2015).

On Feb 26, 2021, the litigation resolved with a historic $650 million settlement, the largest US consumer data privacy settlement to date.

The Ninth Circuit found the plaintiffs had established Article III standing by analogizing a privacy injury from a BIPA violation to a privacy injury at issue in a tort claim for invasion of privacy. Because violations of the statute "actually harm[ed] or pose a material

risk of harm to those privacy interests," the plaintiffs had alleged an injury in fact sufficient to confer Article III standing. Patel v. Facebook, Inc., **932 F.3d 1264** (9th Cir. 2019).

Employee Cases

In November 2017, the first employee complaints alleging BIPA violations were filed in federal court. All five complainants allege that employers violated sections 15(a) and 15(b) in their collection of employee fingerprints for time keeping purposes. **Dixon v. The Washington and Jane Smith Community-Beverly**, No. 1:17-cv-08033 (N.D. Ill. Nov 06, 2017); McGinnis v. US Cold Storage, Inc., No. 1:17-cv-08054 (N.D. Ill. Nov 07, 2017); **McDonald v. ABM Industries Inc.** , No. 1:17-cv-08154 (N.D. Ill. Nov 10, 2017); **Fernandez v. Kerry, Inc., No. 1:17-cv-08971** (N.D. Ill. Dec 13, 2017); and **Kislov v. American Airlines, Inc., No. 1:17-cv-09080** (N.D. Ill. Dec 18, 2017).

On February 10, 2021, home security company ADP agreed to a $25 million settlement to employees for alleged BIPA violations. At the time, it was the largest settlement amount in a BIPA case and to date is still the largest amount awarded to employee plaintiffs. Kusinski v. ADP LLC, 2017-CH-12364 (Cir. Ct. Cook Cnty. Feb. 10, 2021).

Precedential Cases

The following section discusses significant rulings from the US Court of Appeals for the Seventh Circuit and the Illinois Supreme Court that have helped shape the application of BIPA. The courts have provided clarity regarding standing, injury, and preemption and established a statute of limitations for claims.

Standing-Related Precedent

Bryant v. Compass Grp. USA, Inc., **958 F.3d 617** (7th Cir. 2020).

- The Seventh Circuit held that a company's failure to disclose a policy generally, a violation under **section 15(a)**, is not enough to confer Article III standing. This is because it is a duty owed to the public generally, and not an individual harm.
- BIPA does not include a statute of limitations. The Seventh Circuit held the five-year "catch all" statute of limitations applied to the law. **735 ILCS 5/13-205**.

Fox v. Dakkota Integrated Sys., LLC, **980 F.3d 1146** (7th Cir. 2020)

- A failure to develop and comply with a biometric collection and retention policy in violation of Section **15(a)** creates a particularized harm that confers Article III standing.
- 7th Cir. held that the unlawful collection or retention of biometric data alone, a violation of Section **15(b)**, is not a concrete and particularized harm to confer Article III standing.

Thornley v. Clearview AI, Inc., **984 F.3d 1241** (7th Cir. 2021).

- The Seventh Circuit found that there was no standing in a case alleging violations of Section **15(c)** when the plaintiff alleges only a "bare statutory violation" of 15(c), and not a particularized harm.

Injury-Related Precedent

The Illinois Supreme Court clarified the statute's "aggrieved person" standard in *Rosenbach*. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, 432 Ill. Dec. 654, **129 N.E.3d 1197**.

- Illinois Supreme Court held that violations of **Section 15(b)** actually harmed or posed a material risk of harm to an individual's privacy interests, creating an "injury in fact" to confer statutory standing.
- The Illinois Supreme Court concluded that an individual qualifies as "aggrieved" if their rights under the act have been violated. They are not required to prove any additional adverse effect or actual injury to be entitled to seek liquidated damages and injunctive relief under the BIPA.

The Northern District Court held that an "active step" is required for a Section 15(b) claim to succeed. *Jones v. Microsoft Corp.*, No. 22-CV-3437, **2023 BL 6184** (N.D. Ill. Jan. 9, 2023).

- The court found that a violation of Section 15(b) "requires something beyond possession," meaning the defendant must have undertaken some effort to collect or obtain biometric identifiers or information. **Id**.

The Illinois Supreme Court established a standard for BIPA claim accrual. Cothron v. White Castle Sys., Inc., 2023 IL 128004.

- The Illinois Supreme Court affirmed a lower court holding that claims accrue at each violation, not just on first unlawful collection

Preemption-Related Precedent

BIPA claims are preempted by the Railway Labor Act (45 U.S.C. § 152). *Miller v. Southwest Airlines Co.*, 926 F.3d 898 (7th Cir. 2019).

- Employees and employers bound by the Railway Labor Act must peruse avenues to remedy established by the act regarding alleged violations of BIPA.

BIPA claims brought by employees covered by a collective bargaining agreement are preempted under federal law. Fernandez v. Kerry, Inc., 14 F.4th 644 (7th Cir. 2021). The Illinois Supreme Court agreed with this finding in Walton v. Roosevelt Univ., 2023 IL 128338 (Ill. Mar. 23, 2023).

Statute of Limitation-Related Precedent

The Seventh Circuit held BIPA had a 5-year statute of limitations. Bryant v. Compass Grp. USA, Inc., 503 F. Supp. 3d 597 (N.D. Ill. 2020).

- BIPA does not include a statute of limitations. The Seventh Circuit held that the state's Code of Civil Procedure five year "catch all" statute of limitations applied to the law. 735 ILCS 5/13-205.

The Illinois Supreme Court also found a five year statute of limitations applies to BIPA claims. Tims v. Black Horse Carriers, Inc., 2023 IL 127801.

- The state's top court affirmed a lower court holding establishing a five-year statute of limitations for BIPA claims.

PRACTICAL GUIDANCE

Employment, Checklist - Biometrics Enforcement by the FTC

Editor's Note: On May 18, 2023, the US Federal Trade Commission (FTC) issued a policy statement addressing biometric information misuse and potential harms to consumers. The FTC has stated that this guidance applies to biometric use generally, regardless of the context, though it does not specifically mention workplace use. It is best practice for employers to assume employees fall under the FTC's definition of "consumers" until advised otherwise.

This checklist covers best practices to ensure that an employer's use of biometric information technology does not violate Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in commerce.

For information on state biometric privacy laws and developments, see In Focus: Biometrics and Practical Guidance: Privacy & Data Security.

When developing effective and compliant biometric use policies, attorneys should ask:

Does the employer's use of biometric information constitute a deceptive trade practice? While deceptive trade practices usually apply to marketing efforts, the FTC statement also includes, "deceptive statements about the collection and use of biometric information." If employers plan to collect biometrics from their employees they must do so in a non-deceptive fashion, specifically disclosing the purpose of the collection and using the biometric identifiers only for that purpose.

This will be familiar to employers already complying with the Illinois Biometric Information Privacy Act, which requires disclosure of a specific purpose before collection of biometrics can take place.

Does the employer's use of biometric information constitute an unfair trade practice? The legal test for determining whether a practice is unfair is whether the use will cause, or will likely cause, substantial injury to consumers that is not easily avoidable by the consumers themselves and the potential for injury is not outweighed by the countervailing benefits to consumers or competition. Biometric information is highly personal and unique, meaning that a data breach or accidental disclosure of these details could result in severe harms to an individual.

To determine if an employer's use amounts to an unfair trade practice, consider the following:

Can an employee opt out of the collection of their biometric identifiers? The most conservative approach to using biometrics in the workplace would be to allow employees to opt out of biometric collection. The FTC's statement says that harms associated with collecting biometrics "are not reasonably avoidable by consumers if the collection and use of such information is not clearly and conspicuously disclosed or if access to essential goods and services is conditioned on providing the information."

Conditioning employment on the employee's consent to the collection of their biometrics may violate Section 5 because the employee can't easily avoid potential harms related to the use of their biometrics. The FTC hasn't provided guidance on this specific issue.

If an employer adopts a policy that requires biometric collection as a pre-requisite to employment, the employer must at the very least disclose the collection and use of the information clearly and conspicuously. It would also require heightened security of the biometric information to ensure that the benefit of using the technology will outweigh the risks.

Does the employer have reasonable data security practices in place to guard against data breaches and prevent accidental disclosure of biometric identifiers? Employers should ensure that any collected biometric information is protected from unauthorized access—whether that access stems from an external cybersecurity breach or unauthorized internal access by employees, contractors, or service providers.

Has the employer assessed foreseeable harms before collecting biometric information? Businesses should consult counsel, human resources, and IT professionals to assess potential risks associated with collecting, using, and storing biometric information. This assessment should consider privacy concerns, the technological components required to collect biometrics, and bias concerns by testing for any differential performance across demographic groups. This assessment may reveal that the purpose for collecting biometric data can be more efficiently and safely achieved using a less sensitive identifier.

Does the employer have procedures in place to mitigate foreseeable risks? If an employer decides collecting biometric information is reasonable to meet the organization's goals, it must take measures to address the risks discovered during the assessment phase. This may include designating a specific person or team to handle issues that arise and ensuring all relevant personnel is aware of their responsibilities in the event of a data breach or accidental disclosure. It is important to consider specific state privacy law requirements regarding data breach risk mitigation and reporting requirements.

Has the employer provided adequate training for employees and contractors who will have access to the technology and/or data? Ensuring that employees receive sufficient training about the collection tools and data management is an essential part of risk mitigation. This training should be done before collecting biometric information, and periodic additional trainings may be required for employees to stay up to date on proper use of the tools and data.

Is it clear to employees when and why their biometric information is collected? The FTC has signaled that "engaging in surreptitious and unexpected collection or use of biometric information may, in some situations, be unfair in and of itself." Employers must make their employees aware of when and why their biometrics are being collected. This may be done by including a consent form to employees during onboarding, like those required by the **Illinois Biometric Privacy Act**.

A sample of this consent form is available here: **Employment, Sample Notice - Biometrics Collection (Annotated)**.

Has the employer fully evaluated the practices and capabilities of any third parties who may be given access to employee biometric information? Employers will often use a third party's equipment to process or store employee biometric information, such as a fingerprint scanning timeclock. Before incorporating this technology, employers should consult with counsel, IT, and human resources to determine which programs best fit the organization's needs and present the least amount of risk.

PRACTICAL GUIDANCE

Employment, Sample Notice - Biometrics Collection (Annotated)

Editor's Note: This sample notice is intended to (1) inform employees of the employer's biometric information collection, use, and destruction policy and (2) obtain informed consent to that collection, use, sharing, and/or disclosure.

It is drafted to comply with the **Illinois Biometric Information Privacy Act** (BIPA), which has strict requirements for private entities that collect biometric information or identifiers. See **740 ILCS 14/10**. Other states have similar, though less encompassing, notice requirements. Consult the law in your jurisdiction for applicable requirements.

Employers must provide this notice, in addition to a full internal biometric use policy, to all employees. Employers must obtain written, informed consent from new employees before collecting any biometric identifiers. Employers must notify and obtain written consent from current employees before any changes to the policy take effect.

For more guidance on BIPA Compliance, see **Data Collection & Management, Checklist - Biometric Privacy Compliance (Annotated)**.

For information on state biometric privacy laws and developments, see **In Focus: Biometrics**, **Practical Guidance: Privacy & Data Security**.

Notice to Employees of [Employer's] Biometric Information Collection, Storage, Use and Destruction Policy

This notice is intended to give you an overview of what kind of biometric information is being collected, why it is being collected, how it is stored, used, and destroyed, as well as where you can find more information about [Employer's] policy. If you have not fully read [Employer's] Biometric Information Collection, Storage, Use and Destruction Policy, please do so first before returning to this notice.

You are receiving this notice because you are a new or current employee and [Employer] has updated their existing policy. As a condition of your employment, you must read, acknowledge, and give consent to the terms of [Employer's] policy. If you have questions, please contact [Contact Person Name and Contact Information].

Comment: Most state laws require private entities to designate specific points of contact for handling questions about their Biometric Information Policy. This could be a manager, HR professional, or in-house counsel, for example.

By signing this notice, you are signaling that you give informed consent to [Employer's] collection and use of your biometric data as it is outlined in the policy. You will be notified in writing before any changes to this policy are implemented.

What is [Employer's] specific purpose for collecting my biometric Information? [Employer] reserves the right to collect, use, and store, either internally or via a third party, an employee's biometric information for the purposes of [EXAMPLE: verifying Employee's identity and for timekeeping purposes]. By signing this notice, [Employee] consents to collection for these purposes.

Comment: Policies and notices must include the "specific purpose," or explicit reason why biometric information is collected, stored, and used.

In this section, you should specify current and reasonably foreseeable purposes for which the company utilizes or may utilize the employee's biometric information. If the scope of purposes included in the original release expands, additional consent should be obtained before using the biometric data for a materially different purpose. For more state biometric data laws, see **U.S. State Overview - Privacy & Data Security Chart**.

How will my biometric information be collected? Biometric information will be collected in the form of [Example: Employee scanning their fingerprint at the timecard machine when clocking in at the beginning of their shift, at break times, and when clocking out].

Comment: This section informs employees of the method(s) used to collect their biometric identifiers and biometric information. Commonly, employers will collect an employee's biometric information through timekeeping machines that identify employees using their fingerprints.

Include any foreseeable method biometrics will be collected for the enumerated specific purposes. These may include devices that perform facial scans to open work or palm print readers to access doors.

How will my biometric information be stored and for how long? This information will be stored by [Entity Name] for [Established Period], but not to exceed three years from [Employer's] most recent interaction with the Employee. Upon the employee leaving [Employer] or termination, [Employer] must destroy their biometric identifiers in a timely manner and/or direct the above third party to do so.

Comment: Policies and notices must include the length of time the biometric information will be collected, stored, and used.

This section tells the employee where their information will be stored and for what duration. Biometric information is typically stored by a third-party vendor (for example, the company who operates the timecard machine or your payroll processor). Be sure to include that entity's name in your policy.

States laws regulating the collection and use of biometric information usually allow data to be stored for a "reasonable amount of time." Be aware of the statutory guidelines for retention in your state. For example, in Illinois, information may not be stored for more than three years (**IL 740 ILCS 14/15**) and in Texas, for no more than one year (**Tex. Bus. & Com. Code § 503.001(c)(3)**).

For more state biometric data laws, see **U.S. State Overview - Privacy & Data Security Chart**.

What is [Employer's] policy on disclosing my biometric information to third parties? How will [Employer] dispose of my information once it is no longer needed? Employee consents to [Employer] disclosing or disseminating Employee's biometric information to third parties for disclosed business purposes or when required by law and acknowledges that the Employee's information will be retained and destroyed according to the methods detailed in [Name of Policy].

Comment: This section covers the Employer's retention, third-party disclosure, and destruction of employee biometric information policies and procedures. It should reflect the Employer's internal policy regarding retention, disclosure, and destruction of biometric information. Consider, if an employer were to be sold or go out of business, what employees would need to know to determine who is in possession of their private biometric identifiers and what data the entity possesses.

There are also some legal reasons disclosure may be required to law enforcement or for other legal reasons. These are usually enumerated within the statute. To determine when disclosure may be legally required, consult your state's statute here: **U.S. State Overview - Privacy & Data Security Chart**.

For more guidance on drafting a policy that provides employees with sufficient information to be able to give informed consent, see **Data Collection & Management, Checklist - Biometric Privacy Compliance (Annotated)**.

Where can I find [Employer's] Biometric Information Collection, Storage, Use and Destruction Policy for future reference? [Employer's] Biometric Information Collection, Storage, Use and Destruction Policy will be made available for employees to reference. It can be located [Example: near the timeclock in the break room and by request from management].

Comment: BIPA requires that a company's retention and destruction policy be publicly available. **IL 740 ILCS 14/15**. This refers to the full internal policy, not only the parts included in this notice. A best practice would be to post this policy alongside other required posters, typically in a break room or where employees clock in/out. Alternatively, the policy could be accessible via an online employee portal or publicly on the employer's website. It is essential that employees be made aware of where the full policy can be located and that it is always accessible.

Employee Consent & Acknowledgment of Policy

I, _____, have read [Employer]'s Biometric Information Collection, Storage, and Use Policy, and I consent to its terms. I understand that [Employer] may require the collection of my biometric information (e.g., a retina or iris scan, fingerprint, voice print, hand scan, facial geometry), and that my information will be stored, collected, used, disclosed, and destroyed pursuant to this policy. By signing, I acknowledge that I have been properly notified of the collection of my biometric information and I consent to Employer using, disclosing, and/or disseminating my biometric information and identifiers for the purposes laid out in the policy.

Signed: _____

Dated: _____

Comment: Consent should be obtained in either hard copy paper form or digital file. Don't rely on "passive consent" obtained while setting up an employee's timeclock profile. Employees should keep one copy of this notice for their records and management should keep a copy on file.

A release that is executed electronically satisfies the "in writing" requirement for BIPA. In Illinois, in the context of employment, "written release" means a release executed by an employee as a condition of employment. This may be signed by the employee or by an agent of the employee on their behalf. 740 ILCS 14/10. Recent case law has clarified that employees who are represented by a union consent to the biometric information policy included in their collective bargaining agreement.

For an alternative version of an employee consent to collection, see **Employment, HR Form - Consent to Collection of Biometric Data**.

About Bloomberg Law

Bloomberg Law helps legal professionals provide counsel with access to action-oriented legal intelligence in a business context. Bloomberg Law delivers a unique combination of Practical Guidance, comprehensive primary and secondary source material, trusted content from Bloomberg Industry Group, news, timesaving practice tools, market data, and business intelligence.

For more information, visit **pro.bloomberglaw.com**.

Bloomberg Law

© 2024 Bloomberg Industry Group, Inc. 0224 1009900