Tucker Ellis LLP

Are You Using Biometric Technology in Illinois? Tread Carefully!

By: Greg Abrams, Partner

Are You Using Biometric Technology in Illinois? Tread Carefully!

Products using biometric technology – such as fingerprints or facial scans – have become more widespread over the last decade, and this trend shows no signs of slowing. According to one source, the global biometric technology market size was valued at $34.27 billion in the U.S. in 2022, with expected 20% growth into 2030. But this increased prevalence of biometrics brings potential legal risk. And perhaps nowhere is this threat greater than in Illinois.

This article discusses the Illinois law regulating biometrics, its potential landmines, and recent court developments in this area.

Background to the Illinois Biometric Information Privacy Act

In 2008, Illinois enacted the Biometric Information Privacy Act, or "BIPA."[1] The catalyst was when a company went into bankruptcy, and consumers feared what may become of the purported biometric data, which by its nature is unique and unchangeable, that this company maintained. As the Illinois legislature explained, "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the

individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[2]

Accordingly, through BIPA, Illinois required multiple procedural steps be followed for entities that collect or use biometrics in Illinois, finding that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[3]

In the last several years, there has been an avalanche of class action lawsuits alleging BIPA violations, namely that its procedural requirements were disregarded by companies collecting biometrics from Illinois employees and consumers. These lawsuits have implicated multiple types of alleged biometric devices, including timeclocks that scan an employee's finger for time entry, voice recognition software, door entry systems, remote monitoring software, and even cell phone applications for trying on glasses or simulating new hair styles.

Some major companies have agreed to massive settlements over alleged BIPA violations. Facebook agreed to pay $650 million to resolve a lawsuit primarily about its photo face-tagging technology. TikTok agreed to resolve multiple lawsuits brought under BIPA for $92 million. And in the first BIPA class action to proceed through trial, a judge awarded $228 million for alleged BIPA violations to a class of 45,000-plus people (although, as noted below, this judgment was later vacated).

To Whom Does BIPA Apply?

BIPA's requirements can apply to any individual, company, or organization (excluding government agencies).[4] The entity need not be in Illinois; thus, a company based in Missouri could still be subject to BIPA. But courts generally have concluded that any alleged biometric collection must have taken place *in* Illinois.

What Types of Information is Covered under BIPA?

BIPA obligations apply to two types of biometric data.

First, BIPA covers a "biometric identifier," which is defined as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.[5] BIPA though expressly *excludes* multiple items. One such exclusion is for photographs, as these do not implicate biometrics.

Second, BIPA applies to "biometric information," which is information – regardless of how it is captured – based on an individual's biometric identifier that is used to identify an individual.[6] For example, a scan of a photograph that captures facial geometry for identification purposes potentially could be considered "biometric information," even though the underlying photograph itself does not contain biometrics.

What does BIPA require?

Notice: *Before* collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a biometric identifier or biometric information, the entity must provide *written* notification that (a) biometrics are being collected or stored, and (b) identifies the specific purpose and length of time for which such data is being collected, stored, and used.[7]

Authorization: *Before* collecting this information, the affected individual must provide a *written* release authorizing this activity.[8] The notice and authorization/release can be within the same document.

Retention Schedule and Destruction: An entity in possession of biometrics also must develop a written retention schedule and guidelines for permanently destroying this information when the initial purpose for collecting or obtaining this information has been satisfied, or within three years of the individual's last interaction with the entity, *whichever occurs first*.[9] Thus, if

biometric information is collected from an employee (such as through an alleged biometric timeclock), it typically needs to be purged once that individual terminates employment.

Additionally, the retention schedule must be "available to the public."[10] It is not clear what this term means. Some companies post this schedule on their websites or include it in employee handbooks to meet this obligation.

Other Obligations: Other BIPA requirements include that an entity may not sell, lease, trade, or otherwise profit from someone's biometric information; may not disclose this information without consent (subject to certain exceptions, such as pursuant to a court order); and must use a "reasonable standard of care" to protect this information, including with the same rigor with which it protects other confidential and sensitive information.[11]

What are the Consequences of Not Complying with BIPA?

In short, they can be severe. That is because BIPA provides a private right of action to anyone "aggrieved" by a BIPA violation.[12] So unlike in other states (such as in Texas and Washington), where companies may be fined civilly for violations, in Illinois, an individual can bring a class action lawsuit against a non-compliant company.

Moreover, BIPA imposes liquidated damages for violations. An entity that "negligently" violates a BIPA provision could be on the hook for $1,000 for each violation.[13] An "intentional" or "reckless" violation could lead to $5,000 for each violation.[14] A prevailing plaintiff also may recover attorneys' fees and cost, as well as an injunction (such as to mandate BIPA compliance).[15]

Critically, in January 2019, the Illinois Supreme Court held (in *Rosenbach v. Six Flags Entertainment Corp.*)[16] that these damages may be recovered even if the plaintiff did *not* suffer any actual harm. Consequently, even absent identity theft (or even a threat of identity theft) or

other tangible harm, failure to follow the procedural steps addressed above could lead to these statutory damages – which, in a class action, could be substantial.

Recent Court Developments Favor Plaintiffs in BIPA Litigation.

In addition to the *Rosenbach* case, the Illinois Supreme Court recently has weighed in on two issues concerning BIPA – both of which favor plaintiffs, thereby further opening the floodgates for class action litigation.

One issue concerned the appropriate statute of limitations for a BIPA claim. BIPA does not set forth a statute of limitations, which means a court must apply the most analogous limitation period. Defendants had argued for a one-year limitations period under 735 ILCS 5/13-201, which applies to "publication of matter violating the right of privacy." The plaintiff's bar countered that the five-year "catch-all" limitations period set forth in 735 ILCS 5/13-205 should control. In February 2023, in *Tims v. Black Horse Carriers Inc.*,[17] the Illinois Supreme Court concluded that the *five-year* statute of limitations was most appropriate, and that this limitations period applies for any BIPA claim – meaning an individual has five years (rather than only one) to bring suit under BIPA.

Just two weeks later, the Illinois Supreme Court clarified *when* this statute of limitations starts to run, or "accrues." That is, it addressed the question of whether the clock to file suit starts running the *first time* someone's biometrics were collected or transmitted, or *each time* that occurs. In a 4-3 decision, the Illinois Supreme Court held in *Cothron v. White Castle System, Inc.*,[18] that the statute of limitations begins to run *each time* a private entity collects or transmits an individual's biometrics in violation of BIPA, rather than at the first such collection or transmission.

The upshot of the *Cothron* decision is that potential plaintiffs have more leeway to claim BIPA violations. For example, in the context of alleged biometric timekeeping systems, an

individual can bring a BIPA claim if they can allege an unlawful scan or transmission within five years of *last* using the machine – even if the *first* use was more than five years earlier. This means more potential plaintiffs and larger potential class sizes in BIPA class actions.

A Silver Lining (Perhaps) for Companies.

Left unanswered in *Cothron* was whether its conclusion that BIPA may be violated with each unlawful collection affects how damages are calculated, or if its findings were limited only to the issue of accrual of the statute of limitations. On this point, the Illinois Supreme Court recognized the potential for "astronomical" awards or "annihilative liability" if damages could be recovered for every alleged unlawful scan or transmission (i.e., in the context of that case, up to $5,000 each time any employee scanned their finger on a timekeeping system). The Court stated though that it was constrained to follow clear statutory language and that large potential damages awards incentivize companies to comply with BIPA.

Nonetheless, the Court did *not* expressly endorse this approach to damages. Rather, in what could be a silver lining for defendants, the Court made clear that judges in class actions possess discretion to fashion damages as appropriate. Moreover, the Court noted that BIPA "appears" to make damages "discretionary rather than mandatory," since it provides that a prevailing party "may recover" (rather than "shall recover") damages.[19] And the Court also warned against damages awards "that would result in the financial destruction of a business."

Following this decision, in the one BIPA case that went to a jury verdict (*Rogers v. BNSF Railway Co.*), the Northern District of Illinois federal court vacated a $228 million damages award and ordered a new trial on the issue of damages. The court relied upon the Illinois Supreme Court's commentary that the amount of damages is discretionary, not mandatory. As a result, the damages award after a finding of liability is a question for the jury.

This *BNSF* decision keeps open the option for companies to argue against the application of a strict $1,000/$5,000 per violation framework to avoid unreasonable damages awards. The prospect of an award other than automatic liquidated damages may help curb excessive settlement demands from the plaintiff's bar. On the other hand, it remains to be seen whether entrusting this decision to a jury could lead to more reasonable damages awards or assuage the lingering uncertainty of how damages may be calculated under BIPA.

Conclusion

For companies doing business in Illinois, it is imperative to take stock of whether they are engaging in activity that may implicate BIPA. This could include having employees in Illinois who use timeclocks with finger-scans, or deploying technology in Illinois that potentially captures biometrics. If so, companies should move swiftly to implement a BIPA-compliance process as class actions under this statute continue to be filed at a breakneck pace.

---

[1] 740 ILCS 14/1 *et seq.*
[2] 740 ILCS 14/5(c).
[3] 740 ILCS 14/5(g).
[4] 740 ILCS 14/10.
[5] 740 ILCS 14/10.
[6] 740 ILCS 14/10.
[7] 740 ILCS 14/15(b)(1), (3).
[8] 740 ILCS 14/15(b)(3).
[9] 740 ILCS 14/15(a).
[10] 740 ILCS 14/15(a).
[11] 740 ILCS 14/15(c), (d), (e).
[12] 740 ILCS 14/20.
[13] 740 ILCS 14/20(1).
[14] 740 ILCS 14/20(2).
[15] 740 ILCS 14/20(3), (4).
[16] 2019 IL 123186.
[17] 2023 IL 127801.
[18] 2023 IL 128004.
[19] 740 ILCS 14/20.