Published on *The National Law Review* https://natlawreview.com

Illinois Supreme Court Expands Private Entities' Exposure to Liability & Damages

Article By:

Lisa Handler Ackerman

Michael J. Duffy

Joseph M. Dybisz

Michael J. O'Malley

Joseph J. Stafford

On February 17, 2023, in a 4–3 decision, the Illinois Supreme Court ruled that a separate claim accrues under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. (BIPA) *each time* a person scans or transmits their biometric information rather than simply the first time. In Cothron v. White Castle, defendant White Castle argued BIPA claims accrue only the first time a person's biometric information is collected or disclosed without consent. By contrast, plaintiff Latrina Cothron argued each individual scan constitutes a separate BIPA violation. In agreeing with Cothron, the Illinois Supreme Court unquestionably expanded the potential exposure of private entities to both liability and damages.

Background

Cothron, a manager of a White Castle restaurant in Illinois, alleged that White Castle obtains an employee's fingerprint and stores it in its database. Thereafter, employees must use their fingerprints to access paystubs or White Castle computers. White Castle contracted with a third-party vendor to store the biometric data in an off-site database and verify each scan. Cothron alleges this biometric-collection system violated sections 15(b) and (d) of BIPA, which prohibit the unauthorized collection and disclosure of a person's biometric information, respectively. After taking the case under advisement, the United States Court of Appeals for the Seventh Circuit certified a question to the Illinois Supreme Court seeking clarity on the issue.

The Ruling

In short, the Illinois Supreme Court held *each separate scan* of a person's fingerprint constituted a "collection" under section 15(b), and *each separate disclosure* of a person's biometric information to

a third-party constituted a "dissemination" under section 15(d), regardless of whether the disclosure is to the same third party. The Court expressly rejected White Castle's argument that claim accrual is limited to only the *first* instance biometric information is collected or disclosed without consent, reasoning that the plain language of the statute supported a per-violation basis, which would incentivize compliance with BIPA.

Importantly, the Court acknowledged that its holding may lead to "annihilative liability" – for example, potentially subjecting White Castle to "astronomical" damages **in excess of *$17 billion***. Nevertheless, the Court reasoned that despite these potentially "unjust" results, the legislature was best positioned to remedy this effect under the BIPA statute.

Three justices dissented to the majority opinion, pointing to a prior landmark BIPA decision[1] in which the Illinois Supreme Court identified the "precise harm" the legislature sought to prevent as the loss of an individual's right to maintain their biometric information as private. The dissent, therefore, reasoned that claim accruals should be limited to the *first* violation because that is when a person loses their privacy interest in their biometric information. The dissent also criticized the majority's failure to take into account the ruinous effect of its ruling on defendants as inconsistent with the intent of the Illinois Legislature. The dissent posited that the Legislature did not intend to destroy Illinois businesses nor incentivize the complete abrogation of the collection and use of biometric information.

Analysis

The *Cothron* decision, at least for now, is a narrow but clear victory for BIPA plaintiffs. For businesses, the cost of receiving clarity from the state's highest court comes in the form of increased exposure to potentially ruinous damages awards. For instance, in the wake of this ruling, White Castle's potential exposure increased from the not insignificant sum of $50 million (if only the first scan was actionable) to the astronomical, and seemingly unrealistic, sum of ***$17 billion***. Other businesses will face the potential of similar annihilative liability.

By way of example, an earlier BIPA case, *Rogers v. BNSF Ry. Co.*, resulted in a jury verdict imposing damages of $228 million on the defendant based on a "per employee" violation. In the wake of this ruling, those damages could have been upwards of ***$285 billion*** or more depending on the amount of scans.[2] These enormous sums certainly beg the question of whether BIPA's liquidated damages are excessive, unconstitutional awards, especially when viewed in light of any actual damage sustained.

The *Cothron* decision also might cause more BIPA lawsuits brought by individuals, as opposed to putative class action suits, because the damages an individual can recover can total in the millions of dollars. Indeed, before *Cothron*, employees who worked five days a week and scanned their fingerprints to clock in and out of work each day, including when taking lunch breaks, were entitled to statutory damages valued at $1,000 per day (or $5,000 in cases of willful violations). Now, individual plaintiffs can seek damages for *each scan* and related damages awards as high as $4,000 per day – or $20,000 for one week's worth of violations in cases of non-willful violations. As the dissent in *Cothron* notes, the Court's ruling treating each scan as a separate, actionable violation arguably incentivizes plaintiffs to delay bringing suit as long as possible for purposes of "racking up" damages.

Cothron is now at least the third Illinois Supreme Court opinion that seemingly justifies exorbitant damage awards as a way to encourage private businesses to comply with BIPA.[3] Thus, although businesses are "incentivized" to comply with BIPA, the threat of massive claims and damages leaves them with little room to maneuver should they face allegations of noncompliance. This is an

unenviable and seemingly untenable position that could lead to a new pattern where businesses – facing damages that would lead to bankruptcy – opt to aggressively defend and litigate BIPA disputes, rather than attempt to negotiate an early settlement. Such a dynamic would not only add to Illinois's already heavy BIPA case docket but also result in increased litigation costs for all parties.

The *Cothron* decision will likely renew constitutional challenges to BIPA damages on the grounds that such exorbitant damages (1) are not rationally related to Illinois's interest in protecting biometric information and (2) violate the Due Process Clause of the Fourteenth Amendment because they are grossly excessive or imposed without adequate procedural protections.

In the interim, businesses must cope with the prospect of facing crippling liability. To avoid a potential chilling effect on economic activity in the state, one possible avenue of relief is to pass a "safe-harbor" amendment to allow businesses a grace period to come into compliance with BIPA and/or relax the consent requirements of the statute. New York City's Biometric Law[4] serves as a model for this, as businesses have 30 days to provide a written response stating that any violation has been remedied. Absent a similar amendment to BIPA, businesses may effectively be forced to stop collecting and using biometric information altogether.[5]

---

1 *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186.

2 *Rogers v. BNSF Ry. Co.*, 2022 U.S. Dist. LEXIS 45578.

3 *Supra* note 3.

4 NYC Admin. Code §§ 22-1201–1205, effective July 2021.

5 Certain organizations may be particularly vulnerable to BIPA lawsuits. On January 18, 2023, the Illinois General Assembly filed a new bill (HB 1230), which if passed, will amend BIPA to exempt health care employers. Given that Illinois law requires health care organizations to perform fingerprint-based background checks on their employees, this exemption could shield them from BIPA lawsuits.

National Law Review, Volume XIII, Number 59