Updates
February 23, 2023

Every Scan You Make: The Illinois Supreme Court Rules BIPA Claims Accrue With Each Biometric Data Collection or Disclosure

The Illinois Supreme Court recently opened the floodgates for class actions under the Illinois Biometric Information Privacy Act (BIPA) and created potentially catastrophic exposure for Illinois businesses. In a close 4-3 ruling, the landmark decision in *Latrina Cothron v. White Castle System Inc.* holds that every individual scan or transmission of biometric data made without the proper disclosures amounts to a separate violation of BIPA. This Update explains the ruling and its substantial, wide-ranging implications for companies that do business in Illinois or handle biometric data of Illinois residents, including how this decision affects businesses from data privacy, employment law, and insurance perspectives.

The *White Castle* Decision

The *White Castle* case is a putative class action filed in 2018 by Latrina Cothron, a former employee of White Castle System, Inc. The suit alleges that White Castle violated sections 15(b) and 15(d) of BIPA by using a system that required its employees to scan their fingerprints to access their pay stubs and computers, which led to the collection and disclosure of employees' biometric data without their consent and without providing the disclosures required under BIPA. White Castle argued that the lawsuit was untimely under BIPA's statute of limitations because Ms. Cothron's claim "accrued" in 2008, when White Castle first obtained her biometric data. Ms. Cothron argued that her suit was timely because a new BIPA violation occurred each time she scanned her fingerprints and each time White Castle sent her biometric data to its third-party vendor.

After years of the case winding its way through the district court, the U.S. Court of Appeals for the Seventh Circuit ultimately certified the claim "accrual" question to the Illinois Supreme Court. The Illinois Supreme Court considered whether each individual employee scan or biometric data transmission was an individual, independent violation of BIPA, or whether every scan and transmission for a single employee amounted to one violation that "accrued" at the time of the first scan or transmission. This issue received substantial media and legal attention because the timing of the BIPA statute of limitations is a substantial question in light of the thousands of class actions filed to date. Additionally, BIPA's statutory damages are assessed on a "per violation" basis at $1,000 per negligent violation and $5,000 per reckless or intentional violation. However, whether a plaintiff is entitled to damages for each violation was not squarely before the court as it was not included in the certified question. The determination of how many "violations" occurred could have potentially devastating effects on Illinois businesses if a single employee or consumer could identify hundreds (or even thousands) of individual biometric data collection or transmission events.

In addition to focusing on the plain language of BIPA, White Castle argued that (1) construing the statute to allow for repeated violations tied to the continued conduct of one individual employee could potentially result in "astronomical" damage awards that would constitute "annihilative liability" not contemplated by the legislature; and (2) reading the statute to define each scan or transmission as its own violation raised substantial constitutional concerns. Indeed, White Castle and amici estimated that, in White Castle's own case, classwide damages could exceed $17 billion based on a class of 9,500 current and former White Castle employees. Significantly, in various pleadings throughout the litigation, including on appeal, even Cothron recognized that

such damages would be "absurd" and "bizarre."

Relying on the plain language of BIPA, a four-justice majority (over three dissents) rejected these arguments and held that "[a] party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection." Similarly, the court found that the plain language of section 15(d) supports the conclusion that a claim accrues upon *each transmission* of a person's biometric identifier or information without prior informed consent.

The court reasoned that, where statutory language is clear, it must be given effect, even though the consequences may be harsh, unjust, absurd, or unwise. The court observed that the Illinois legislature intended to subject private entities to substantial potential liability under the statute as written. As noted, the damages issue was not one of the questions certified by the Seventh Circuit to the Illinois Supreme Court. The court did, however, suggest that trial courts have discretion with respect to damages under BIPA, so trial courts may not be obligated to award the full statutory damages contemplated under its ruling. The court also strongly suggested that the Illinois General Assembly is the branch of government best positioned to address the public policy concerns raised by White Castle and amici.

Practical Implications for Illinois Businesses

The *White Castle* decision has major practical implications for Illinois employers as well as for businesses that collect or disclose biometric information from Illinois residents, and raises the already-high stakes presented by BIPA litigation. First, the potential for devastatingly large damages is almost certain because the *White Castle* decision now allows for $1,000 in damages (or $5,000 for intentional or reckless violations) *per scan*. While the *White Castle* decision acknowledged that BIPA damages are discretionary rather than mandatory, it remains to be seen whether this implicit instruction will be observed by trial courts to rein in astronomically large damage awards. (Note that the one case to proceed to judgment on the merits saw a $228 million jury award.) The court also suggested that the legislature should address the issue of potentially excessive damages awards, opening the door to possible legislative intervention during the current or future legislative sessions.

Second, the decision follows another Illinois Supreme Court decision, *Tims v. Black Horse Carriers, Inc.*, Case No. 127801, granting a five-year statute of limitations to all biometric privacy claims. When read in tandem, companies face even more exposure: Since claims accrue for each new scan, it will be increasingly difficult to raise a statute of limitations defense. As noted by the dissent, plaintiffs may actually be incentivized to sit on their claims before filing suit in order to maximize damage awards.

Third, and a potential bright spot for businesses in this opinion, the court clarified that "[t]he active verbs used in section 15(b)—collect, capture, purchase, receive, and obtain—all mean to gain control[.]" Companies could rely upon this clarification if they themselves do not gain control of the biometric information.

Additionally, this ruling will undoubtedly sound alarm bells for insurers underwriting Illinois businesses. In response to the wave of BIPA-related litigation in the past six-plus years, insurers have increasingly been adding biometric data-related exclusions to general liability (CGL/GL), professional liability (E&O/D&O), and cyber insurance policies—especially for companies doing business in Illinois. We anticipate that such exclusions will become uniform across the marketplace in much the same way that insurers have added "communicable disease" exclusions to their commercial policies in the aftermath of the COVID-19 pandemic. Indeed, we would not be surprised if insurers attempted to add biometric-related exclusions immediately (if these are not already present) without waiting for the insured's next annual policy renewal.

With respect to existing policies, extensive BIPA-related coverage litigation has already taken place, with much of it favoring policyholders. Most significantly, in 2021, the Illinois Supreme Court concluded that BIPA class actions trigger the "personal and advertising injury" coverage (Coverage B) in standard form general liability (CGL/GL) insurance policies. Additional Illinois federal court rulings since 2021 have also favored policyholders by finding that certain commonly raised CGL/GL policy exclusions do not bar coverage for BIPA lawsuits.

Takeaways

The *White Castle* decision is likely to substantially raise exposure levels in BIPA-related cases. For companies doing business in Illinois that may have exposure under BIPA, we recommend immediately doing the following:

- Closely evaluate the continued collection, use, or disclosure of even potential biometric data. For some employers, the administrative burden and risk of compliance with BIPA may outweigh any benefits.
- For those employers or businesses who wish to continue to collect biometric data, work closely with counsel to review and update their biometric practices, policies, and procedures, as well as general data collection policies, to ensure that they are fully compliant with BIPA.
- Have existing policies audited by an insurance professional or coverage counsel to confirm the extent of available BIPA-related coverage.
- Prepare for insurers to deny coverage for any BIPA-related lawsuit even if it is likely covered under existing policy language and Illinois law as the size of the potential exposure will incentivize carriers to force their policyholders to expend time and resources fighting for coverage.

Authors

Debra R. Bernard

Of Counsel
DBernard@perkinscoie.com 312.324.8559

Calvin Cohen

Counsel
CCohen@perkinscoie.com 312.263.3018

Sara W. Davey

Counsel
SDavey@perkinscoie.com 312.324.8520

Bradley Dlatt

Counsel
BDlatt@perkinscoie.com 312.324.8499

Mylan Traylor

Associate
MTraylor@perkinscoie.com 312.263.3069

Explore more in

Labor & Employment Privacy & Security Class Action Defense Insurance Recovery Law Digital Media & Entertainment, Gaming & Sports

Related insights

Update

FERC Meeting Agenda Summaries for October 2024

Update

New White House Requirements for Government Procurement of AI Technologies: Key Considerations for Contractors