Articles + Publications | September 18, 2023

Illinois Court Eliminates Another BIPA Defense

WRITTEN BY

Molly S. DiRago | Ketan D. Bhirud | John Sample

This summer, the U.S. District Court for the Southern District of Illinois further bolstered Illinois' Biometric Information Privacy Act's (BIPA) nearly unfettered private right of action in *Lewis v. Maverick Transportation*. In a simple but firm four-page ruling, Judge Rosenstengel denied the defendant's motion to dismiss, holding that a cause of action under BIPA does not require a plaintiff to plead that data collected is used for identification purposes. The ruling serves to highlight the apparent lack of any real technical defenses to the statute — making it imperative that companies focus on strict compliance before they find themselves in court.

Background

BIPA is a privacy statute that prohibits, among other things, the collection and dissemination of biometric data without consent. To effectuate this goal, BIPA regulates the collection, use, safeguarding, and storage of biometric information and biometric identifiers such as fingerprints, retina scans, or face scans — also known as "biometric information." Under BIPA, private entities in possession of biometric information are required to: (1) develop a written policy governing management of the biometric information; (2) inform the owner of the biometric information; and (3) obtain consent from the employee to gather the biometric information.

Due to the uniquely plaintiff-friendly contours of the statute, courts have seen a panoply of putative class actions, leaving countless companies scrambling to develop workable defenses. This summer, the Southern District of Illinois eliminated one of those efforts.

Lewis v. Maverick Transportation

In its motion to dismiss, the defendant, *Lytx*, which provides video and analytic services — such as its DriveCam — to the transportation industry, argued that the plaintiff failed to adequately plead a BIPA claim because he did not allege that the captured information was used for identification purposes. In asserting this argument, the defendant relied on the BIPA statute's text, which defines biometric information as "any information…used to identify an individual." Because BIPA exclusively regulates biometric identifiers and biometric information, the defendant presumed that failing to allege that such information had actually been used to identify the plaintiff represented a fatal flaw in the pleading. In short, the defendant argued that BIPA requires plaintiffs to plead that the collected information is used to identify them.

The Southern District disagreed. Relying on dicta from the District of New Jersey and the Seventh Circuit, the court determined that, contrary to the defendant's arguments, "BIPA does not require a plaintiff to plead that the collected information is used to identify them." In so doing, the court reasoned that the purpose of BIPA is not to ensure *how* an individual's information is used (*i.e.*, to identify them) but rather "to ensure that consumers

understand, before providing their biometric data, how that information will be used, who will have access to it, and for how long it will be retained."

Significant Trend

This ruling signals a stark and significant trend for BIPA litigation — particularly in light of two BIPA decisions issued in the spring of 2023. On February 2, the Illinois Supreme Court held that a five-year statute of limitations period applied to all sections of BIPA, partially reversing a previous ruling by the Illinois Appellate Court, which held that a one-year statute of limitations applied in certain instances.[1] Then, on February 17, the Illinois Supreme Court held that a claim is triggered upon each biometric scan rather than just the first — vastly compounding the potential damages available to plaintiffs.[2] Based on this recent spate of rulings, it is evident that neither the courts nor the legislature intend to make life easier for defendants in the near future. Instead, defendants are seeing their exposure increase and their arguments deemed ineffective.

Takeaway

Private entities collecting biometric information must be more vigilant than ever in their efforts to comply with BIPA. Indeed, the exposure that BIPA presents is too significant to risk litigation, particularly when that risk relies on textual interpretation of the statute. Time and again, the courts have made clear that there will be no respite for defendants on the horizon. Given the apparent lack of any technical defenses to the statute, private entities must institute policies and practices that satisfy the statute's strictures and should engage counsel to ensure full compliance before litigation becomes inevitable.

---

[1] *Tims v. Black Horse Carriers, Inc.*, 2023 IL 127801.

[2] *Cothron v. White Castle Sys*., 2023 IL 128004.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber
- Regulatory Investigations, Strategy + Enforcement