Illinois Supreme Court Confirms a 5-Year Statute of Limitations Applies to All BIPA Claims

Labor & Employment Law Update

By Molly Arranz and Michael Chang on February 2, 2023

The BIPA hits keep coming for employers and companies in Illinois. Today, in a long-awaited opinion in *Tims v. Black Horse Carriers, Inc.*, the Illinois Supreme Court found that a five-year statute of limitations applies to all BIPA claims. This is not welcomed news for employers as it broadens the potential exposure under this biometric law that comes with the heaviest penalties for failure to comply—even if no injury is suffered.

The Court reversed the First District Appellate Court's finding that a one-year statute of limitations applied to certain BIPA violations—specifically those brought under the subsections of the statute concerning profiting from biometrics and their unauthorized disclosure. The Appellate Court had found there was a shorter time for these types of BIPA claims, reasoning that such claims involved "publication" of biometrics, such that Illinois' one-year statute of limitations should apply.

Notably, the Appellate Court had already found a five-year statute of limitations applied to BIPA claims for failure to maintain and comply with a publicly available retention policy, failure to provide written notice and receive written consent, and the standard of care for biometric storage. Prior to today's decision, therefore, there were two potential sets of limitations periods, even within the same complaint.

In *Tims*, the Illinois Supreme Court criticized this structure as it "could confuse future litigations about when claims are time-barred … [as] the same facts could support causes of action under more than one subsection[.]" While the Court acknowledged that the Appellate Court was not wrong under the plain language of the statute, when considering the intent of the legislature, and the goals of the statute, the Court concluded "it would be best to apply the five-year catchall limitations period."

At this juncture, there is a still an outstanding BIPA opinion from the Supreme Court— *Cothron*, which will address when certain BIPA claims accrue. Coupled with the expansive limitations period the Illinois Supreme Court has announced

today, *Cothron* **could lead to an exponential increase in exposure and damages** should the Court determine that certain BIPA claims accrue upon each and every scan. Today's opinion does not bode well for those hopeful of a decision favorable to employers.

BIPA makes it illegal for a company to capture, collect, or store the biometric information of anyone, including employees, unless written consent is received from the individual. A written policy describing the capture, collection, and storage must also be in place. The mere failure to inform employees, in writing, of the specific purpose and length of time for which their fingerprints are being collected, stored, and used, and to obtain their informed written consent—without more—can translate to astronomical exposure and potential damages. Identity theft or "unauthorized access" of this sensitive personal information is, in no way, required or needed.

This ruling serves as just another (harsh) reminder that any company that collects data that could reasonably be construed as "biometric" needs to review and audit their data privacy consent protocols and their data privacy disclosures and policies.

Specifically:

1. **Determine what biometric information you are collecting**. Under BIPA, biometric data is sensitive information that is biologically unique—such as iris scans, fingerprints, voiceprints and face geometry. Some of these identifiers can be captured simply through voice or video recording, so think through what information your company may be collecting to determine any necessary disclosures.
2. **Evaluate what disclosures you currently have in place**. To comply with BIPA, companies must provide written notice regarding what biometric information will be collected, stored, or used, as well as an explanation of the purpose of its collection. Additionally, prior to collection obtain express written authorization from consumers to collect and store their biometric information.
3. **Develop a publicly available written policy**. Along with obtaining express consent, it is important to incorporate a public policy establishing a retention schedule and guidelines for destroying biometric information.
4. **Audit your privacy policies and other written disclosures**. Best business practices require a careful look into retention and cataloging of any biometric data or other sensitive personal information—both in-house and by third-party providers.