The Computer & Internet Lawyer

Volume 40 ▲ Number 6 ▲ June 2023

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Illinois Supreme Court Gives the Green Light for Damages Fines Under the Illinois Biometric Information Privacy Act

By Jami Vibbert, Daniel E. Raymond, Brian J. Lohan, D. Tyler Nurnberg, Maja Zerjal Fink and Steven Wickman

A recent *New York Times* podcast[1] titled "The 'Enemies List' at Madison Square Garden" (the Podcast) brought to light the use of facial recognition technology at Madison Square Garden (MSG) not only for legitimate security purposes, but also as a means of creating and enforcing bans of lawyers suing MSG (by obtaining pictures of the attorneys from their law firm's website). The Podcast noted that Illinois and Texas have statutes governing the nonconsensual collection of biometric information. In the context of the Podcast discussion, one could conclude that such statutes are beneficial.

However, as discussed below, the Illinois statute – as has been interpreted by the Illinois Supreme Court – could be financially devastating for companies collecting biometric information in a much more benign manner.

The authors, attorneys with Arnold & Porter Kaye Scholer LLP, may be contacted at jami.vibbert@arnoldporter.com, daniel.raymond@arnoldporter.com, brian.lohan@arnoldporter.com, tyler.nurnberg@arnoldporter.com, maja.zerjalfink@arnoldporter.com and steven.wickman@arnoldporter.com, respectively.

THE DECISION

In a 4-3 decision, the Illinois Supreme Court in *Cothron v. White Castle System, Inc.*,[2] answered the following certified question from the Seventh Circuit:

> Do Section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?

A divided court held that a separate claim accrues under the Biometric Information Privacy Act (BIPA or the Act)[3] each time a private entity scans or transmits an individual's biometric identifier or information in violation of Section 15(b) or 15(d).[4] As a result, White Castle System, Inc. (White Castle) could be held liable under the Act for each time a White Castle employee used

their fingerprint to access their paystubs and computers since 2008, subjecting White Castle to damages in excess of $17 billion. The decision also vastly increases the litigation exposure of businesses that collect biometric data in Illinois.

The case stems from a proposed class action filed by plaintiff, Latrina Cothron, on behalf of all Illinois employees of defendant, White Castle. Cothron alleges that her employer, White Castle, violated Sections 15(b) and (d) of BIPA by requiring employees to scan their fingerprints to access their paystubs and computers and disclosing their fingerprint scans to a third-party vendor who verified each scan and authorized the employee's access.[5] Cothron alleges that White Castle implemented this biometric-collection system without obtaining her consent in violation of the Act,[6] which became effective in 2008.[7] Notably, Cothron alleges that the fingerprint scanning system was introduced in 2004 – four years before BIPA was enacted.

The case was originally filed in Illinois state court and removed to the Northern District of Illinois. White Castle moved to dismiss the case, arguing that Cothron's claims were untimely because the statute of limitations had run since her claims accrued in 2008, which was the first time she scanned her fingerprint after BIPA was enacted. The district court concluded that the lawsuit was timely because every unauthorized fingerprint scan was a separate violation of the statute and a new claim accrued with each unauthorized scan.[8] The Seventh Circuit referred the case to the Illinois Supreme Court to answer the certified question mentioned above.

THE NARROW MAJORITY FINDS EVERY COLLECTION AND DISCLOSURE IS A VIOLATION OF BIPA

Despite noting that the decision is unfavorable to businesses in Illinois, the court agreed with the district court that every collection and disclosure of biometric data between the same two parties constitutes a new BIPA violation.

The court, interpreting the "plain language of the statute" found that it supports Cothron's interpretation that claims under Section 15(b) and 15(d) accrue every time a private entity collects or disseminates biometric data without prior informed consent. White Castle argued that, under Illinois law, a claim accrues when a legal right is first invaded and an injury inflicted. The court, interpreting its earlier decision in *Rosenbach v. Six Flags Entertainment Corp.*, was unconvinced. Instead, the court interpreted *Rosenbach* as "clearly recogniz[ing] the statutory violation itself is the 'injury' for purposes of a claim" under BIPA. The court could not have been clearer: a simple statutory violation alone is a sufficient injury without anything more.

The majority recognized the extreme and absurd damages that could result from its interpretation. For instance, White Castle estimated that if Cothron can bring claims on behalf of as many as 9,500 current and former White Castle employees, where employees potentially scan their fingerprints multiple times per shift, the damages in her action may exceed $17 billion. But, the court offered a hollow limiting factor: that "[a] trial court presiding over a class action – a creature of equity – would certainly possess the discretion to fashion a damage award that (1) fairly compensated claiming class members and (2) included an amount designed to deter future violations, without destroying defendant's business." The court also noted that the Illinois General Assembly chose to make damages discretionary rather than mandatory under the Act.[9]

Indeed, the court made it clear that there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business. Finding it was not the court's place to rewrite the statute, the court demurred to the legislature, requesting that it was the proper place to review these policy concerns and make clear its intent regarding the assessment of damages under BIPA.

THE DISSENT'S SOUND REASONING

Joined by Chief Justice Theis and Justice Holder White, Justice Overstreet penned a vehement and sound dissent. The dissent argued that the majority's interpretation cannot be reconciled with the plain language of the statute, the purposes behind the Act, or the court's case law, and it will lead to consequences that the legislature could not have intended. Moreover, the dissent argued that the majority's interpretation renders compliance with BIPA especially burdensome for employers. The dissent argued that the court should have answered the certified question by saying that a claim accrues under Section 15(b) or 15(d) of the Act[10] only upon the first scan or transmission.

The dissent agreed with White Castle's argument on appeal – namely, that plaintiff's injury under Section 15(b) or (d) occurred, if at all, the first time that her biometrics were collected without her consent and/or disclosed, not each subsequent time that her finger was rescanned. The dissent homed in on the notion that there was only one loss of plaintiff's privacy, and that this happened when the information was first obtained and/or disclosed in violation of BIPA.

The dissent pointed out that BIPA's legislative findings and intent showed that the legislature recognized the utility of biometric technology and wanted to

facilitate its safe use by private entities by regulating how it is used.[11] The dissent stated that "nothing in the Act indicated that the legislature intended to impose cumbersome requirements or punitive, crippling liability on corporations for multiple authentication scans of the same biometric identifier." The dissent claimed that the legislature's intent was to ensure the safe use of biometric information, not to discourage its use altogether.

CONCLUSION

This is the second major Illinois Supreme Court decision this month to go against defendants. Earlier this month, the court in *Tims v. Black Horse Carriers, Inc.,* held that BIPA claims were subject to a five-year statute of limitations.

These two more recent decisions, along with the court's 2019 decision in *Rosenbach*, create a nightmare for BIPA defendants. Read together, the three decisions provide that:

(1) A BIPA plaintiff need not plead any actual injury or harm aside from a purely procedural violation of BIPA;
(2) Each unauthorized scan is a violation of BIPA (entitling plaintiffs to at least statutory damages of $1,000 to $5,000 for each violation); and
(3) The statute of limitations extends to violations that occurred up to five years prior to when a suit is filed.

The Illinois Supreme Court's interpretation of BIPA is an important national issue. Many states, in the rush to "level-up" their privacy protections, look to BIPA.

As mentioned above, the Podcast references BIPA as a "good law" protecting against the nonconsensual taking of one's biometric data. However, the Podcast and many state legislatures fail to grasp that strict enforcement of laws like BIPA is likely to have a significant impact on Illinois businesses that are (1) using new technologies to simplify normal business practices, and (2) creating innovative solutions to solve or simplify normal business practices. Verifying that the individual viewing personal information on a paystub is authorized to view such information is a different scenario than denying entry to a stadium because of where a person works. Indeed, as the dissent in *Cothron* cautioned, the cost of protecting individuals' data privacy rights could far outweigh the benefits if the end result is the destruction of businesses that form the backbone of the American economy.

Notes

1. "The 'Enemies List' at Madison Square Garden," The Daily Podcast, The New York Times, Jan. 18, 2023, available at https://podcasts.apple.com/us/podcast/the-enemies-list-at-madison-square-garden/id1200361736?i=1000595192217.
2. Cothron v. White Castle System, Inc., Ill., No. 128004 (Feb. 17, 2023).
3. Enacted in 2008, BIPA was one of the first state laws to address the collection and disclosure of biometric data. The law:
   - Requires informed consent prior to collection and/or disclosure of biometric data;
   - Mandates a requisite standard of care for the handling of biometric data;
   - Prohibits profiting from a person's or customer's biometric data;
   - Establishes a private right of action for injured persons; and
   - Provides statutory damages of up to $1,000 for each negligent violation and up to $5,000 for each intentional or reckless violation.

   See 740 ILCS 14/1 et seq.
4. Section 15(b) provides that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without first providing notice to and receiving consent from the person. 740 ILCS 14/15(b). Section 15(d) provides that a private entity may not "disclose, redisclose, or otherwise disseminate" biometric data without consent. Id. § 15(d).
5. Cothron v. White Castle Sys. Inc., 20 F.4th 1156 (7th Cir. 2021).
6. 740 ILCS 14/1 et seq.
7. Pub. Act 95-994, § 1 (eff. Oct. 3, 2008).
8. Id.
9. See 740 ILCS 14/20 (West 2018) (detailing the amounts and types of damages that a "prevailing party *may* recover" (emphasis added)).
10. Id. § 15(b), (d).
11. See 740 ILCS 14/5(a) ("The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.").

Copyright © 2023 CCH Incorporated. All Rights Reserved.
Reprinted from *The Computer & Internet Lawyer*, June 2023, Volume 40,
Number 6, pages 3–5, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com