December 17, 2021

Claim Accrual under the Illinois Biometric Information Privacy Act: What Recent Rulings Could Mean for Your Company

Hannah Griffin

Novack and Macey LLP

The First District of the Illinois Appellate Court ruled on Wednesday that a cause of action accrues under the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*, *each time* a company collects or uses biometric information in a manner that allegedly violates the Act and not when the company *first obtains* the plaintiff's biometric information. *Watson v. Legacy Healthcare Financial Services*, LLC, 2021 IL App (1st) 210279, ¶ 46. The Seventh Circuit is poised to issue a highly-anticipated decision on the same issue in *Cothron v. White Castle, Inc.*, Case No. 20-3202. As explained below, it seems likely that the Seventh Circuit will certify the question of when claims accrue under BIPA to the Illinois Supreme Court.

The implications of the accrual question for corporate defendants cannot be understated. In addition to determining when the statute of limitations period starts running for claims brought under the Act, the accrual question will determine whether continuing violations of the Act constitute separate claims. And, because the Act imposes liquidated damages for *each violation* of the Act, the answer to the accrual question could exponentially increase a company's potential liability.

What Are Biometrics and How Do Companies Use Them?

By way of background, biometrics generally refer to the measurement and/or analysis of biological information or physical characteristics. Biometric technology can be used to identify individuals through DNA, fingerprints, facial features, retinal features, and even odor – to name just a few examples. It can also identify individuals through behavioral characteristics such as their voice, gait, and typing rhythm.

Why are companies interested in collecting and utilizing biometrics? Biometrics allow employers to efficiently manage their workforce and increase workplace safety and security. Proponents argue that the use of biometrics is a more efficient way for employers to manage employee time and attendance. Biometric technology also makes companies less vulnerable to cybersecurity attacks because things like fingerprints and facial markers cannot be easily lost, shared, or stolen – unlike a PIN or password. Similarly, biometrics provide a reliable way to restrict access to a facility or different areas within that facility.

Companies also use biometrics to authenticate the identity of customers, which allows companies to serve customers quickly and more efficiently. Supporters also contend that the use of biometric technology helps protect customers from fraud and increases security. One obvious example of customer-facing biometric technology is using your face or fingerprint to open your iPhone. Some airlines are currently experimenting with using facial recognition technology in lieu of a boarding pass to streamline the boarding process.

Requirements for Illinois Companies under the Biometric Information Privacy Act

Championed by the ACLU of Illinois and passed unanimously by the Illinois legislature in 2008, the Biometric Information Privacy Act was the first state law to regulate companies' collection and use of biometric information. A driving force behind the passage of the Act was the idea that, when it comes to biometric information, the proverbial toothpaste cannot be put back in the tube. Indeed, the Act sets forth the legislative intent to safeguard biometric information because "biometrics are unlike other unique identifiers [that] … when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse[.]" 740 ILCS § 14/5. A person cannot change their fingerprints or DNA, for example.

Accordingly, the Act imposes the following duties on "private entities" possessing biometric identifiers or information:

- Develop a written policy setting forth retention and destruction practices. §15(a).
- Obtain informed consent and a written release prior to collection. §15(b).
- Protect and retain collected information in a reasonably confidential and secure manner. §15(e).

The Act also prohibits private entities from:

- Selling or otherwise profiting off of collected information. §15(c).

- Disclosing or disseminating collected information except in certain limited circumstances, such as in response to a subpoena or warrant. §15(d).

A crucial feature of the Act, which distinguishes it from other state privacy laws, is that it creates a private right of action for those whose rights under the statute are violated. BIPA supporters celebrate that any Illinois citizen can protect their rights by directly suing a company, rather than being reliant on state prosecutors. Critics of BIPA argue that the private right of action for alleged BIPA violations has caused companies to spend enormous sums of money defending frivolous lawsuits, including class actions.

The Rise of Employee and Customer Class Actions

Between 2015 and 2020, there was a surge of customer-based and employee-based class actions filed in Illinois federal and state courts alleging BIPA violations. Companies quickly discovered that BIPA claims represent a huge liability: *for each violation*, BIPA plaintiffs can recover $1,000 in liquidated damages or their actual damages, whichever is greater, for negligent violations or $5,000 in liquidated damages or their actual damages, whichever is greater, for reckless violations. 740 ILCS § 14/20. Successful BIPA plaintiffs can also recover their attorneys' fees. *Id*.

Then, in 2019, the Illinois Supreme Court issued a ruling that made stating a BIPA claim even easier for plaintiffs and putative classes. In *Rosenbach v. Six Flags Entertainment Corporation*, the Court ruled that, under BIPA, a plaintiff need not show any actual injury or damages to succeed on a cause of action -- only that there was a violation of the plaintiff's rights under the Act. 2019 IL 123186, ¶ 36. With so few barriers to filing, the number of BIPA class actions has continued to soar. Indeed, there are hundreds of BIPA class actions currently pending in Illinois state and federal courts, with a noticeable uptick in filings after the *Rosenbach* decision.

Corporate defendants hoped that the one-year statute of limitations applying to privacy actions, 735 ILCS 5/13-201, would provide a strong defense to putative class claims, but the Illinois Appellate Court's recent decision in *Tims v. Blackhorse Carriers, Inc.*, 2021 IL App (1st) 200563 somewhat dashed those hopes. Answering a certified question regarding what statute of limitations applies to BIPA claims, the First District ruled that the one-year statute of limitations applies only to violations of sections 15(c) and 15(d) of BIPA -- the sections that contain a publication or dissemination element. The Court further ruled that the five-year statute of limitations contained in section 13-205 of the Code of Civil Procedure applies to violations of sections 15(a), (b), and (e).

The Crucial Implications of the Accrual Question for Corporate Defendants

In *Cothron*, the plaintiff and putative class representative alleged that she was required to scan her fingerprint each time she accessed her work computer and weekly paystubs in the course of her employment with White Castle, to which she did not consent, and that her fingerprint data was repeatedly disclosed to a third party, also without her consent. Judge Tharp of the United District Court for the Northern District of Illinois held that Cothron's BIPA claims accrued, and the statute of limitations period began to run, at the time of each scan of her fingerprint and each time White Castle disclosed her biometric information to a third party without consent. Defendant White Castle appealed the trial court's ruling to the Seventh Circuit, arguing that the injury happened the very first time that Cothron's biometric information was collected without her consent because the real injury is the loss of control over one's biometric information without consent.

The implications of the accrual question are far-reaching. If each instance of a fingerprint scan or dissemination of fingerprint data without the plaintiff's consent is a discrete injury, then only the instances arising outside of the applicable statute of limitations are time-barred. By contrast, if the injury occurred only the first time a plaintiff's fingerprint data is gathered without consent, then the entire claim would be time-barred if that initial instance occurred outside the applicable statute of limitations.

A panel comprised of Chief Judge Sykes and Circuit Judges Easterbrook and Brennan heard oral argument in the *Cothron* case on September 14, 2021. Comments from the panel, particularly Judge Easterbrook, suggested that the Court is leaning toward certifying the accrual question for the Illinois Supreme Court under Seventh Circuit Rule 52 in the interest of allowing Illinois to interpret its own statutes and because of pending Illinois cases on the issue, which would control the outcome of the case.

As of the date of argument, neither the Illinois Supreme Court nor the Illinois Appellate Court had issued a decision directly addressing when BIPA claims accrue. But, on December 15, 2021, the First District of the Illinois Appellate Court ruled in *Watson v. Legacy Healthcare Financial Services*, LLC, 2021 IL App (1st) 210279, that the plain language of the Act establishes that the plaintiff's claims accrued each time his employer made a non-compliant capture or use of his fingerprint or hand scan. This is the same holding made by the Northern District of Illinois in the *Cothron* case.

The First District's ruling in *Watson* is not binding on the Seventh Circuit. But it is persuasive – indeed, the First District's opinion contains an in-depth analysis of the text of the statute, as well as the legislative history of the Act. Accordingly, it is possible that the Seventh Circuit will rule on *Cothron*, relying on *Watson* as persuasive authority. Yet, it seems more likely that the Seventh Circuit will certify the question to the Illinois Supreme Court.

How is the Illinois Supreme Court on certification likely to answer the accrual question? It's unclear, but one possibility is that a court could split the baby similarly to the Illinois Appellate Court's approach in *Timms*. Applying the single-publication rule recognized by Illinois courts in defamation cases, a court could hold that for violations of section 15(c) and (d), the claim accrues at the moment of the first instance of publication or dissemination. By contrast, each violation of sections 15(a), (b) and (e) could be viewed as discrete wrongs which accrue at the time of each distinct violation. What is clear is that the answer to the question will have huge implications for plaintiffs and defendants alike.

Proposed Legislative Amendments May Become More Prominent

As counsel for White Castle argued before the Seventh Circuit, BIPA class actions have the potential to bankrupt Illinois companies depending on how courts interpret the statute. Accordingly, some companies are advocating amending the Act. Indeed, several legislative amendments have been proposed to BIPA in the Illinois legislature in 2021. At least one such proposal would seek to repeal BIPA altogether, but it is unlikely to pass and indeed never made it out of the Rules Committee.

But, other proposed amendments to BIPA suggest certain limitations, which may gain renewed support given the recent developments in the case law described above. For example, one proposed amendment would rewrite the Act to require that the plaintiff suffer actual harm apart from the mere violation of the statute. Another proposed amendment would remove the private right of action from the statute and vest sole authority for enforcing BIPA with the Attorney General.

LATEST POSTS

- Claim Accrual under the Illinois Biometric Information Privacy Act: What Recent Rulings Could Mean for Your Company
- Vaccine Mandates: Considerations for Illinois Employers in Manufacturing
- Lawyers Behaving Badly: Uncivil Discourse Is Both Unethical and Unwise
- How LLCs Can Prevent Deadlocks From Leading To Business Divorce
- Green Leases Unite Landlords and Tenants to Lower a Building's Carbon Footprint

See more »

WRITTEN BY:

Novack and Macey LLP

Contact + Follow

 Hannah Griffin + Follow

PUBLISHED IN:

Appeals + Follow

Biometric Information + Follow

Biometric Information Privacy Act + Follow

Class Action + Follow

Cyber Attacks + Follow

Cybersecurity + Follow

Data Collection + Follow

DNA + Follow

Facial Recognition Technology + Follow

Fingerprints + Follow

IL Supreme Court + Follow

Policies and Procedures + Follow