No. 20-3202

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

LATRINA COTHRON,
Individually and on behalf of all others similarly situated,
Plaintiff-Appellee,

v.

WHITE CASTLE SYSTEM, INC.,
Defendant-Appellant.

On appeal from the United States District Court
for the Northern District of Illinois
No. 19-cv-00382
The Honorable John J. Tharp

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PLAINTIFF-APPELLEE & IN SUPPORT OF CERTIFICATION TO THE ILLINOIS SUPREME COURT

ALAN BUTLER
Counsel of Record
MEGAN IORIO
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
butler@epic.org
Counsel for Amicus Curiae EPIC

June 4, 2021

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 20-3202

Short Caption: Cothron v. White Castle

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐ **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Electronic Privacy Information Center

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

N/A

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: _____ Date: June 4, 2021

Attorney's Printed Name: Alan Butler

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ☑ **No** ☐

Address: 1519 New Hampshire Ave. NW

Washington, DC 20036

Phone Number: (202) 483-1140 Fax Number: (202) 483-1248

E-Mail Address: butler@epic.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy issues.[1]

EPIC has previously participated as *amicus* in cases concerning the scope of redressable injuries under state and federal privacy laws, including the Illinois Biometric Information Privacy Act ("BIPA"). *See* Brief for EPIC as *Amicus Curiae* Supporting Petitioner/Plaintiff, *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197 (Ill. 2018) (arguing an individual is "aggrieved" and suffers a BIPA injury when protected information is collected without proper authorization); Brief for EPIC as *Amicus Curiae* Supporting Plaintiffs-Appellees, *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2018) (arguing unlawful collection of biometric information in violation of BIPA is an invasion of a legal right that confers Article III standing). EPIC routinely participates as *amicus* to explain how violations of privacy rights constitute redressable legal injuries. *See, e.g.*, Brief for EPIC et al. as *Amici Curiae* Supporting Respondents, *Spokeo v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339) (arguing that the violation of a consumer's privacy rights under

[1] The parties consent to the filing of this *amicus curiae* brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party. EPIC Appellate Advocacy Fellow Melodi Dincer contributed to this brief.

federal law constitutes an injury-in-fact sufficient to confer Article III standing); Brief for EPIC as *Amicus Curiae* Supporting Respondent, *TransUnion LLC v. Ramirez*, No. 20-297 (U.S. filed Mar. 8, 2021) (urging the Court to hold individuals have standing to sue under federal privacy statutes because violations of individual privacy rights are concrete injuries); Brief for EPIC as *Amicus Curiae* Supporting Plaintiff-Appellant, *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909 (7th Cir. 2017) (arguing that violations of the Cable Communications Policy Act confer standing); Letter Brief for EPIC as *Amicus Curiae*, *Eichenberger v. ESPN, Inc.*, 876 F.3d 979 (9th Cir. 2017) (arguing that violations of the Video Privacy Protection Act confer standing); Brief of *Amicus Curiae* for EPIC Supporting Appellants, *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) (arguing that violations of statutory or common law rights confer standing without requiring additional consequential harm); Brief for EPIC as *Amicus Curiae* Supporting Plaintiffs-Appellants/Cross-Appellees, *In re SuperValu, Inc. Customer Data Sec. Breach Litig.*, 870 F.3d 763 (8th Cir. 2017) (same).

SUMMARY OF THE ARGUMENT

The Illinois Biometric Information Privacy Act ("BIPA") created unique and powerful biometric privacy rights for millions of Illinois residents. These privacy rights are directly enforceable under BIPA's private right of action, which empowers "aggrieved" individuals to bring suits to ensure that companies are held accountable when the individuals' rights are violated. In *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Supreme Court established a simple rule to determine when an individual is "aggrieved": Whenever a regulated entity violates an individual's BIPA rights as defined by the terms of the statute, the individual is "aggrieved" and can vindicate their rights in court. 129 N.E.3d 1197 (Ill. 2019). The lower court in this case recognized and followed the *Rosenbach* rule, and this Court should do the same.

But White Castle now asks this Court to overrule the Illinois Supreme Court on a question of state law and adopt instead a "loss of control" standard. The standard proposed by White Castle has no basis in the statutory text or in the Illinois Supreme Court's analysis in *Rosenbach*. Instead, White Castle attempts to import arguments about Article III standing into the BIPA statutory injury analysis. The constitutional Article III "injury-in-fact" test has nothing to do with the statutory "aggrieved" standard under BIPA. Under *Rosenbach*, each collection or

disclosure of an employee's biometric data without consent is actionable under BIPA.

White Castle is also mistaken about the underlying purpose of BIPA. The law does not protect against a facile "loss of control" of biometric data that only occurs the first time a biometric is collected or disclosed. BIPA protects against the risk that an individual's biometric data will be compromised. The risk of compromise does not go away when a company fails to obtain consent the first time it collects or discloses biometric data. Requiring companies to adopt responsible data practices and to seek individuals' consent for those practices is integral to minimizing the risk of compromise no matter whether it is the first or hundredth time a biometric has been collected or disclosed.

White Castle's rule would also undermine BIPA's remedial purposes. A rule that makes it impossible to recover for repeated violations would remove the key incentive for companies who previously violated BIPA to come into compliance, adopt responsible biometric data practices, and seek informed consent. Such a rule would increase the risk that individuals' biometric data could be breached or misused. The rule would also unfairly absolve long-time offenders while imposing liability on companies that have a one-time lapse in compliance. Neither BIPA's text nor *Rosenbach* support such a radical evisceration of the statute's unique privacy protections.

If this Court doubts the district court's interpretation of BIPA's text or the application of the *Rosenbach* standard as it relates to claims accrual, the Court should certify the question to the Illinois Supreme Court. The issues in this case purely concern Illinois state law and their resolution will have wide-ranging effects on BIPA enforcement beyond this case. The Illinois Supreme Court is best positioned to construe an Illinois statute on first impression and to construct an accrual rule for BIPA in line with its holding in *Rosenbach*.

ARGUMENT

I. An individual is "aggrieved" and suffers legal injury under BIPA any time a regulated entity violates an individual's statutory rights.

BIPA codifies a robust right to privacy in biometric data. The law imposes certain duties on regulated entities to ensure that they collect, retain, disclose, and destroy biometric data responsibly. 740 ILCS 14/15. These requirements "define the contours of [the] statutory right" to biometric privacy. *Rosenbach*, 129 N.E.3d at 1206. The law also provides individuals a right of action when companies fail to comply with any of these requirements. Under BIPA, "[a]ny person aggrieved by a violation of this Act" can bring suit against a noncompliant company. 740 ILCS 14/20. This private right of action is the primary enforcement mechanism for BIPA's privacy-protecting requirements. *Rosenbach*, 129 N.E.3d at 1203.

In *Rosenbach v. Six Flags*, the Illinois Supreme Court established a simple rule for determining when an individual is "aggrieved" under BIPA: An individual

suffers a legal injury and can sue any time their BIPA rights are violated by a regulated entity. *Rosenbach*, 129 N.E.3d at 1206. Specifically, whenever a company fails to comply with BIPA's requirements, "that violation constitutes an invasion, impairment, or denial of [an individual's] statutory rights." *Id.* The person is "entitled to seek recovery" through BIPA's private right of action for each violation because "[t]he violation, in itself, is sufficient to support the individual's . . . statutory cause of action." *Id.* Claimants do not need to plead or prove any additional harm beyond a BIPA violation to vindicate their rights. *Id.*

White Castle disregards *Rosenbach*'s simple rule and instead asks this Court to look beyond BIPA's statutory text to the purpose underlying the statute. White Castle asks this Court to consider not whether the plain text of the statute has been violated but whether an individual has "lost control" of their biometric data. White Castle argues that an individual whose biometric data has been collected without consent cannot, as a matter of law, be "aggrieved" by subsequent violations of their biometric privacy rights because they "lost control" of their biometrics upon the first nonconsensual collection. That standard would fundamentally rewrite the law, and the Court should reject it.

In essence, what White Castle seeks to do is to replace the Illinois Supreme Court's simple standard for BIPA statutory injury under *Rosenbach* with a complicated analysis more akin to an Article III standing inquiry under *Spokeo,*

Inc. v. Robins, 136 S. Ct. 1540 (2016). Some courts, when applying the *Spokeo* analysis, have analyzed legislative intent to determine the scope of actionable rights under Article III. *Id.* at 1549; *see, e.g.*, *Salcedo v. Hanna*, 936 F.3d 1162, 1169 (11th Cir. 2019) (acknowledging that the statute was violated but an analysis of the statutory purposes was necessary to determine Article III injury); *Dutta v. State Farm Auto. Ins. Co.*, 895 F.3d 1166, 1174–75 (9th Cir. 2018) (relying on legislative intent to limit injury under the statute); *Casillas v. Madison Ave. Associates*, 926 F.3d 329, 335–36 (7th Cir. 2019) (same). White Castle presents a similar analysis here when it argues that the General Assembly's concern for control—and not the statutory text—should be considered the touchstone for evaluating BIPA injuries. But this Court has previously said that federal courts applying Article III standing requirements and state courts applying statutory injury standards "define 'injury in fact' differently." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 623 (7th Cir. 2020), *as amended on denial of reh'g and reh'g en banc* (June 30, 2020). And the Illinois Supreme Court was clear in *Rosenbach* that an individual is aggrieved and suffers a legal injury whenever a regulated company fails to comply with BIPA's requirements. *Rosenbach*, 129 N.E.3d at 1206.

White Castle's argument has no support in the statutory text. The term "control" does not appear a single time in the BIPA, including in the legislative

findings and intent section. 740 ILCS 14/5. Control thus has no bearing on whether an individual is "aggrieved" under BIPA. The requirements for consent also clearly anticipate that some entities would repeatedly collect the same type of biometric data and require that the time and purpose provisions of an individual's consent cover each collection. 740 ILCS 14/15 (the regulated entity must "inform the subject . . . of the specific purpose and length of term for which a biometric identifier or biometric information is *being collected*, stored, or used") (emphasis added). Accordingly, each allegation that White Castle collected its employees' biometric data without consent within the statute of limitations is actionable under *Rosenbach*.

The Court should also reject White Castle's argument that common law analogies should govern the scope of redressable injuries under BIPA. Some federal courts applying the Article III *Spokeo* test have reached back to analyze whether certain privacy rights track common law privacy torts in order to determine whether violations of those rights are sufficiently "concrete" to confer standing. 136 S. Ct. at 1549. These common law comparisons have caused significant confusion among courts about the enforceability of federal privacy laws, often leading to litigants "hammering square causes of action into round torts." *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020)

(en banc). There is no need for the Court to look to common law in this case, where the statutory standard under state law is already well established.

Establishing a BIPA injury is straightforward and does not require plaintiffs to fit square modern privacy harms into round common law torts. Common law privacy violations are simply not relevant or necessary to determine legal injury under BIPA because they do not involve statutory rights defined by the Illinois General Assembly to protect against harms unique to biometric data. Legal injury under BIPA is a question of statutory interpretation, not a vague question of legislative purpose or analogies to common law privacy harms. There is no need to reconstruct purposes or draw tortured analogies to privacy torts to establish a statutory injury, because the Illinois Supreme Court has declared an entirely different, straightforward benchmark—whether or not the individual's statutory right was violated. Any collection or disclosure made without consent is a violation of the statute that results in legal injury.

II. BIPA violations are not "one and done" and adopting such a rule would hamper BIPA's remedial purpose by allowing longtime offenders to avoid liability for past statutory violations.

This Court need not consider the purposes underlying BIPA to determine when claims accrue. But even if the legislative purposes were relevant, White Castle's proposed "loss of control" purpose is too facile. BIPA protects against the risk that biometric data will be compromised. Biometrics are compromised when

they are obtained by a third party or used for an unintended purpose. The risk that an individual's biometrics will be compromised does not disappear after the first time they are collected or disclosed without consent—as long as a regulated entity is collecting, storing, using, and disclosing biometric data without adopting the data practices required by BIPA's plain text and obtaining informed consent for those practices, there is an increased risk that the data will be obtained by a third party or used for other purposes.

White Castle's rule on accrual would in fact undermine BIPA's purposes. The rule allows longtime and systematic BIPA violators to avoid liability if their first offense occurred outside the statute of limitations. Under White Castle's atextual interpretation of legal injury, the only actionable BIPA claims would be against entities that recently began collecting biometric data or, perversely, those who have been compliant but who had a one-time lapse in compliance within the statute of limitations. White Castle's rule produces unfair results that flip BIPA's remedial purpose on its head, eviscerating any incentive to comply for those who have been noncompliant for long enough.

A. BIPA addresses the risks posed by the collection and use of biometric data by granting rights and imposing responsibilities to ensure the data is protected.

BIPA protects against the risk that biometric data will be compromised by requiring companies that collect biometrics to adopt responsible data policies, to

inform individuals of these policies, and to obtain individuals' consent before collecting or disclosing their biometric data. BIPA's rules minimize the risk that biometrics will be stolen or misused by incentivizing adoption of responsible data practices for collection, use, storage, and disclosure of biometric data. BIPA's rules also engender trust between individuals who consent to collection and disclosure of their biometrics and companies that collect their data by setting concrete expectations for the information's retention and use and demystifying an otherwise opaque practice.

The Illinois General Assembly specifically indicated in the statutory findings that they intended for BIPA to address the risks of compromise inherent in the collection of biometrics. The legislature recognized that "biometrics are unlike other unique identifiers" because they are "biologically unique" and "once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c). Because the risks posed by collection of biometrics made the public "weary" of participating in biometric-facilitated transactions, 740 ILCS 14/5(d), the legislature determined that it must "regulat[e] the collection, use, safeguarding, handling, storage, retention, and destruction" of biometric data. 740 ILCS 14/5(g).

Biometrics are not necessarily "compromised" when they are collected without BIPA's required consents; rather, the collecting of biometric information

(and the storage and disclosure of that data) increases the risk that a third party will obtain the identifier and use it to the individual's detriment. Anxiety over who might obtain biometric data from companies that individuals directly interact with was one of the motivations behind BIPA's enactment. BIPA was passed after a controversy spurred by the bankruptcy of a fingerprint scanning company, Pay By Touch. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276 (statement of Illinois state Rep. Kathy Ryg). In her floor statement on the bill, BIPA's sponsor specifically referenced the questions raised by the Pay By Touch bankruptcy, noting that residents were "wondering what will become of their biometric and financial data," *i.e.*, whether the data would be sold like the company's other assets, who would obtain it, and what they would do with it. *Id.*

Biometrics are also an attractive target of hackers, who might sell the data to identity thieves or use the data to steal identities themselves. In 2015, a data breach at the United States Office of Personnel Management ("OPM") resulted in the theft of 5.6 million digitized fingerprints. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018).[2] In 2019, Customs and Border Control ("CBP") also suffered a data breach of 184,000 images from CBP's facial recognition pilot program, some of which, CBP found, were posted to the dark web. Dep't of Homeland Sec., Off. of Inspector Gen., *Review of CBP's Major Cybersecurity Incident during a 2019*

[2] https://www.opm.gov/cybersecurity/cybersecurity-incidents.

Biometric Pilot (Sep. 21, 2020). Hackers have also targeted Aadhaar, the largest biometric database in the world. Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, Wash. Post (Jan.4, 2018).[3]

BIPA requires companies that collect biometric data to adopt responsible data practices that decrease the risk that the biometrics they collect will be compromised by data breach or misuse. BIPA's consent requirement for collection of biometrics requires companies to limit the types of biometric data they collect, the purposes they use the biometrics for, and the length of time they will collect, store, and use the data. 740 ILCS 14/15(b). BIPA's requirement to establish a retention schedule and plans for permanently destroying the identifiers after a certain period of time ensures that a company does not retain an individual's biometrics indefinitely. 740 ILCS 14/15(a). The requirement to obtain consent for disclosures and redisclosures is meant to limit and discourage transmission of biometrics to third parties. 740 ILCS 14/15(d). The statutory imperative to incentivize these behaviors does not diminish after a single nonconsensual collection or disclosure of biometric data. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 So. Cal. L. Rev. 241, 283–87 (2007) (describing how privacy laws

[3] https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft.

incentivize businesses to limit collection of sensitive information to limit the risk of breach).

The consent requirements also directly address the public's "weary" attitude toward biometrics by setting expectations for how long their biometrics will be collected, stored, and used, and to whom they will be disclosed. The consent requirements are a direct application of fundamental privacy law principles—dating back to the 1970s—that help to "eliminate misunderstanding, mistrust, frustration, and seeming unfairness." U.S. Dep't of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems XX-XXIII*, at 46 (1973). The need to engender trust between companies that collect biometric data and the individuals whose data they collect does not diminish after the first nonconsensual collection—if anything, it increases.

Because consent to the collection of biometric data must be limited in both time and purpose, consent to collection of biometric data is not a simple on/off switch; it is a continual process that ensures that regulated companies take the necessary steps to protect biometrics as they continue to collect, store, and use them. White Castle's arguments focus on the "burden" of compliance with the regulatory scheme, but that is the law operating precisely as the Illinois General Assembly intended. And "whatever expenses a business might incur to meet the

law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded." *Rosenbach*, 129 N.E.3d at 1207.

B. White Castle's rule would undermine BIPA's remedial purpose and would benefit longtime and repeat offenders.

A key part of the remedial structure of BIPA is that companies face increasing liability if they fail to come into compliance with the statute's biometric privacy requirements. *Rosenbach*, 129 N.E.3d at 1207. Potentially significant liability faced by noncompliant companies is a critical feature of the law and the primary force ensuring compliance. By complying with BIPA's requirements, companies can avoid this liability and protect biometric privacy by minimizing any risk that biometric data may be compromised.

White Castle ignores BIPA's text and *Rosenbach* to argue that an individual is only "aggrieved" the first time they "lose control" over their biometric data. Under this theory, a company that repeatedly violates BIPA's requirements over a number of years could only be sued for the first violation and couldn't be sued at all if the statute of limitations has run on that first violation. Not only does this rule lack support in the text or in caselaw, it would upend BIPA's core remedial role. Under White Castle's proposed standard, companies would be incentivized to hide early BIPA violations until after the statute of limitations has run, and then afterwards would have no incentive to comply with the law.

White Castle's rule would also lead to absurd results by reducing the liability of repeat offenders and punishing them the same as (or less than) companies that failed to comply a single time. In effect, a company that violated BIPA only once within the statute of limitations and immediately deleted the data would be just as liable as a company that repeatedly violated BIPA within the same time period. Even worse, under this theory, individuals whose biometric data was collected without the proper informed consent before BIPA was enacted could never be "aggrieved" by a BIPA violation since they had already "lost control" of their biometric data before BIPA gave them a legal right that could be vindicated. The worst offenders, companies who flagrantly collect, store, use, and disclose biometric data without consent, would also evade liability so long as their first offense occurred outside the statute of limitations. These companies would be disincentivized to comply with BIPA because the clock has already run on any claims they could have faced. Longtime offenders would thus have no reason to adopt responsible data management practices to protect biometric data—the very reality BIPA was designed to prevent.

Under White Castle's rule, BIPA would essentially become a trivial penalty statute that would mostly punish companies who only recently began collecting biometric data or, paradoxically, companies who had been in compliance with BIPA but had a one-time lapse in compliance because they recently changed their

data practices without seeking new consent. For example, if a company failed to seek additional consent when the original time period in their retention or deletion policies had lapsed, started using biometric data for purposes beyond those initially outlined in the consent form, or disclosed data to entities omitted from previous consent forms or policies, it would be on the hook to the same extent (or more) than longtime, flagrant offenders.

By limiting legal injury to only the initial "loss of control," White Castle's proposed rule would undercut BIPA's remedial purpose by imposing uneven penalties on the companies that tried to comply with the law and flagrantly noncompliant offenders. This absurd result suggests that BIPA claims would only be actionable if a company violated the law for the first time at just the right moment. By narrowing the window of viable BIPA claims so severely, White Castle would successfully evade liability in the instant case while ensuring that other companies, including those who historically and systematically violate the law, may do so as well. That cannot be what the Illinois General Assembly meant when it enacted BIPA.

III. This appeal concerns important questions of state law that should be resolved by certification of the question to the Illinois Supreme Court.

BIPA's statutory text and *Rosenbach* clearly support finding that an individual is aggrieved (legally injured) and may sue under BIPA whenever a regulated company violates the law's requirements. However, if this Court believes

there are unresolved issues of claim accrual under BIPA, those questions should be certified to the Illinois Supreme Court to ensure uniformity in the application of state law.

This Circuit may certify any question to a state supreme court if "the rules of the highest court of a state provide for certification to that court." 7th Cir. R. 52(a). The Illinois Supreme Court allows certification for questions of state law "determinative of the said cause" and unanswered by "controlling precedents." Ill. S. Ct. R. 20(a). When exercising discretion to certify a question under these rules, "the most important consideration is whether we find ourselves genuinely uncertain about a question of state law that is key to a correct disposition of the case." *In re Hernandez*, 918 F.3d 563 (7th Cir. 2019).

BIPA is an important state law that protects the privacy rights of millions of Illinois residents. BIPA's private right of action is an important method of enforcing BIPA's obligations, and cases are routinely filed by Illinois residents whose biometric data was allegedly collected and disclosed without consent. Some cases involve longtime and systematic BIPA violators, as is the case with White Castle's decade-long collection and disclosure of employees' fingerprints without consent. *See, e.g.*, *Miller v. Sw. Airlines Co.*, 926 F.3d 898 (7th Cir. 2019) (alleging unlawful fingerprint scanning beginning in 2006); *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019) (alleging unlawful facial scanning beginning in 2010);

Monroy v. Shutterfly, Inc., 2017 WL 4099846 (N.D. Ill. 2017) (alleging unlawful facial scanning since 2014).

The question of when BIPA claims alleging longtime and systematic violations accrue is a significant one that could shut the courthouse doors on millions of affected individuals. The question of claim accrual must be resolved based on BIPA's text and the application of state law accrual principles.

The Illinois Supreme Court is best positioned to construe any ambiguity in BIPA and resolve the accrual rule in a way consistent with *Rosenbach*. The question of whether longtime and systemic BIPA offenders may be held accountable, based on the statutory accrual rule, is clearly a question of state law that is "determinative" in this case and amenable to certification.

Certification would also be useful in this case because it would avoid creating conflicts between state and federal courts over the scope of enforcement authority under BIPA. Federal court interpretations of the Article III injury-in-fact standard are more limiting than the simple statutory injury standard adopted by the Illinois Supreme Court in *Rosenbach*. If a federal court were to limit BIPA's enforcement based on narrower concepts of injury inconsistent with *Rosenbach*, that would create a split that could lead to inconsistent results in state and federal BIPA cases. The goal of all courts should be to adopt predictable and uniform standards for litigants, lawmakers, and courts. The best way to do that in this case

would be to certify any ambiguous questions of state law to the Illinois Supreme Court.

CONCLUSION

Amicus respectfully requests that this Court affirm the decision below or, alternatively, certify the question in this appeal to the Illinois Supreme Court.

Respectfully submitted,

/s/ Alan Butler
Alan Butler
Counsel of Record
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Circuit Rule 29. This brief contains 4,433 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and Circuit Rule 32(b) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14-point Times New Roman style.

Dated: June 4, 2021

/s/ Alan Butler
Alan Butler
Counsel of Record
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on June 4, 2021, this brief was electronically filed with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit through the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Dated: June 4, 2021

/s/ Alan Butler
Alan Butler
Counsel of Record
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140