E-FILED
4/19/2022 3:19 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

No. 128004

IN THE
ILLINOIS SUPREME COURT

LATRINA COTHRON, Plaintiff-Appellee, v. WHITE CASTLE SYSTEM, INC., Defendant-Appellant.	Question of Law Certified by the United States Court of Appeals for the Seventh Circuit, Case No. 20-3202 Question of Law ACCEPTED on December 23, 2021 under Supreme Court Rule 20 On Appeal from the United States District Court for the Northern District of Illinois Under 28 U.S.C. § 1292(b), Case No. 19-cv-00382 Hon. John T. Tharp

Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC) in Support of Plaintiff-Appellee

Megan Iorio (*pro hac vice*)
Sara Geoghegan
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, D.C. 20036
(202) 483-1140
iorio@epic.org
geoghegan@epic.org
Counsel for *Amicus Curae*
April 8, 2022

POINTS AND AUTHORITIES

INTEREST OF THE AMICUS

EPIC is a public interest research center in Washington, D.C., that focuses on consumer and civil rights issues involving new technologies.[1] EPIC is particularly concerned about the proliferation of biometric technologies and advocates for strong biometric privacy rights. *See, e.g.*, *EPIC v. U.S. Postal Service*, No. 21-2156 (D.D.C. filed Aug. 12, 2021) (suing to stop the U.S. Postal Service's law enforcement arm from using face recognition and social media monitoring tools); Rachel Metz, *Activists Pushed the IRS to Drop Facial Recognition. They Won, but They're Not Done Yet*, CNN Business (Mar. 7, 2022) (detailing a successful coalition effort to pressure the IRS to stop using face recognition); EPIC *et al.*, Comments to the Office of Science and Technology Policy on Public and Private Sector Uses of Biometric Technologies (Jan. 15, 2022) (stressing the importance of robust, timely, and transparent impact assessments to mitigate privacy and human rights risks of biometric technologies). EPIC participated as *amicus* in this case before the Seventh Circuit and has filed amicus briefs in this Court and other courts concerning injury under the Illinois Biometric Information Privacy Act ("BIPA"). *See* Brief for EPIC as *Amicus Curiae* Supporting Plaintiff-Appellee & Supporting Certification to the Illinois Supreme Court, *Cothron v. White Castle System*, 20 F.4th 1156 (7th Cir. 2021); Brief for EPIC as *Amicus Curiae* Supporting Petitioner/Plaintiff, *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186; Brief for EPIC as *Amicus Curiae* Supporting Plaintiffs-Appellees, *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2018).

[1] EPIC law fellow Thomas McBrien and former EPIC law fellow Melodi Dincer contributed to this brief.

SUMMARY OF 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.*, this 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. 2019 IL 123186. It follows that an individual is aggrieved, and a claim accrues, each time a company violates an individual's BIPA rights.

But White Castle now asks this Court to overrule its recent holding and adopt instead a "loss of control" standard. The standard proposed by White Castle has no basis in the statutory text or in this 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 gives individuals the right to control their biometric data by giving them the right to know who is collecting or disclosing that data and allowing the individuals an opportunity to say, "No, you cannot collect or disclose my biometric data." That control interest does not go away the first time a company collects

or discloses an individual's biometric data without consent—in fact, it becomes more urgent that the company informs the individual that their biometric is being collected and disclosed and gives them the opportunity to say "no."

BIPA also 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. The rule could particularly harm the right to control one's faceprint or voiceprint because these biometrics can be collected more clandestinely than fingerprints, making it easier for companies to hide their initial collection and disclosure until the statute of limitations has lapsed. Neither BIPA's text nor *Rosenbach* support such a radical evisceration of the statute's unique privacy protections.

ARGUMENT

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

The Illinois Biometric Information Privacy Act ("BIPA") imposes clear responsibilities on any private entity that collects or possesses biometric identifiers. This includes strict limitations on collection and disclosure of that data. In particular, the law prohibits collection of biometric information absent (1) disclosure in writing notifying the data subject of the collection, (2) disclosure in writing detailing both the "specific purpose" and "length of term" for which the data will be "collected, stored, and used," and (3) obtaining a "written release" from the data subject. Biometric Information Privacy Act, 740 ILCS 14/15 ("BIPA").

BIPA codifies a robust right to privacy in biometric data. The duties that BIPA imposes on regulated entities to ensure that they collect, retain, disclose, and destroy biometric data responsibly "define the contours of [the] statutory right" to biometric privacy. *Rosenbach*, 2019 IL 123186, ¶ 36. 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*, 2019 IL 123186, ¶ 37.

In *Rosenbach v. Six Flags*, this 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*, 2019 IL 123186, ¶ 33. 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 this 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*, 578 U.S. 330 (2016). Some courts, when applying the *Spokeo* analysis, have analyzed legislative intent to determine the scope of actionable rights under Article III. *Id.* at 340; *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 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 this 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*, 2019 IL 123186, ¶ 33.

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. 578 U.S. at 330. 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 an analogy 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 this Court has already 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 repeated 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. The right to control one's biometric information

under BIPA requires, at minimum, that a person know who is collecting and disclosing their data and to have a meaningful opportunity to tell the company, "No, you cannot collect or disclose my biometric information." That right is invaded every single time a company collects or discloses a biometric without notice or consent. As long as a person has not received notice of or given consent to the collection or disclosure, the person has not been given the opportunity to control their biometric information. Yet, under White Castle's theory, if a company fails to give notice and seek consent the very first time they collect or disclose a biometric and survives the statute of limitations, they never have to notify the individual that they are collecting their biometric information or to allow the person to say "no." That would allow companies to continuously invade a person's right to control their biometric data in perpetuity without consequence.

BIPA also 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. Their rule would allow 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. This is especially true in contexts where biometrics can be collected and disclosed clandestinely for years, such as many cases involving facial or voice recognition.

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 and companies 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 for 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*

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

CBP's Major Cybersecurity Incident during a 2019 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 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,

[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.

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.

Finally, the biometric information collected on one scan is not necessarily the same as the information collected on subsequent scans, so each scan creates a new risk of compromise. Biometric matching works by first collecting a biometric identifier, called the template, which is enrolled in a database. Ted Dunstone & Neil Yager, *Biometric System and Data Analysis: Design, Evaluation, and Data Mining* (2009), at 28. Upon each scan, the program collects new biometric information and creates a new biometric identifier, which is then compared to the template in the database. *Id.* at 29. The new biometric identifier and the template do not have to be exact matches—they only have to be similar enough that the program deems them a match. *Id.* at 29, 30. The new biometric identifier can add additional information about a person's fingerprint, voiceprint, or faceprint that could make it easier to identify the individual in the future.

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*, 2019 IL 123186, ¶ 37.

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

A key part of BIPA's remedial structure is that companies face increasing liability if they fail to come into compliance with the statute's biometric privacy requirements. *Rosenbach*, 2019 IL 123186, ¶¶ 36–37. Potentially significant liability faced by noncompliant companies is a critical feature incentivizing compliance with the law. 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.

This would result in especially perverse outcomes where biometric collection can be hidden for long periods of time. Unlike fingerprint scans, which generally require

contact with a scanner, faceprints and voiceprints can be collected without the knowledge of the individual. Hidden cameras and voice recorders can capture peoples' faces and voices clandestinely. Faceprints and voiceprints can also be collected from photos and voice recordings scraped from the internet or stored in archives. If claims only accrue the first time an individual's biometric is collected, companies that hide their initial noncompliance until the statute of limitations has passed would be allowed to compile massive biometric databases without legal consequence.

Some companies have already attempted to quietly build massive biometric databases that can identify nearly anyone in the world. One of the most notorious examples involves the company Clearview AI, which quietly engaged in abusive faceprint collection for years before a *New York Times* story informed the public. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020).[4] Without any public scrutiny or consent, Clearview scraped billions of photos from social media sites, job sites, and other internet sources, knowingly violating websites' terms of service in the process. *Id.* It used these photos to generate faceprints for millions of people, which it then fed into a face-search engine that it sold to hundreds of law enforcement agencies and other companies. *Id.* In a recent financial presentation, Clearview stated its plan to have 100 billion facial photos so that "almost everyone in the world will be identifiable." Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement*, Wash. Post (Feb. 16,

[4] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

2022).[5] It also explained its intent to expand to new contexts such as monitoring gig workers, despite originally claiming on its "Principles" page that it would only market to law enforcement. *Id.* Under White Castle's proposed rule on claim accrual, if a company secretly builds and markets such a database and waits out the statute of limitations on the first collection, as Clearview nearly did, then it could continue to use the software without legal consequence forever.

Similar issues with transparency and consent plague the voiceprint industry. Companies boast how much easier it is to collect voiceprints compared to other biometrics, noting that "You don't need to go anywhere or touch anything to verify your biometric authentication." Dan Hansen, *Voiceprint: A Security Game-Changer for Banks and Credit Unions of All Sizes*, BizTech Magazine (Nov. 5, 2018).[6] Research shows that many 1-800 contact centers, for example, take voiceprints without consent. *See* Joseph Turow, *Hear That? It's Your Voice Being Taken for Profit.*, N.Y. Times (Sep. 12, 2021).[7] Millions of people are installing companies' microphones in their homes in the form of devices such as Amazon's Echo, Google's Home, and Apple's HomePod. *See* Statista, *Installed Base of Smart Speakers in the United States from 2018 to 2022* (Mar. 2022),[8] Already, some of these devices have collected and transmitted users' conversations without knowledge or consent. *See, e.g.*, Tim De Chant, *After 75,000 Echo Arbitration*

[5] https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.
[6] https://biztechmagazine.com/article/2018/11/voiceprint-security-game-changer-banks-and-credit-unions-all-sizes.
[7] https://www.nytimes.com/2021/09/12/opinion/voice-surveillance-alexa.html.
[8] https://www.statista.com/statistics/967402/united-states-smart-speakers-in-households/.

Demands, Amazon Now Lets You Sue It, ArsTechnica (June 1, 2021);[9] Saumya Kalia, *Apple's Siri Was 'Accidentally' Recording Conversations Without People's Consent*, Swaddle (Feb. 14, 2022).[10] Lawsuits now allege that the companies derived biometric voiceprints from these conversations. *See, e.g.*, *Wilcosky v. Amazon*, 517 F.Supp.3d 751 (N.D. Ill. 2021); Compl., *Reid v. Amazon*, No. 21-cv-06010 (N.D. Ill. filed Nov. 9, 2021); Compl., *Zaluda v. Apple*, No. 2019-ch-11771 (Ill. Cir. Ct., filed Oct. 10, 2019). And when an internet-connected home device creates a voiceprint for a houseguest, they may not even know that the device exists or is recording them the first time they visit another person's home. Even toymakers have sent children's voice recordings to companies that create and sell voiceprints. *See* EPIC et al., Complaint and Request for Investigation, Injunction, and Other Relief (Dec. 16, 2016).[11]

Ruling that BIPA claims only accrue on the first instance of abuse would shield the most opaque and abusive companies like Clearview AI from liability. It is too easy for companies to clandestinely collect faceprints and voiceprints from secret devices or archives photos, videos, or audio files. If not for the *New York Times*'s reporting, the plaintiffs in the Clearview litigation would have never known of the company's alleged BIPA abuses. As biometrics continue to invade daily life, there are no guarantees that consumers will learn of violations in the first instance.

[9] https://arstechnica.com/tech-policy/2021/06/after-75000-echo-arbitration-demands-amazon-now-lets-you-sue-it/.
[10] https://theswaddle.com/apples-siri-was-accidentally-recording-conversations-without-peoples-consent/.
[11] https://epic.org/wp-content/uploads/privacy/kidså/EPIC-IPR-FTC-Genesis-Complaint.pdf.

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, to inform individuals that their data is being collected and disclosed, and to give people the opportunity to say "no"—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 regularly comply with BIPA but had a one-time lapse 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.

White Castle's rule could also disincentivize best practices for data management, such as data minimization. A growing use of biometrics is verifying that a person is who they say they are to set up an account online. Companies such as ID.me have entered this space to provide identity verification for various online services. The company collects two biometric identifiers: one from a person's government-issued ID, and one from the person's face in a real-time selfie photo or video. *See, e.g.,* ID.me, *IRS–How Do I Verify for the IRS with Self-Service?* (2022).[12] If the two biometrics match, the company considers the identity to be verified, and account creation can continue. *Id*. After the company has successfully matched the two biometric identifiers, it could delete the biometrics until the person wants to verify their identity in another context. Doing so would greatly diminish the risk that the biometric identifier would be compromised. But a company that has collected biometric information without consent would have no incentive to delete that data because it has already violated the collection provision to the greatest extent it possibly can and would minimize the risk of further violation if it retains the biometric indefinitely.

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

[12] https://help.id.me/hc/en-us/articles/4402761436823-IRS-How-do-I-verify-for-the-IRS-with-self-service-.

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.

* * *

For the foregoing reasons, this Court should strictly interpret BIPA to define an "aggrieved party" as anyone whose biometric information is collected in violation of the statute. "Collection" is the threshold safeguard in a privacy law. If that provision is not enforced, the statute's subsequent provisions are of little consequence.

CONCLUSION

EPIC respectfully requests that this Court rule that BIPA 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.

April 8, 2022

Respectfully submitted,

/s/ Megan Iorio

Megan Iorio (*pro hac vice*)
Sara Geoghegan
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, D.C. 20036
(202) 483-1140
iorio@epic.org
geoghegan@epic.org
Counsel for Amicus Curiae

RULE 341(c) CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 19 pages.

Dated: April 8, 2022

/s/ Megan Iorio
Megan Iorio

CERTIFICATE OF FILING AND SERVICE

I hereby certify that on April 8, 2022, I electronically filed the foregoing "Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC)" with the Clerk of the Illinois Supreme by using the electronic filing system.

Dated: April 8, 2022

/s/ Megan Iorio
Megan Iorio