No. 128004

IN THE
SUPREME COURT OF ILLINOIS

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 THE ILLINOIS CHAMBER OF COMMERCE AND THE CHAMBER OF COMMERCE OF THE UNITED STATES AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT WHITE CASTLE SYSTEM, INC.

Michael A. Scodro
Jed W. Glickstein
MAYER BROWN LLP
71 S. Wacker Dr.
Chicago, Illinois 60606
(312) 782-0600
mscodro@mayerbrown.com
jglickstein@mayerbrown.com

Counsel for Amici Curiae

E-FILED
3/14/2022 11:23 AM
CYNTHIA A. GRANT
SUPREME COURT CLERK

TABLE OF CONTENTS

INTEREST OF THE *AMICI CURIAE*

The Illinois Chamber of Commerce (the "Illinois Chamber") is a non-profit organization composed of businesses and organizations of all types and sizes across the State of Illinois. The Illinois Chamber is the unifying voice of the varied Illinois business community and represents businesses in all components of Illinois' economy, including mining, manufacturing, construction, transportation, utilities, finance and banking, insurance, gambling, real estate, professional services, local chambers of commerce, and other trade groups and membership organizations. Members include many small to mid-sized businesses as well as large international companies headquartered in Illinois.

The Illinois Chamber works collaboratively with trade organizations on specific policy issues or in specific areas of activity. It is dedicated to strengthening Illinois' business climate and economy for job creators. Accordingly, the Illinois Chamber provides businesses with a voice as it works with state lawmakers to make business-related policy decisions. The Illinois Chamber also operates an Amicus Briefs Program to bring attention to specific cases and provide additional information for the Court to consider. Over the last few years, the Illinois Chamber has appeared before this Court in matters of significant importance to its members, including the appropriate role and compensation of relators in Illinois false claims actions, limitations on a municipality's authority to tax, and an employee's fiduciary duty of loyalty to his or her employer.

The Chamber of Commerce of the United States of America (the "Chamber") is the world's largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than 3 million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber files *amicus curiae* briefs in cases, like this one, that raise issues of concern to the nation's business community.

Amici's members have substantial experience with the Illinois Biometric Privacy Act ("BIPA" or the "Act"). Indeed, BIPA litigation has exploded in recent years, with one study finding more than 900 lawsuits brought in state and federal court through the first quarter of 2021. *See generally* U.S. Chamber of Commerce, Institute for Legal Reform, *A Bad Match: Illinois and the Biometric Information Privacy Act* (Oct. 2021).

Companies understand the importance of protecting employees' and consumers' biometric data. And BIPA does not need to be construed to impose crushing liability on businesses, which would also chill the development and application of useful technologies, to promote these important goals. *Amici* submit this brief to explain to the Court the broader implications of its ruling for the Illinois business community, and why it is important to interpret

BIPA's accrual rules in a manner consistent with the statute's text, overall structure, and purpose.

INTRODUCTION AND SUMMARY OF ARGUMENT

BIPA, in Sections 15(b) and 15(d), prohibits the collection or disclosure of an individual's biometric information without the individual's consent. 740 ILCS 14/15(b), (d). It also bars the sale of such information and requires companies to establish policies and use reasonable care when handling biometric data. 740 ILCS 14/15(a), (c), (e). The statute creates a private cause of action for "[a]ny person aggrieved by a violation of this Act" and authorizes recovery for "each violation" of "liquidated damages" of $1,000 for negligent violations and $5,000 for intentional or reckless violations or actual damages if greater. 740 ILCS 14/20.

This case presents an extremely important question regarding the meaning of the phrase "violation of this Act"—whether a new claim accrues each time a defendant allegedly collects or discloses the same biometric data[1] from the same individual without consent, or whether multiple collections of the same data or disclosures of the same data to the same party each constitute a single collection or disclosure "violation," respectively.[2]

Amici agree with Defendant-Appellant White Castle System, Inc. that the plain text of the statute and relevant case law demonstrate that collection

[1] BIPA applies to both "biometric identifiers" and "biometric information." *See* 740 ILCS 14/10. For simplicity, this brief refers to both categories as "biometric data."
[2] This case involves repeated disclosure of the same information to the same third-party vendor, not the serial disclosure of the information to different third parties.

and disclosure claims involving the same biometric data and the same recipient accrue only once, at the time of the allegedly unauthorized initial collection or disclosure of the particular individual's biometric data. That is when the individual suffers the alleged injury the Act is intended to prevent, and, in the words of this Court, the privacy interest protected by the statute "vanishes into thin air." *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 34. That accrual rule is consistent with BIPA's text and purpose and with the accrual rules governing other privacy-based causes of action in Illinois.

Amici file this brief to emphasize additional considerations supporting this conclusion. The accrual rule advocated by Plaintiff-Appellee Latrina Cothron—that each collection or disclosure of the same information constitutes a separate violation—should be rejected because it would lead to damages awards that are divorced from any reasonable estimate of harm and entirely disproportionate to BIPA's deterrent purposes.

The legislature did not provide that separate scans or disclosures of the same information to the same parties would constitute separate violations, as it has in other statutes. And that construction of BIPA would be entirely illogical given the parallel prohibition on selling biometric data—the legislature's focus in enacting the law—which does not permit such astronomical awards. The legislature also made its rejection of draconian monetary awards clear by providing for a recovery of "liquidated damages"

rather than a statutory penalty. Moreover, construing the statute to permit such awards would raise significant constitutional concerns.

Finally, while the legislature intended to place limits on the collection and use of biometric data, and to provide substantial liquidated damages for violation of the Act's provisions, permitting statutory damages that would wildly exceed any remotely reasonable estimate of harm, and would ruin rather than deter violators, would unbalance the entire statutory scheme. Ms. Cothron's accrual rule would place tremendous pressure on businesses of all sizes to settle meritless claims. It would also create unacceptable opportunities for gamesmanship by plaintiffs seeking to run up the value of their claims.

Finally, because of its draconian consequences, Ms. Cothron's accrual rule will inevitably dissuade many companies from deploying useful technologies; the risk will simply be too great that a company will find itself named in a lawsuit seeking exorbitant damages that threaten the business's continued existence. But these technologies provide important benefits—for example, safeguarding the confidentiality of employees' personal information (social security numbers, pay information, etc.), increasing traffic safety by identifying fatigued drivers, and protecting homes and schools by stopping intrusions by unauthorized individuals. Preventing realization of those benefits will harm consumers and employees as well as businesses. The legislature could not have intended that result, which further confirms that

collection and disclosure claims do not accrue repeatedly with each scan or disclosure of the same individual's biometric data.

ARGUMENT

Plaintiff Latrina Cothron alleges that, beginning in 2007, Defendant White Castle employed fingerprint-scanning technology to gather and disclose employee biometric data for administrative purposes (*e.g.*, clocking employees in and out of work shifts). SAC ¶¶ 29-31, 40-44.[3] In 2019, Ms. Cothron sued White Castle on behalf of a putative class of White Castle employees for allegedly violating BIPA's collection and disclosure requirements. *Id.* ¶¶ 80-98. She disclaimed actual damages and instead sought only liquidated damages for each alleged collection and disclosure violation. *Id.* ¶¶ 58, 89, 98. The initial collection of Ms. Cothron's biometric information occurred in 2007, which is outside the governing statute of limitations.[4]

To avoid dismissal of her action on limitations grounds, Ms. Cothron argued—and the district court held—that her claims were timely because "[e]ach time an employee scans her fingerprint to access the system" without

---

[3] "SAC" refers to the Second Amended Complaint, *Cothron v. White Castle System, Inc.*, No. 19-cv-00382 (N.D. Ill.), Dkt. 44.

[4] It is not clear whether BIPA claims are subject to a one-year statute of limitations under 735 ILCS 5/13-201, a five-year statute of limitations under 735 ILCS 5/13-205, some other limitations period, or some combination thereof. This Court will address that question in *Tims v. Black Horse Carriers, Inc.*, No. 127801, but the district court here took no position on it. Nor does this case require the Court to decide whether a "discovery rule" delays the accrual of a BIPA claim until a plaintiff knew or reasonably should have known of her wrongful injury. *See, e.g.*, *Am. Fam. Mut. Ins. v. Krop*, 2018 IL 122556, ¶ 21 (a discovery rule may be applied "in certain circumstances to alleviate the harsh consequences of statutes of limitations"); *Meegan v. NFI Indus., Inc.*, 2020 WL 3000281, at *3 (N.D. Ill. June 4, 2020) (applying a discovery rule to a BIPA claim).

consent, and "each time [the employer] discloses or otherwise disseminates [the employee's] biometric information without consent," the employer "violates the statute." *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 732-33 (N.D. Ill. 2020). The court held that "each post-BIPA scan of her fingerprint constituted a separate violation of Section 15(b) and each disclosure to a third-party over that same period a separate violation of Section 15(d)," and therefore that "at least a portion" of her claims were timely. *Id*. at 729.

The district court's accrual rule would have wholly implausible consequences for BIPA's liquidated damages provision. If each scan or each disclosure is a "separate violation" of BIPA, then BIPA would authorize exorbitant monetary awards vastly larger than any conceivable estimate of damages or amount needed for effective deterrence.

Because the legislature could not have intended to authorize such exorbitant monetary awards, and the "per-scan" (or "per-disclosure") accrual rule is inconsistent with the statutory text and settled principles of statutory interpretation, the Court should reject that approach and hold that multiple collections of the same individual's biometric information or multiple disclosures of that information to the same person constitute a single collection or disclosure "violation," respectively, that accrues when the plaintiff can first bring suit—*i.e.*, at the first unauthorized collection or disclosure. *See Khan v. Deutsche Bank AG,* 2012 IL 112219, ¶ 20 ("A cause of action 'accrues' when facts exist that authorize the bringing of a cause of action.").

I. A "Per-Scan"/"Per-Disclosure" Accrual Rule Would Inevitably Produce Stratospheric Liquidated Damages Awards.

BIPA expressly authorizes plaintiffs to recover liquidated damages "for *each* violation" of the Act. 740 ILCS 14/20 (emphasis added). This allows for multiple claims if, for example, a defendant violates both Section 15(b) and Section 15(d) of the statute. But it does not allow for virtually unlimited claims for the same violation of the same provision—the straightforward consequence of Ms. Cothron's construction of the statute.

If an entity commits a "separate violation" each time it collects or discloses an individual's biometric data without consent, as the district court held (477 F. Supp. 3d at 730), then the statutory text necessarily permits plaintiffs to seek a minimum of $1,000 in damages, and up to $5,000, for each allegedly unauthorized scan or disclosure. That construction would produce liquidated damages awards that could easily reach into the millions of dollars *per person*—even if, as is almost always the case, a plaintiff has no actual injury from repeated collections or disclosures of the same biometric data.

Suppose an employee works 5 days a week for 48 weeks a year and clocks in and out of work via a fingerprint scanner once each day. Over just a single year, a "per-scan" accrual rule would imply 480 violations of Section 15(b), and a "per-disclosure" accrual rule would imply another 480 violations of Section 15(d). That would result in a statutory award of $960,000 to $4,800,000 in liquidated damages for one plaintiff in one year—*before* considering any awards for absent class members. Moreover, depending on the applicable

statute of limitations, *see supra* n.4, damages could extend for up to five years, producing a potential award of roughly $5 to $25 million for a single employee. If the employee similarly clocked in and out for lunch or other breaks, that amount could easily double or triple.

Many courts have recognized that, "taken to its logical conclusion," a per-scan or per-disclosure accrual rule "would lead [defendants] to potentially face ruinous liability." Mem. 5, *Robertson v. Hostmark Hosp. Grp.*, No. 18-CH-5194 (Ill. Cir. Ct. May 29, 2020); *see also* Mem. 3, *Smith v. Top Die Casting Co.*, No. 19-L-248 (Ill. Cir. Ct. Mar. 12, 2020) ("the interpretation plaintiff desires would likely force out of business—in droves—violators who without any nefarious intent installed new technology and began using it without complying with section (b)").[5] Even the district court here "fully acknowledge[d]" what it euphemistically called the "large damage awards that may result" from its holding. *Cothron*, 477 F. Supp. 3d at 733.

Similarly, before the U.S. Court of Appeals for the Seventh Circuit, Ms. Cothron argued that White Castle "violated Section 15(b) each and every time it collect[s] [a plaintiff's] biometric data without her informed consent" and that "each disclosure, redisclosure or other dissemination of a biometric identifier or biometric information constitutes an independent violation of Section 15(d)." Seventh Cir. Pl. Br. 16, 27.[6] Ms. Cothron seeks "statutory damages of $5,000

[5] These opinions are reproduced in the Appendix to White Castle's brief.
[6] "Seventh Cir. Pl. Br." refers to Ms. Cothron's brief in the Seventh Circuit, *Cothron v. White Castle Sys., Inc.*, No. 20-3202 (7th Cir.), Dkt. 40.

for *each* reckless and/or intentional violation of BIPA . . . or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA." SAC, Prayer for Relief. One of the inescapable consequences of her accrual rule, therefore, is that a defendant can be held liable for hundreds or thousands of "independent violations" with respect to a single individual's biometric information.

Likely recognizing the adverse consequences of that reality for her construction of the statute, Ms. Cothron told the Seventh Circuit that it should not "speculat[e], in the abstract, how Cothron's damages might play out under each party's competing interpretation." Seventh Cir. Pl. Br. 35. That is wrong as a matter of law and common sense.

One of the "fundamental principles of statutory construction is to view all provisions of an enactment as a whole." *Mich. Ave. Nat'l Bank v. Cnty. of Cook*, 191 Ill. 2d 493, 504 (2000). As this Court recently reiterated, "[w]hen construing statutory language, we view [a] statute in its entirety, construing words and phrases in light of other relevant statutory provisions and not in isolation," and considering "the reason for the law, the problems sought to be remedied, the purposes to be achieved, and the consequences of construing the statute one way or another." *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶ 18 (quoting *Eighner v. Tiernan*, 2021 IL 12601, ¶ 18 and citing *Hubble v. Bi-State Dev. Agency of the Ill.-Mo. Metro. Dist.*, 238 Ill. 2d 262, 268 (2010)). It is therefore not only appropriate, but necessary for this

Court to apply "deductive reasoning based on the language and purposes of the law and the consequences of a contrary construction." *Nelson v. Artley*, 40 N.E.3d 27, 35-36 (Ill. 2015).

The same flaw infected the Appellate Court's recent conclusion that BIPA "applies to each and every capture and use of plaintiff's fingerprint or hand scan." *Watson v. Legacy Healthcare Fin. Servs., LLC*, 2021 IL App (1st) 210279, ¶ 46. *Watson* expressly refused to "decide at this time whether each scan was a new and separate violation or a continuing violation" for purposes of damages. *Id.* ¶ 66. By bifurcating the inquiry, that court ignored this Court's instructions that a statute must be interpreted holistically and with regard for the consequences of a particular interpretation.

Moreover, speculation is not required to recognize the inevitable consequences of Ms. Cothron's construction: draconian liquidated damages liability. A great majority of BIPA cases involve claims that the defendant routinely collected (and often disclosed to a third party) the same information multiple times—whether in the employment context to verify employees' hours or regulate employee access each day, as here; or in consumers' use of technology that stores and categorizes photographs or similar data. *See, e.g.*, *Stauffer v. Innovative Heights Fairview Heights, LLC*, 480 F. Supp. 3d 888, 894 & n.1 (Aug. 19, 2020 S.D. Ill.); *Peatry v. Bimbo Bakeries USA, Inc.*, 2020 WL 919202, at *1-2 (N.D. Ill. Feb. 26, 2020) (same); *Tims v. Black Horse Carriers*, 2021 IL App (1st) 200563, ¶ 10 (same). The complaints in these cases typically

allege hundreds of putative class members who worked for the defendant or used their services during the class period.[7] Under Ms. Cothron's approach, case after case necessarily involves huge numbers of "violations," resulting in gigantic liquidated damages claims in the many millions of dollars, such as the claims asserted here.

For these reasons, this Court—in determining the proper construction of the statutory term "violation"—must take account of the dramatically different scale of liquidated damages awards that will result from the parties' differing interpretations of the statute.

II. A "Per-Scan" Accrual Rule Is Inconsistent With BIPA's Text And Longstanding Principles Of Statutory Interpretation.

Applying settled rules of statutory construction to BIPA's text compels the rejection of the district court's accrual rule and requires that the statute be interpreted to create a single claim for collection or disclosure of a given individual's biometric information, not multiple claims for each collection of the same information or disclosure of the same information to the same party.

A. BIPA's Text Indicates That Collection And Disclosure Claims Accrue Once When They Involve The Same Information.

Two elements of BIPA's text make clear that the legislature did not view repeated collections or disclosures of the same information as independent violations of the statute.

---

[7] *See, e.g.*, Second Amended Class Action Complaint ¶88, *Stauffer v. Innovative Heights Fairview Heights, LLC*, No. 20-cv-46 (S.D. Ill.), Dkt. 98 ("on information and belief the total number of members in the Class is, at a minimum, in the hundreds").

First, when the legislature wants continuing conduct to trigger repeated, separate statutory violations, it includes text expressly specifying that result. *See, e.g.*, 820 ILCS 325/5-20 ("Each day that a violation continues constitutes a separate violation."); 30 ILCS 570/7.15(a)(2) ("Each violation of this Act for each worker and for each day the violation continues constitutes a separate and distinct violation."); 815 ILCS 511/10(c) ("The injured person . . . may elect, in lieu of recovery of actual damages, to recover the lesser of $10 for each and every unsolicited electronic mail advertisement transmitted in violation of this Section, or $25,000 per day.").

The legislature included no such language in BIPA, confirming that it did not intend each additional scan or disclosure of the same biometric data to constitute a separate violation.

Second, under Ms. Cothron's logic, a defendant who intentionally sells biometric data to a third party would be liable for only $5,000 in liquidated damages, while a defendant who merely discloses the same data to a third party on an ongoing basis would have "violated" the statute hundreds or thousands of times over. There is no logical reason to penalize companies that simply collect and disclose the very same biometric data far more severely than companies that sell the data outright.

Indeed, legislative history demonstrates that the potential sale of biometric data collected by Pay by Touch was the "primary impetus" behind BIPA's passage. *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st)

180175, ¶¶ 63-64; *see also* 95 Ill. Gen. Assemb., House Proceedings, May 30, 2008, at 249 (statement of Rep. Ryg: "The California Bankruptcy Court recently approved the sale of their Pay By Touch database. So, we are in very serious need of protections for the citizens of Illinois when it comes to biometric information.").

The legislature was concerned that the purchaser of such data could use it in a manner not contemplated by consumers and could sell it to other entities. Given the legislature's focus on the risk posed by sales of data, it would be particularly bizarre if the sale of data was routinely subject to vastly smaller liquidated damages than collection or disclosure.

B. The Legislature's Use Of the Term "Liquidated Damages" Precludes Interpreting The Statute To Authorize Draconian Levels Of Damages.

Recognizing a separate violation based on each scan or disclosure of the same biometric data is also inconsistent with the legislature's creation of a right to recover "liquidated damages." 740 ILCS 14/20.

When the legislature uses a term that "has a settled legal meaning," courts "will normally infer that the legislature intended to incorporate the established meaning." *People v. Young*, 960 N.E.2d 559, 562 (Ill. 2011). Under Illinois law, liquidated damages have long been understood to refer to a *reasonable* estimate of harm—one that "bear[s] some relation to the damages that might occur." *Smart Oil, LLC v. DW Mazel, LLC*, 970 F.3d 856, 863 (7th Cir. 2020); *see also Grossinger Motorcorp, Inc. v. Am. Nat'l Bank & Tr. Co.*, 240 Ill. App. 3d 737 (1st Dist. 1992).

In *Rosenbach*, this Court stated that "when a private entity fails to adhere to the statutory procedures, . . . 'the right of the individual to maintain [his or] her biometric privacy vanishes into thin air.'" 2019 IL 123186, ¶ 34. But under Ms. Cothron's rule, new claims (and new damages) continue to accrue long after biometric privacy has vanished. Requiring a defendant to pay up to $5,000 each time it collects an individual's fingerprint is not a reasonable estimate of damages. It is a draconian penalty.

As described above, moreover, the total damages under such a theory can quickly reach absurd levels—producing potential liquidated damages for a single individual of $1 million or more. When a liquidated sum is "far in excess of the probable damage on breach, it is almost certainly a penalty." Damages, Black's Law Dictionary (11th ed. 2019); *cf. also Rosenbach*, 2019 IL 123186129, ¶ 32 (considering Black's Law Dictionary definition of "aggrieved" in interpreting BIPA). Because the legislature authorized awards of "liquidated damages" and not "penalties," the Court should interpret the statute in accordance with the meaning of that statutory term.[8]

[8] As the Seventh Circuit observed, some federal statutes—for example, the junk-fax ban in the Telephone Consumer Protection Act—provide for (much smaller) continuous damages. *Cothron v. White Castle System, Inc.*, 20 F.4th 1156, 1162 (7th Cir. 2021). But that potential analogy cannot help Ms. Cothron. This Court recently emphasized that "regulating telephone calls, faxes, and e-mails is fundamentally different from regulating the collection, use, storage, and retention of biometric identifiers and information." *W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978, ¶ 55. In addition, the Telephone Consumer Protection Act protects a privacy interest in seclusion—and therefore, unlike with BIPA, each successive unwanted fax or telephone call inflicts new harm. *Valley Forge Ins. Co. v. Swiderski Elecs., Inc.*, 223 Ill. 2d 352, 365-66 (2006).

In addition, it is well-settled that courts should "presume[] that the General Assembly did not intend absurdity, inconvenience, or injustice in enacting legislation." *People v. Casler*, 2020 IL 125117, ¶ 24; *see also Dynak v. Bd. of Educ. of Wood Dale Sch. Dist. 7*, 2020 IL 125062, ¶ 16 (same). A reading of BIPA that would produce hundreds or even thousands of independent violations based on the same course of conduct—permitting potential liquidated damages of $1 million or more for individual claims—is manifestly absurd.

To be sure, the legislature intended BIPA to impose "substantial consequences" for noncompliance with the statute's requirements. *McDonald*, 2022 IL 126511, ¶ 48. BIPA therefore permits a plaintiff to recover up to $5,000 for collection and $5,000 for disclosure without any showing of actual injury. *Rosenbach*, 2019 IL 123186, ¶¶ 35-37. Particularly because these claims are brought as class actions—often in industries with high staff turnover—the consequences for noncompliance under a "per-scan" accrual rule can be very substantial indeed. A small business with just 50-100 employees could easily face a claim of $50-$250 million or more.

None of this Court's cases, however, suggest that BIPA's already generous liquidated damages awards—and allowance for any greater actual damages proved by a plaintiff—can or should be bolstered by an accrual rule that multiplies the statutory damages figure hundreds or even thousands of times when a defendant collects or discloses the same information. To the

contrary, the decision to cap liquidated damages at $5,000 shows that the legislature did *not* wish to expose companies to effectively unlimited liability. *See Nelson*, 40 N.E.3d at 35 (rejecting a reading of a statute that would subject certain companies to "unlimited liability" because there was "no clear reason why the legislature would have wanted" to do so).

C. "Per-Scan" Accrual Would Raise Significant Constitutional Concerns.

This Court has long recognized that "an interpretation under which the statute would be considered constitutional is preferable to one that would leave its constitutionality in doubt." *Braun v. Ret. Bd. of Fireman's Annuity & Benefit Fund of Chi.*, 108 Ill. 2d 119, 127 (1985). Because interpreting BIPA to treat each scan or disclosure of the same biometric data as an independent violation would raise significant constitutional concerns, the Court should reject that approach.

It has long been established that "the Due Process Clause of the Fourteenth Amendment imposes substantive limits 'beyond which penalties may not go.'" *TXO Prod. Corp. v. Allied Res. Corp.*, 509 U.S. 443, 453-54 (1993); *see also State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 416-17 (2003) ("[t]he Due Process Clause of the Fourteenth Amendment prohibits the imposition of grossly excessive or arbitrary punishments on a tortfeasor"); *St. Louis, I.M. & S. Ry. v. Williams*, 251 U.S. 63, 66–67 (1919) (statutory damages may violate due process where "the penalty prescribed is so severe and oppressive as to be wholly disproportioned to the offense and obviously

unreasonable"). Awarding millions of dollars to individual plaintiffs that have suffered little or no actual damages (and thus seek only liquidated damages) is grossly disproportionate to any legitimate compensatory or deterrent purpose. *Cf. Int'l Union of Operating Eng'rs, Local 150 v. Lowe Excavating Co.*, 225 Ill.2d 456, 490 (2006) ($325,000 punitive damages award was grossly excessive where actual damages amounted to just $4,680); *Parker v. Time Warner Ent. Co.*, 331 F.3d 13, 22 (2d Cir. 2003) (acknowledging "legitimate concern that the potential for a devastatingly large damages award, out of all reasonable proportion to the actual harm suffered by members of the plaintiff class, may raise due process issues").

In *Watson*, the Appellate Court suggested that worries about excessive damages were premature because, under the Act, damages "are discretionary not mandatory." 2021 IL App (1st) 210279, ¶ 66 n.4. But as a practical matter, this does little to address the problem. BIPA provides no guardrails to structure the trial court's discretion and no guarantee that a defendant who rolls the dice will not face annihilative liability. And as explained below, the prospect of such liability will force companies to settle meritless claims before a court has a chance to exercise its discretion to limit damages.

In sum, BIPA's text and structure, its importation of liquidated damages principles, and the absurd and likely unconstitutional consequences of a "per-scan" reading, all demonstrate that BIPA claims accrue only once, with the initial collection or disclosure of biometric data from or to a particular party.

III. A "Per-Scan" or "Per-Disclosure" Accrual Rule Would Create A Wholly Unbalanced Cause Of Action.

The accrual rule Ms. Cothron advocates is not only inconsistent with BIPA's text and purpose. It also would upset the careful balance the legislature struck in BIPA by, as one federal judge put it in a similar context, transforming "a shield for protecting consumer privacy into a sword for dismembering businesses." *Stillmock v. Weis Markets, Inc.*, 385 F. App'x 267, 275 n.* (4th Cir. 2010) (Wilkinson, J., concurring).

BIPA seeks to ensure that individuals have control over biometric data and confidence in biometric technology to *promote* the development and use of that technology in Illinois. As the statute itself recognizes, "[t]he use of biometrics is growing in [these] sectors" and "appears to promise streamlined financial transactions and security screenings." 740 ILCS 14/5(a). Because "many members of the public" were "deterred from partaking in biometric identifier-facilitated transactions," however, the legislature found that the public would "be served by regulating" this data under certain circumstances. 740 ILCS 14/5(e), (g).

Simply put, BIPA seeks to regulate biometric technology, not to make such technology radioactive. The accrual rule advocated by Ms. Cothron plainly seeks a "different balance" than the one the legislature chose in BIPA, *McDonald*, 2022 IL 126511, ¶ 49, and therefore should be rejected.

A. The District Court's Rule Will Inflict Significant Harm On Illinois Businesses And Encourage Unjustified Litigation.

In the few years since *Rosenbach*, hundreds of BIPA cases have been filed against Illinois businesses and employers. In 2019, over 360 BIPA cases were filed in Illinois federal and state courts; over 230 more were filed in 2020; and 66 were filed in just the first quarter of 2021—roughly 660 cases in little more than two years. U.S. Chamber of Commerce, Institute for Legal Reform, *A Bad Match: Illinois and the Biometric Information Privacy Act* 5 (Oct. 2021).

"While the technology giants have been sued for allegedly violating BIPA, so too have countless other companies . . . from locker rental companies to tanning salons." Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 Ill. B.J. 34, 35 (2018). Indeed, small businesses increasingly are targeted by BIPA suits. For example, a plaintiff filed a lawsuit against a family-run company in South Holland, Illinois with just 65 employees. *Kirby v. Gurtler Chems., Inc.*, Case No. 2019-CH-09395 (Ill. Cir. Ct., Cook Cnty. filed Aug. 14, 2019). Six days later, the same law firm brought a nearly identical complaint against a heating and air conditioning company. *Truss v. Four Seasons Heating & Air Conditioning, Inc.*, Case No. 2019-CH-09633 (Ill. Cir. Ct., Cook Cnty. filed Aug. 20, 2019). A search of the Courthouse News database shows hundreds of new BIPA cases filed

against grocery stores, electrical services firms, powder finishing companies, restaurants, and other small and medium sized companies.[9]

Plaintiffs have also targeted multiple companies for the same purported privacy harm. In one recent case, for example, the technology vendor (Kronos) reportedly settled BIPA claims for $15 million even though plaintiffs' counsel were also suing the employers that used Kronos's timekeeping technology. *See* Jonathan Bilyk, *Timeclock vendor Kronos agrees to pay $15M to end fingerprint scan class action; Lawyers to get $5M*, Cook County Record (Feb. 11, 2022), https://tinyurl.com/4v86cetk.

For smaller companies, the multiplier effects of the district court's accrual rule would be devastating. A company with 100 employees could easily face claims of tens of millions of dollars under the per-scan and per-disclosure approach. *E.g.*, *Jones v. CBC Rest. Corp.*, No. 19-cv-6736 (N.D. Ill. Oct. 22, 2020) (class of approximately 4,000 employees); *Fluker v. Glanbia Performance Nutrition, Inc.*, No. 2017-CH-12993 (Ill. Cir. Ct., Cook Cnty. filed Aug. 20, 2020) (900+ employees).

Such huge claims are life-threatening for many companies, and will inevitably coerce unjustified settlements by companies of all sizes because, "[f]aced with even a small chance of a devastating loss, defendants will be

[9] *See, e.g.*, *Ramsey v. Lake Ventures LLC dba Fresh Thyme Market*, Case No. 2022-L-176 (Ill. Cir. Ct., DuPage Cnty. filed Feb. 18, 2022); *Chavez v. Julian Elec. Servs. & Eng'g Inc. dba Julian Electric*, Case No. 2022-CV-14 (Ill. Cir. Ct., Will Cnty. filed Jan. 31, 2022); *Navarro v. S&B Finishing Co., Inc.*, Case No. 2022-CH-581 (Ill. Cir. Ct., Cook Cnty. filed Jan. 24, 2022); *Williams v. Wings Over Englewood LLC*, Case No. 2022-CH-326 (Ill. Cir. Ct., Cook Cnty. filed Jan. 14, 2022).

pressured into settling questionable claims." *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011); *see also Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 445 n.3 (2010) (Ginsburg, J., dissenting) ("When representative plaintiffs seek statutory damages, [the] pressure to settle may be heightened because a class action poses the risk of massive liability unmoored to actual injury."); *In re Rhone–Poulenc Rorer Inc.*, 51 F.3d 1293, 1297-98 (7th Cir. 1995) ("Judge Friendly, who was not given to hyperbole, called settlements induced by a small probability of an immense judgment in a class action 'blackmail settlements.' Judicial concern about them is legitimate.") (citation omitted).

These problems are especially acute in BIPA cases because unjustified BIPA claims are very difficult to defeat without expensive discovery. Even if the plaintiff signed a BIPA-compliant consent, for instance, fact questions may remain regarding the circumstances of the consent (*e.g.*, whether it preceded the scan) and the treatment of the collected data (*e.g.*, whether and how it was shared with a third party). Here, for example. Ms. Cothron did not plead details about the purportedly unlawful disclosure to third-parties, and the court held that this fact question could not be resolved without discovery and the attendant threat of gigantic damages. *Cothron*, 477 F. Supp. 3d at 732 n.7; *see also, e.g.*, *Roberson v. Maestro Consulting Servs. LLC*, 507 F. Supp. 3d 998, 1017-18 (S.D. Ill. 2020).

As new technologies emerge, the discovery burdens associated with applying BIPA's requirements will become more substantial because a particular technology may only *appear* to capture biometric data—but expensive discovery would still likely be needed to establish that the technology does not do so. Thus, when the complaint alleges that a defendant is using biometric technology, the defendant rarely will be able to prevail on a motion to dismiss even if the technology does not implicate BIPA, because demonstrating whether given technologies meet the statutory criteria requires information outside the record or is perceived to raise "fact" disputes. *E.g.*, *In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155, 1171-72 (N.D. Cal. 2016) ("as the facts develop, it may be that 'scan' and 'photograph' with respect to Facebook's practices take on technological dimensions that might affect the BIPA claims").

The district court's accrual rule would thus usher in a regime where weak claims are easy to generate, difficult to defeat, and coercively ruinous to the defendant. That is not what the legislature envisioned in passing BIPA.

B. The District Court's Rule Creates Perverse Incentives.

Ms. Cothron's proposed accrual rule also will give plaintiffs the unfair and unjustified ability to act unilaterally to multiply dramatically the size of their claims.

In the consumer-technology context, for example, plaintiffs allege that software that scans their or their friends' faces or voices constitutes the collection of biometric information covered by the statute. *E.g.*, *Hazlitt v. Apple*

Inc., 500 F. Supp. 3d 738 (S.D. Ill. 2020). Individual consumers on any given day may upload hundreds of photographs and ask their digital assistants dozens of questions. Simply increasing the quantity of photographs uploaded or number of questions asked would increase the liquidated damages claim.

In the employer context, prospective plaintiffs could continue to use fingerprint scanners or other technology after becoming aware of their potential claims (perhaps multiple times a day) and rack up hundreds of separate violations to use as settlement leverage. The number of scans per individual—and thus the level of exposure under the district court's rule—can be nearly limitless.

By enacting BIPA, moreover, the legislature plainly wanted to encourage businesses to take action to correct perceived inadequacies regarding "biometric identifier-facilitated transactions." 740 ILCS 14/5(e). Consistent with this purpose, a rule that a single claim accrues with the first unauthorized collection or disclosure encourages plaintiffs to bring suit promptly, so that any defects in a company's biometric policies can be remedied. Ms. Cothron's proposed rule, by contrast, encourages plaintiffs to delay bringing suit to increase the number of violations. Even if there is an argument that a plaintiff constructively consents by proceeding in this manner, proving such consent would raise evidentiary issues and require costly discovery, all while plaintiffs use the coercive settlement pressure produced by multiplying the number of violations.

As one member of this Court recognized in *McDonald*, the opportunity for gamesmanship in these cases is significant and should be considered in interpreting and applying BIPA's provisions. 2022 IL 126511, ¶ 59 (Burke, J., concurring) ("This opportunity for gamesmanship in pleading highlights the incongruity of applying the Compensation Act's exclusivity provisions to Privacy Act claims that allege actual injuries but not to those that allege technical violations."). Other courts have recognized similar concerns when interpreting analogous statutes. *E.g.*, *Deutsche Bank Nat'l Tr. Co. v. Quicken Loans Inc.*, 810 F.3d 861, 868 (2d Cir. 2015) (rejecting an interpretation that would "invite litigation gamesmanship"); *Stillmock*, 385 F. App'x at 275 n.* (Wilkinson, J., concurring) ("The potential for such abuse counsels against the plaintiffs' preferred per-receipt interpretation.").

C. The District Court's Rule Will Harm Consumers And Chill Innovation.

Finally, the district court's interpretation will deter innovation and harm consumers and individuals, again contrary to the legislature's intent in passing BIPA.

The legislature observed that biometric technology has important benefits, including the "promise" of "streamlined financial transactions and security screenings." 740 ILCS 14/5(a). But there are many other important applications. Using biometrics, security cameras can recognize strangers outside a home, fingerprint readers can prevent access to sensitive information, and facial recognition systems can help locate missing children

online. As a recent report detailed, biometric technologies soon may increase driver safety by identifying driver fatigue and promote school safety by identifying unauthorized individuals. *See* CBInsights, *9 Industries Biometrics Technology Could Transform* (Dec. 12, 2019), https://tinyurl.com/2s72zwjs.

If BIPA is construed to impose draconian liability, far outstripping any actual harm, then companies will naturally be hesitant to develop these technologies or to deploy them in Illinois. *See, e.g.*, Jack Nicas, *Why Google's New App Won't Match Your Face to Art in Some States*, Wall St. J. (Jan. 18, 2018), https://on.wsj.com/3wjID1w.

The technology at issue in employer cases also has important benefits. For example, businesses use biometrics to keep timekeeping records that are more accurate than traditional time clocks and to prevent "buddy punching" (*i.e.*, the process by which an employee punches in a coworker before they arrive for work, or punches out a coworker after they leave). Biometric technology can also benefit employees, for instance, by protecting the confidentiality of personal information such as the paystubs at issue in this case.

In short, biometric technologies can improve operations, lower costs, improve customer service, and help businesses run more smoothly, all of which benefits business, employees, and consumers. The legislature intended to regulate, not eliminate, these technologies in light of these benefits.

CONCLUSION

For the reasons set forth above, the Court should hold that Section 15(b) and (d) claims accrue only the first time the biometric data is collected or disclosed without consent.

Dated: March 4, 2022

Respectfully submitted,

/s/ Michael A. Scodro
Michael A. Scodro
Jed W. Glickstein
MAYER BROWN LLP
71 S. Wacker Dr.
Chicago, Illinois 60606
(312) 782-0600
mscodro@mayerbrown.com
jglickstein@mayerbrown.com

Counsel for Amici Curiae

Supreme Court 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 27 pages.

/s/Michael A. Scodro
Michael A. Scodro
Mayer Brown LLP