No. 128004

In the

Supreme Court of Illinois

LATRINA COTHRON, individually and on behalf of others similarly situated,

Plaintiff-Appellee,

v.

WHITE CASTLE SYSTEM, INC.,

Defendant-Appellant.

On Certified Question from the United States Court of Appeals
for the Seventh Circuit, Case No. 20-3202.
There Heard on Appeal from the United States District Court
for the Northern District of Illinois, Case No. 19-0382.
The Honorable **John J. Tharp, Jr.**, Judge Presiding.

BRIEF AND SUPPLEMENTAL APPENDIX OF PLAINTIFF-APPELLEE

Ryan F. Stephan
James B. Zouras
Andrew C. Ficzko
Teresa M. Becvar
STEPHAN ZOURAS, LLP
100 North Riverside Plaza, Suite 2150
Chicago, Illinois 60606
(312) 233-1550
rstephan@stephanzouras.com
jzouras@stephanzouras.com
aficzko@stephanzouras.com
tbecvar@stephanzouras.com

Counsel for Appellee Latrina Cothron, individually and on behalf of others similarly situated

ORAL ARGUMENT REQUESTED

COUNSEL PRESS · (866) 703-9373 PRINTED ON RECYCLED PAPER

TABLE OF CONTENTS
AND STATEMENT OF POINTS AND AUTHORITIES

NATURE OF THE CASE

Enacted in 2008, the Illinois Biometric Information Privacy Act ("the Act"), 740 ILCS 14/1, *et seq.*, is an important, though easy-to-comply-with statute governing the collection, dissemination, and use of biometrics by private entities. Under the Act's informed consent regime, a collector is absolutely prohibited from collecting or disseminating a person's biometrics "unless it first" secures their informed consent. For over 10 years, Defendant-Appellant White Castle System, Inc. ("Defendant" or "White Castle") repeatedly collected and disseminated biometrics of its employee, Plaintiff-Appellee Latrina Cothron ("Cothron") without her informed consent.

White Castle contends it violated the Act once and only once—the *first time* it unlawfully collected Cothron's biometric information. At this moment, White Castle claims it effectively stripped Cothron of all her rights under the Act, and White Castle was then free to collect and disseminate biometrics from her indefinitely, as often and for as long as it liked, with no legal consequences.

But as the Appellate Court recently held on indistinguishable facts, White Castle's "one and done" theory is at odds with the plain and unambiguous text of the statute. Echoing the opinion of the lower court in this case, the Appellate Court found that "[a]lmost every substantive section of the Act" shows it applies to each and every scan of a biometric identifier. *Watson v. Legacy Healthcare Fin. Servs., LLC*, 2021 IL App (1st) 210279, ¶ 46 ("*Watson*"); *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 732 (N.D. Ill. 2020) ("*Cothron I*") ("[t]his text is unambiguous and therefore dispositive. A party violates Section 15(b) … the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection.").

After applying the same basic principles of statutory construction, both courts reached the same conclusion, and both got it right. Cothron did not lose her right to make an informed choice before disclosing her biometrics under the Act just because White Castle deprived her of this right once. Immunizing a private entity from subsequent violations in this way would remove any incentive to ever correct its conduct. And despite White Castle's wildly hyperbolic threat of a dystopian future should the Court not see things its way, courts are not authorized to rewrite a statute based on hypothetical or theoretical future outcomes or other so-called "practicalities."

As shown by the well-reasoned path carved by the Appellate Court and District Court for the Northern District of Illinois, the plain text leads to only one conclusion; that a person is "aggrieved," and a claim accrues, any time a private entity collects or disseminates their biometrics without adhering to the Act's straightforward requirements.

ISSUE PRESENTED FOR REVIEW

This Court agreed to answer the following question certified to this Court by the United States Court of Appeals for the Seventh Circuit under Supreme Court Rule 20:

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

SA001-003; *Cothron v. White Castle Sys., Inc.*, 20 F.4th 1156, 1167 (7th Cir. 2021) ("*Cothron II*").

STATEMENT OF FACTS

A. White Castle Repeatedly Collected and Disclosed Cothron's Biometrics Without Her Informed Consent, in Violation of the Act.

Latrina Cothron began working for White Castle in 2004 and remains employed as a restaurant manager. (A015-A016 at ¶¶ 39-40.) In 2004, White Castle introduced a computer system that required Cothron to scan and register her fingerprint to access the computer as a manager and access her paystubs as an hourly employee. (R118 at 23-24.)[1] The fingerprint data captured by the system was not merely stored locally on the device itself. (A013 at ¶ 29; A016 at ¶ 42.) Rather, every time Cothron scanned her finger to access her employer's computer system, White Castle collected, stored and disclosed her fingerprint data to at least two third-party vendors, Cross Match Technologies, Inc. and DigitalPersona, companies which stored her fingerprint data in their databases. (A014 at ¶ 31; A016 at ¶ 41; A018 at ¶ 55; A019 at ¶ 57.)

Much like DNA, distinctive anatomical features like fingerprints, iris scans, voiceprints and scans of hand, and facial geometry (collectively defined as "biometric identifiers" under the Act, 740 ILCS 14/10) are unique, universal, and immutable. For these reasons, beginning in the mid-to-late 2000s, private entities increasingly began deploying biometric identification systems to streamline identity verification. Although the use of these systems in the corporate sector helps maximize profits by increasing productivity and efficiency, the ease with which biometrics are electronically extracted, stored, and disseminated makes them vulnerable to abuse from entities seeking to profit off the data,

[1] For purposes of simplicity, Plaintiff adopts Defendant's citation approach, and all references to "R___" are references to the corresponding docket entries in the district court below.

hackers bent on identity theft, and foreign governments building databases of U.S. citizens. With the rise of biometric technology and commensurate threats posed from its use, the Illinois legislature responded to the "very serious need" to protect the biometrics of Illinois citizens by unanimously passing the Illinois Biometric Information Privacy Act in 2008. 740 ILCS 14/5(a)-(g); 95th Ill. Gen. Assembly, House Proceedings, May 30, 2008, at 249.

White Castle failed to take heed of the new law. Under its plain and unambiguous text, the Act requires a private entity that wants to collect biometrics to first provide written disclosures of specific information and then to "receive" a written release, defined as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." 740 ILCS 14/10, 15(b). For at least ten years, White Castle continued collecting, storing, using, and disseminating Cothron's fingerprints without giving her a meaningful and informed opportunity to say no as required by the Act. (A013 at ¶¶ 27-28.)

B. The District Court Correctly Held That the Statute of Limitations Accrued Each Time White Castle Unlawfully Collected or Disclosed Cothron's Biometrics.

In December 2018, Cothron learned of her biometric privacy rights and brought an action under the Act in Illinois state court, seeking liquidated damages in the amount of $1,000 or $5,000 (for a negligent or reckless and/or intentional violation, respectively) for each count, as well as declaratory and injunctive relief and attorneys' fees and costs. (R1-1.) The case was removed to federal court, and Cothron ultimately filed the operative second amended complaint, where she alleges that White Castle repeatedly captured, collected, stored, used, and disclosed her biometrics for at least ten years without providing the disclosures required by the Act or securing her informed consent. (A007-A028.) After

the Court denied White Castle's motion to dismiss Cothron's second amended complaint, White Castle filed an answer. (R117; R118.) In its answer, White Castle raised a statute of limitations defense and subsequently moved for judgment on the pleadings on the basis that Cothron's claims were time-barred under the maximum five-year limitations period. (R118; R119.) According to White Castle, Cothron's claims accrued once and only once, at its first collection and dissemination of her fingerprints in violation of the Act in 2008, which occurred more than five years before she filed her complaint on December 6, 2018. (R120 at 5.)

The district court disagreed. (A057.) Construing the "plain and ordinary" meaning of the text, the district court found the Act "unambiguous and therefore dispositive" and denied the motion. (A065-66.) With respect to Cothron's claim for *collection* of her fingerprints in violation of Section 15(b), the district court observed that White Castle's biometric device, if it functions as Plaintiff alleges, must capture Cothron's fingerprints each time she accessed the system in order to compare that data to the data captured when the fingerprints were initially registered. (A065.) Applying the text of the Act as written, the district court held that Section 15(b) is violated *not* when an individual "loses control" of her biometrics, as White Castle contended, but "where there is both a failure to provide specific information about collection of biometrics and collection of that data." (*Id.*) This is true the first time a private entity collects biometric information without consent, but "it is no less true with each subsequent scan or collection." (*Id.*) Thus, "for any and all collections, consent must be obtained 'first.'" (A065-66 (quoting 740 ILCS 14/15(b)).) As summarized by the district court, "the only possible conclusion is that White

Castle violated Section 15(b) repeatedly when it collected [Cothron's] biometrics without first having obtained her informed consent." (A066.)

Noting that White Castle failed to set forth any text-based arguments for its position, the district court also denied its motion with respect to Cothron's claim for *disseminating* her fingerprints in violation of Section 15(d). (*Id.*) Particularly because the statute prohibits "redisclosure" of biometrics, the district court held that the "unavoidable" conclusion was that a private entity violates Section 15(d) each time it disseminates biometrics without consent. (*Id.*) Because White Castle failed to obtain consent at any point during the decade following the Act's enactment, the district court held that "each time White Castle disclosed Ms. Cothron's biometrics without consent, it violated Section 15(d)." (*Id.*)

The district court rejected White Castle's contention that following the plain text would lead to "absurd results" in the form of crippling statutory damages, reasoning that imposing "substantial potential liability" is one of the means the legislature adopted to protect biometric information. (*Id.* (quoting *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 36).) Moreover, the district court was bound by "the clear text of the statute," which must be given effect, absurd or not. (*Id.* (citing *Petersen v. Wallach*, 198 Ill. 2d 439, 447 (2002) ("Where the words employed in a legislative enactment are free from ambiguity or doubt, they must be given effect by the courts even though the consequences may be harsh, unjust, absurd or unwise.") (internal quotation omitted).)

C. The Seventh Circuit, on the Heels of the Appellate Court's Decision in *Watson*, Certified the Issue to This Court.

Because Cothron alleged timely violations of Sections 15(b) and 15(d), the district court denied White Castle's motion for judgment on the pleadings. (A067.) The district

court, acknowledging the dearth of apposite Illinois precedent on the issue, granted White Castle's request to certify the ruling for appeal to the United States Court of Appeals for the Seventh Circuit, which accepted White Castle's Petition for Permission to Appeal. (R141; R144.) In her opening brief, Cothron requested the Seventh Circuit to certify the issue to the Illinois Supreme Court for resolution, which White Castle opposed. (Pl.'s Br. at 9-14; Def.'s Reply Br. at 3-7.) Following briefing and oral argument, the Seventh Circuit agreed that Cothron met the requirements for certification and certified the question to the Illinois Supreme Court. (A076-77.)

Weighing the arguments, the Seventh Circuit noted that the premise underlying White Castle's "one-and-done" accrual theory, that "two violations aren't worse than one[,] may simply be wrong." *Cothron II*, 20 F.4th at 1165. "Repeated collections or disclosures of biometrics, even if by the same entity, might increase the risk of misuse or mishandling of biometrics. If so, each violation would seem to independently aggrieve a plaintiff." *Id.* Moreover, the Seventh Circuit noted that White Castle's theory is "hard to square with the broad language in *Rosenbach* that '[n]o additional consequences need be pleaded or proved' other than a violation of the plaintiff's statutory rights." *Id.* (citing *Rosenbach*, 2019 IL 123186 at ¶ 34).) Acknowledging the Illinois Appellate Court's recent decision in *Watson*, which held that a Section 15(b) claim accrues at each unlawful collection, the Seventh Circuit found that, as *Watson* is the only Illinois appellate decision to address claim accrual under the Act, it was proper to certify the issue to the Illinois Supreme Court for "authoritative guidance." *Id.* at 1166 n.2. Thereafter, this Court agreed to answer the certified question of law on December 23, 2021. Order at *1 (Dec. 23, 2021).

STANDARD OF REVIEW

The interpretation of a statute is a question of law that is reviewed *de novo*. *VC&M, Ltd. v. Andrews*, 2013 IL 114445, ¶ 30.

ARGUMENT

I. The Appellate Court Got It Right in *Watson*: A Claim Accrues at Each and Every Collection or Dissemination of Biometric Information.

Interpreting the text of the Act as written, an entity violates Section 15(b) upon "each and every capture and use of plaintiff's fingerprint" without informed consent. *Watson*, 2021 IL App (1st) 210279, ¶ 46. Likewise, "each time an entity discloses or otherwise disseminates biometric information without consent," it violates Section 15(d). *Cothron I*, 477 F. Supp. 3d at 733. Not only is this the only result dictated by the express language of the statute, but it comports with dictionary definitions of the statutory language, best gives effect to every word in the statute, and directly reflects the legislative intent motivating the Act's passage (*i.e.*, to ensure that individuals have a meaningful and informed opportunity to say no to the collection of their biometrics). It also provides the greatest possible incentive for biometrics collectors to take action to mitigate their conduct if they neglected to comply at first.

A. The Plain Text Dictates that Section 15(b) and 15(d) Claims Accrue Each Time a Private Entity Collects or Disseminates Biometrics Without Informed Consent.

The plain text of the Act leads to only one conclusion: each time an entity collects and disseminates an individual's biometric information without prior informed consent, it violates Section 15(b) and 15(d) of the Act. As the Illinois Appellate Court correctly held in *Watson*, "[t]he plain language of the statute establishes that it applies to each and every

capture and use of Plaintiff's fingerprint or hand scan. Almost every substantive section of the Act supports this finding." 2021 IL App (1st) 210279, ¶ 46.

When interpreting a statute, the court's "primary objective is to ascertain and give effect to the intent of the statute's drafters." *Id.* ¶ 34 (citing *VC&M, Ltd. v. Andrews*, 2013 IL 114445, ¶ 30). As such, "the most reliable indicator of the drafters' intent is the language used in the statute itself, which should be given its plain and ordinary meaning." *Id.* Contrary to White Castle's insistence, proper analysis of the accrual question begins by looking to letter of the statute, not "this Court's precedent." *See* Def.'s Br. at 10, 22 (explaining that *Rosenbach, West Bend,* and *McDonald* define an injury under the Act, and the text merely "confirms" it); *Michigan Ave. Nat. Bank v. Cty. of Cook*, 191 Ill. 2d 493, 504 (2000) ("The statutory language must be given its plain and ordinary meaning, and, where the language is clear and unambiguous, we must apply the statute without resort to further aids of statutory construction.").

In full, Section 15(b) of the Act provides:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, ***unless it first***:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b) (emphasis added). Under the express language of the text, an entity violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometrics without *prior* informed consent. *Watson*, 2021 IL App (1st) 210279, ¶ 53. "The word 'first' does not modify or change 'collect' or 'capture,'" but instead, "the word modifies the words 'informs' and 'receives.'" *Id.* (citing 740 ILCS 14/15(b)). In other words, the term "first" describes White Castle's obligations, not the scan of Cothron's fingerprint. As there is no temporal modifier limiting "collect" or "capture," "the requirements apply to each and every collection and capture." *Id.*

Dictionary definitions of the terms the legislature used in the Act confirm the conclusion that White Castle committed a series of repeated, independently-actionable violations. When a statute does not define its own terms, a reviewing court may use a dictionary to ascertain the plain and ordinary meaning of those terms. *Maschek v. City of Chicago*, 2015 IL App (1st) 150520, ¶ 56 (citing *People v. McChriston*, 2014 IL 115310, ¶ 15, and *People v. Bingham*, 2014 IL 115964, ¶ 55).[2] In Section 15(b), the word "collect" can mean "to gather," "'as in '[t]he professor collected the students' exams.'" *Watson*, 2021 IL App (1st) 210279, ¶ 59 (citing Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/collect (last visited Dec. 1, 2021); Dictionary.com, https://www.dictionary.com/browse/collect (last visited Dec. 1, 2021)). Here, as in *Watson*, White Castle "gathered" fingerprint scans from Cothron repeatedly in order to grant her access to its systems each workday, "similar to a professor gathering his

[2] As noted in *Watson*, when interpreting the Act, reviewing Courts in Illinois have looked to definitions from both Merriam-Webster's Dictionary and Dictionary.com. 2021 IL App (1st) 210279, ¶ 56 (citing *Rosenbach*, 2019 IL 123186, ¶ 32; *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175, ¶ 53).

or her students' exams at the end of class." *Id.* The dictionary definition confirms the reading of the plain language of the statute that White Castle's obligations applied to "each and every" fingerprint scan. *Id.* ¶ 60.

The same holds true for violations of Section 15(d). In full, Section 15(d) of the Act provides:

> No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
>
> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d). As under Section 15(b), an entity violates Section 15(d) when it discloses, rediscloses, or otherwise disseminates a person's biometrics without prior consent.

While Section 15(d) does not contain the word "first," Section 15(d)'s use of the word "unless" has the same substantive effect, prohibiting an entity from disclosing an individual's biometrics until consent is obtained from that individual, which, logically, must occur before the disclosure. In other words, any disclosure of biometrics is unlawful unless the individual has provided consent. In Section 15(d), "unless" acts as a conjunction, modifying Section 15(d)'s complete prohibition on disclosure of biometrics and providing

for a limited number of circumstances under which entities in possession of biometrics may disclose, redisclose, or disseminate it. "Unless" is defined as "except on the condition that" or "except under the circumstances that." *See* Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/unless (last visited Apr. 7, 2022); Dictionary.com, https://www.dictionary.com/browse/unless (last visited Apr. 7, 2022). Extending *Watson*'s logic to Section 15(d), an entity cannot disclose, redisclose, or disseminate biometrics "except on the condition" that it has secured consent to the disclosure. The word "disclose" means "to make known." Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/disclose (last visited Apr. 7, 2022); Dictionary.com, https://www.dictionary.com/browse/disclose (last visited Apr. 7, 2022). White Castle "made known" each of Plaintiff's sensitive, private fingerprint scans to third parties that host and store that data. As under Section 15(b), the dictionary definition illustrates that White Castle's obligation to obtain consent applied each time it disclosed Cothron's biometrics to a third party.

This conclusion is "especially unavoidable" because Section 15(d) includes "redisclosure" as an act prohibited without informed consent. *Cothron I*, 477 F. Supp. 3d at 733. While the term "redisclosed" is undefined in either the Merriam-Webster Online Dictionary or Dictionary.com, the prefix "re-" is defined as "again" or "'again and again' to indicate repetition." *See* Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/re (last visited Apr. 7, 2022); Dictionary.com, https://www.dictionary.com/browse/re- (last visited Apr. 7, 2022). Thus, when White Castle "made known" each of Cothron's fingerprint scans to a third-party recipient "again and again"—*i.e.*, "redisclosed" that data—under the express terms of the statute, consent

was not only required for the initial "disclosure," but *also* required for any subsequent "redisclosure."

Looking to other sections of the Act yields the same result. *Watson*, 2021 IL App (1st) 210279, ¶ 46 ("[a]lmost every substantive section of the Act supports th[e] finding" that the Act "applies to each and every capture and use of Plaintiff's fingerprint or hand scan"). In the Act's "Definitions" section, a "[b]iometric identifier" includes, among other identifiers, a "fingerprint." 740 ILCS 14/10. Meanwhile, the same section defines "[b]iometric information" to "mean[ ] any information, regardless of how it is captured," so long as it is "based on an individual's biometric identifier" and "used to identify an individual." *Id.* Here, Cothron has alleged that White Castle captured her fingerprint each time she scanned it to access White Castle's computer system. (A016 at ¶ 40.) Because the Act applies to "any information, regardless of how it is captured," it applies, by its plain terms, to each independent capture of Cothron's fingerprint to identify her. *See Watson*, 2021 IL App (1st) 210279, ¶ 48 (citing 740 ILCS 14/10).

Finally, the legislative purpose explicitly set forth in the Act further demonstrates that the privacy concerns driving the statute's enactment debunk any suggestion that the Illinois General Assembly intended to place artificial, extra-statutory limits on the acts and omissions that could give rise to liability. The findings of the General Assembly reveal its intent to provide Illinois citizens with the broadest and most expansive biometric privacy protections and the urgent need to do so. *See* 740 ILCS 14/5 (f)-(g) ("[t]he full ramifications of biometric technology are not fully known," and the "public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information"); 95th Ill. Gen. Assembly, House

Proceedings, May 30, 2008, at 249 (Illinois in "very serious need of protections for the citizens of Illinois when it comes to biometric information"). "The stated purpose, then, is to regulate not simply the 'collection' but also everything that follows." *Watson,* 2021 IL App (1st) 210279, ¶ 49. This must include the subsequent "use," "handling," "safeguarding," and "storage" of the collected information, evidencing the drafters' clear intent to regulate an entity's conduct past its initial collection and disclosure of an individual's biometrics. *Id.*

Because the plain, unambiguous text mandates that a claim accrues under Section 15(b) and 15(d) each time that White Castle collected, captured, or otherwise obtained Plaintiff's biometrics and disclosed Plaintiff's biometrics to a third party without consent, the Court's analysis must end here. *See, e.g.*, *Maschek*, 2015 IL App (1st) 150520, ¶ 44 ("If the statutory language is clear, we must apply it, without resort to any aids of statutory construction.") (citing *Krohe v. City of Bloomington,* 204 Ill. 2d 392, 395 (2003)).

B. White Castle's Atextual Theory That a Private Entity Can Take a Person's Control (and Now "Secrecy") Only Once Is Both Irrelevant and Wrong.

Rather than engage with the plain text of the statute at the outset, as required by basic principles of statutory construction, White Castle turns the entire analysis on its head to achieve its preordained result. White Castle correctly recognizes that, "when the statutory language is plain and unambiguous, [the Court] may not depart from the law's terms by reading into it exceptions, limitations, or conditions the legislature did not express, nor may we add provisions not found in law." Def.'s Br. at 22 (citing *Rosenbach,* 2019 IL 123186, ¶ 24). However, in its next breath, White Castle dismisses this legal rule and urges the Court to utilize "canons of statutory construction" to "guide the interpretation

of the Act" and "grasp the intended meaning of [the] statutory language." *Id*. Canons of statutory construction only come into play if the language of the statute is ambiguous, and White Castle makes no showing whatsoever on this point. *Chapman v. Chicago Dep't of Fin.*, 2022 IL App (1st) 200547, ¶ 24 (citing *Palm v. Holocker*, 2018 IL 123152, ¶ 21); *see also Watson*, 2021 IL App (1st) 210279, ¶ 42 ("[w]here the language is plain and unambiguous, we apply the statute without resort to further aids of statutory interpretation"). "[S]imple disagreement between the parties will not create ambiguity in the statute." *Mosby v. Ingalls Mem. Hosp.*, 2022 IL App (1st) 200822, ¶ 43.

Because the language of the Act is clear and unambiguous, as set forth above, the analysis ends there. But even if the Court were to look beyond the plain language, the canons of statutory interpretation do not support the result White Castle seeks. In an effort to undermine *Watson*, White Castle argues that the Illinois Appellate Court erred in determining that a Section 15(b) claim accrues at each collection because it "failed to interpret the Act's plain language consistent with its legislative intent, as set forth in *Rosenbach*." Def.'s Br. at 29. But the *Watson* court explicitly considered the Act's legislative intent, purpose, and history as set forth *in the statute itself*. 2021 IL App (1st) 210279, ¶ 49 (the legislative intent is easily determined because the drafters provided specific "legislative findings" and "intent" sections in the Act) (citing 740 ILCS 14/5).

White Castle nevertheless argues that *Rosenbach* "instructs that an injury occurs under the Act when the 'power to say no' is lost." Def.'s Br. at 29 (failing to cite the relevant passage in *Rosenbach*). That much is true, but *Rosenbach* in no way stands for the proposition that a claim accrues only the *first* time a person is deprived of the power to say no to the collection of their biometric information. Rather, *Rosenbach* squares completely

with Cothron's argument that a claim accrues *every* time a fingerprint scan is captured or disclosed without informed consent. In fact, the full text of the "power to say no" quote cited by White Castle stresses that the statute is a regime of informed consent: "The Act vests in individuals and customers the right to control their biometric information *by requiring notice before collection and giving them the power to say no by withholding consent*." *Rosenbach*, 2019 IL 123186, ¶ 34 (citing *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018)) (emphasis added). The Act regulates not only the first collection of biometrics but also what entities use this data for, how it's retained, who they disclose it to, and how and when the data is destroyed. *McDonald v. Symphony Bronzeville Park, LLC et al.*, 2022 IL 126511, ¶ 21. The Act empowers individuals with the opportunity to "say no" when they are properly provided notice of their rights, not just at the initial collection and disclosure.

This Court in *Rosenbach* held that the failure to comply with the requirements of Section 15, *in and of itself*, supports a statutory cause of action for violation of the Act. It explained:

> [w]hen a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach. Consistent with the authority cited above, such a person or customer would clearly be "aggrieved" within the meaning of section 20 of the Act (*id.* § 20) and entitled to seek recovery under that provision. No additional consequences need be pleaded or proved. *The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action*.

Id. ¶ 33 (emphasis added). White Castle repeatedly collected and disclosed Cothron's biometrics for at least ten years without providing any notice of her rights or the

opportunity to "say no" as required under the Act.[3] Under *Rosenbach*, White Castle's failure to comply with Section 15 in 2018 was no different than its failure in 2008. Thus, Cothron has asserted a timely cause of action.

White Castle claims that "[b]ecause the invasion and injury is the loss of control, and control cannot be lost twice, there is no second invasion or injury, the same as there is no thousandth invasion or injury." Def.'s Br. at 21. And, for the first time here, White Castle doubles down by arguing a similar "loss of secrecy" theory. *Compare id.* at 13-16 *with* Appellant's Br. at 19-22, *Cothron v. White Castle Sys., Inc.*, No. 20-3202 (7th Cir. Mar. 29, 2021). These atextual theories are premised upon terms and concepts found nowhere in the Act and are in direct conflict with *Rosenbach*. A person is not "aggrieved" and cannot plead a claim under the Act by alleging a private entity took "control" of biometrics or deprived them of "secrecy." *See Rosenbach*, 2019 IL 123186, ¶ 33 (a person is "aggrieved" under the Act "when a private entity fails to comply with one of section 15's requirements"). The Act doesn't prohibit a collector from taking control of biometrics; it *permits it* after certain conditions are first met. Likewise, individuals are not *less* aggrieved at subsequent noncompliant collections or disclosures than at the first one. They have the same rights (to accurate, specific current information and the right to make a choice) before each collection and disclosure of their biometrics. White Castle is not entitled to continue keeping Cothron in the dark and making choices for her just because it did so once.

[3] White Castle suggests that Cothron voluntarily enrolled and "consented" to the use of its fingerprint system when it originally began harvesting biometric data in 2004. Def.'s Br. at 5-6. However, the question of whether Cothron's "generic consent" complies with the requirements of the Act was rejected by the District Court and is not before this Court. *Cothron v. White Castle Sys., Inc.*, 467 F. Supp. 3d 604, 614 (N.D. Ill. June 16, 2020).

Thus, whether "control" over biometrics can be "lost twice" is irrelevant; that is not the nature of the "right to control" defined in *Rosenbach* and the Act itself (*i.e.*, notice and the power to say no). Instead, White Castle's nebulous "loss of control" accrual theory rests on a faulty comparison to invasion of privacy and data breach claims that accrue once, when personal information is *actually compromised* and cannot be recovered.

Numerous courts, including this Court and the Appellate Court, have all rejected the contention that the Act provides redress only once a person's biometrics have actually been compromised. Indeed, the General Assembly noted that "once [biometrics are] compromised, the individual has no recourse." 740 ILCS 14/5(c). The Act is not aimed at redressing harm that occurs as a result of a generic loss of privacy, security breach or identity theft (none of which give rise to a cause of action under the statute), but rather is designed to prevent such problems "by imposing safeguards to insure that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to begin with." *Rosenbach*, 2019 IL 123186, ¶ 36.

White Castle's proposed "one and done" accrual rule makes no sense in light of the risks the Act guards against. Not only does this effective re-writing of the statute undermine the General Assembly's authority, it makes a mockery of the serious and ever-evolving threats to biometric privacy—both known and unknown—and the critical need to inform and secure consent from an otherwise largely unaware general public. As this Court observed in *McDonald*, "[t]he General Assembly has tried to head off such problems before they occur by imposing safeguards to ensure that the individuals' privacy rights in their biometric identifiers and biometric information are properly protected before they can be compromised and by subjecting private entities who fail to follow the statute's

requirements to substantial potential liability." 2022 IL 126511, ¶ 48. "The stated purpose, then, is to regulate not simply the 'collection' but also everything that follows, including the subsequent 'use' and 'storage' of the collected information." *Watson,* 2021 IL App (1st) 210279, ¶ 49 (citing 740 ILCS 14/5(g)).

If this Court allows White Castle's interpretation to stand, private entities would have no incentive to comply with the Act. In fact, White Castle's "one and done" accrual rule incentivizes collectors of biometrics *not* to take any corrective action to mitigate their violations, safeguard data, or provide contemporaneous information once they fail to do so the first time and forever relieves them from their duty to take action. For example, had White Castle realized its mistake one month after its first unlawful collection and provided Cothron with the proper disclosures, she could have considered the information, asked questions and if not satisfied with White Castle's answers, instructed it to stop any future collection and future dissemination of her biometrics. She also could have asked White Castle to destroy the data it already illegally collected from her. As the Seventh Circuit emphasized, the longer a private entity has biometrics, the greater the potential for a breach or other future abuse. *Miller v. Sw. Airlines Co.*, 926 F.3d 898, 902 (7th Cir. 2019). Accordingly, the rights afforded under the Act are designed to work in conjunction with the duty to safeguard the data.

But under White Castle's theory, after its first unlawful collection, there was no limit on what it could do with the data (sell it, disseminate it to anyone it likes, store it however and wherever it likes), and it ***never had to tell Cothron what it was doing***. This contravenes the purpose of the Act to level the playing field between the collector and those whose biometrics are collected, without which White Castle has all the information and the

unfettered ability to make all decisions for Cothron. This is but one example of the perverse incentives that reward the worst violators, like White Castle, that repeatedly break the law for the longest periods of time. Unquestionably, any consideration of the stated purpose of the Act favors applying the statute exactly as written.

White Castle also misapplies this Court's *Feltmeier* decision to support its "one-and-done" claim accrual theory. According to *Feltmeier*, "[g]enerally, a limitations period begins to run when facts exist that authorize one party to maintain an action against another." *Feltmeier v. Feltmeier*, 207 Ill. 2d 263, 278 (2003). White Castle then suggests that "[o]nce the train left the station" and Cothron was harmed by the White Castle's first violation of the Act, "any further harm to Plaintiff was what *Feltmeier* deems a 'continual effect' of her initial loss of control over and privacy in her biometrics." Def.'s Br. at 12 (quoting *Feltmeier*, 207 Ill. 2d at 279). *Watson* flatly rejected this argument. 2021 IL App (1st) 210279, ¶¶ 68-69. First, it again falsely assumes the nature of the injury is "loss of control," which it is not, and ignores all the subsequent occasions, after the initial violation, that White Castle inflicted the actual injury of collecting, using, and disseminating Cothron's biometrics without informed consent. *Id.* ¶ 69. Second, as the *Watson* Court noted, this Court's use of the word "generally" preceding the legal precepts shows it is not "absolute." *Id*. Third, as the plain text reads, "the Act places the burden of notification of a possible injury squarely on the entity choosing to utilize the information rather than on the person from whom the information is obtained." *Id*. Interpreting the statute as White Castle advocates instead flips the burden, imposing the duty on individuals to guard against private entities mishandling biometrics and shifting away from the proactive, compliance-based nature of the statute as written. Finally, the court reasoned that its finding is

consistent with this Court's reasoning in *Rosenbach*, holding, "when a private entity fails to comply with *one of* section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person." *Id.* (emphasis in original) (quoting *Rosenbach*, 2019 IL 123186, ¶ 33). As the *Watson* Court concluded, *Feltmeier* is inapposite.

White Castle's position is also impossible to reconcile with the Seventh Circuit's characterization of the Act in *Bryant v. Compass Group USA, Inc.* as a privacy statute that guards against "informational injuries." 958 F.3d 617, 623-25 (7th Cir. 2020). In *Bryant*, the Seventh Circuit reinforced *Rosenbach's* holding that the mechanism of "control" in the context of Section 15(b) is the informed consent regime that lies at "the heart of" the Act—that is, "a right to receive certain information from an entity that collects, stores, or uses a person's biometric information[.]" *Id.* at 621, 626. Accordingly, the injury Cothron seeks to redress is White Castle's failure to provide "substantive information to which [she] was entitled" that "thereby deprived her of the ability to give the *informed* consent section 15(b) mandates." *Id*. at 626 (emphasis original).

As Cothron alleges, White Castle collected her biometrics each time she scanned her fingerprint to access its computer system. Because each collection throughout Cothron's employment (or at least through 2018 at the earliest) was done without obtaining written informed consent, White Castle violated the Act each time Cothron scanned her fingerprint. White Castle's "loss of control" theory finds no support in the text of the Act or the Act's interpretation by numerous courts and must be rejected.[4]

[4] Plaintiff agrees with the position of amici the American Association for Justice and Employment Law Clinic of the University of Chicago Law School's Edwin F. Mandel

C. White Castle's Accrual Theory is Supported Only by a Confused, Convoluted and Twisted Interpretation of the Act.

White Castle submits its so-called text-based arguments only as an afterthought to confirm its "one-and-done" accrual theory. Def.'s Br. at 23-27, 30-33. Implicitly acknowledging that the plain text leads squarely to the conclusion that a claim accrues each time a private entity collects or disseminates a person's biometrics, White Castle's hollow invocation of the Act's terms ignores their plain and ordinary meaning.

White Castle first declares war with the plain text of Section 15(b) by wholly ignoring basic rules of English grammar, defining the term "first" only by reference to its adjective form. Def.'s Br. at 23. As the term "first" in Section 15(b) modifies a verb (*i.e.*, "informs" and "receives") rather than a noun, the appropriate definition to consider is that associated with its adverb form. *See* 740 ILCS 14/15(b). Doubling down, White Castle then submits that "first" must be read to refer to "a singular point in time," that must "precede, or occur before, collection." Def.'s Br. at 23-24. Despite setting forth definitions for each verb in Section 15(b), White Castle strips away their independent meanings to conclude they each "involve gaining control of biometrics," "an action that only happens once." Def.'s Br. at 24-25 (pointing to the canons *noscitur a sociis* and *ejusdem generis* to support its conclusion). But White Castle's argument has a glaring flaw: it points to nothing in the text to support its assertion that "gaining control of biometrics," in and of itself, somehow gives rise to a cause of action, or that it is "an action that only happens once." *Id.* at 26. "Defendant[ ] seek[s] to rewrite the statute so that it reads "before an entity *first* collects or captures," but the statute is not written that way." *Watson*, 2021 IL App (1st) 210279, ¶ 53.

Legal Aid Clinic that the continuing violation doctrine can apply, under which a BIPA violation accrues upon the last unlawful act.

Because the term "first" modifies the verbs "informs" and "receives," rather than the triggering verbs "collect," "capture," or "obtain," the plain text clearly establishes that "the requirements apply to each and every collection and capture." *Id.*

Again disregarding the statute's plain text, White Castle similarly relies on *noscitur a sociis* to supplant the plain meaning of Section 15(d) to limit a Section 15(d) violation to the singular moment of initial disclosure of biometrics without informed consent. Def.'s Br. at 33. Ignoring the term "unless," White Castle claims that "Section 15(d) requires consent in order for a private entity to 'disclose, redisclose, or otherwise disseminate' an individual's biometrics." Def.'s Br. at 31. White Castle again concludes, with no analysis or anchor in the text, that "Section 15(d) bars the disclosure of biometrics, without consent, to a new party that did not previously have them."

What is in the statute, however, is an explicit prohibition on both "disclosing" and "redisclosing" biometrics without informed consent. White Castle relies on a definition from a European online dictionary never before referenced in any published opinion by any court in the United States, to sweep the term "redisclose" under the rug, explaining that it "means 'to disclose what has been disclosed to the discloser'" and "is meant to ensure that downstream entities are subject to Section 15(d)." Def.'s Br. at 31-32. White Castle fails to mention that the first listed definition of the term "redisclose" in its preferred dictionary is "to disclose again." *See* WordSense Online Dictionary, https://www.wordsense.eu/redisclose/ (last visited Apr. 7, 2022). And White Castle acknowledges that the Merriam-Webster Dictionary defines the prefix "re-" as "again" and "disclose" as "to make known or public," meaning that "redisclose" is most logically defined as "to make known again." *See* Def.'s Br. at 32-33. But White Castle does not

accept the plain meaning of Section 15(d)'s prohibition on redisclosure, as held by the district court, to mean multiple disclosures from one entity to another and instead proposes the most illogical and unnatural reading—that it refers to a disclosure from one entity to another entity who then *rediscloses* the same biometrics to a third entity. Def.'s Br. at 30-31.

White Castle's reading renders the term "redisclosure" as used in the statute redundant. *People v. Baskerville*, 2012 IL 111056, ¶ 25 (a court is obligated to presume that each part of a statute has meaning and avoid a construction that renders a part of the statute superfluous or redundant). Section 15(d)'s duty to obtain consent for disclosure applies to any "private entity *in possession* of a biometric identifier or biometric information," regardless of whether the entity received the data from another entity or it collected the data itself. 740 ILCS 14/15(d) (emphasis added). Whether the data is being disclosed to a third, fourth, or fifth entity, the requirement to obtain consent for that disclosure is the same.

Under White Castle's reading, though, the terms "disclosure" and "redisclosure," as used in the statute, are indistinguishable. While White Castle asserts that "it would be antithetical to this Court's precedent (and plain English) to read 'redisclose' to meaning [*sic*] anything substantially different than to 'disclose' or to 'disseminate,'" Def.'s Br. at 33, nothing in the statutory text compels such a restrictive reading of Section 15(d). *See People v. Clark*, 2019 IL 122891, ¶ 47 (a "court may not 'constructively' add a requirement to a statute that the legislature plainly chose not to include"). Limiting Section 15(d) violations only to the "first" disclosure reads a requirement into the statute that simply is not there.

D. Section 15(d) Violations Are Wholly Distinct From Violations of Publication-Based Privacy Statutes.

As the first informed consent statute in the nation that protects biometrics, the Act was not enacted to codify a privacy tort or provide legislative protection of a traditional privacy right. Instead, by passing the Act, the General Assembly intended to give individuals the opportunity to make informed choices about to whom and for what purpose they will relinquish control of their biometrics. In this way, other than being a law that protects privacy rights, the Act has nothing in common with the publication-based Illinois privacy statutes to which White Castle seeks to analogize.

On its face, the "single-publication rule" plainly has no applicability, because violations of Section 15(d) are not torts and are not premised upon a "single publication," but repeated non-consensual disclosure of biometrics. As codified in the Uniform Single Publication Act, 740 ILCS 165/1, *et seq.*, the single-publication rule provides that:

> No person shall have more than one cause of action for damages ***for libel or slander or invasion of privacy or any other tort founded upon any single publication*** or exhibition or utterance, such as any one edition of a newspaper or book or magazine or any one presentation to an audience or any one broadcast over radio or television or any one exhibition of a motion picture.

740 ILCS 165/1 (emphasis added). At its core, the single-publication rule "protects speakers and writers from repeated litigation arising from a single, but mass-produced, defamatory publication" in order to prevent piecemeal litigation in actions for libel, slander, invasion of privacy, or other torts requiring publication as an element. *Pippen v. NBCUniversal Media, LLC*, 734 F.3d 610, 615 (7th Cir. 2013). This Court has noted that the "clearest example" of application of the single-publication rule is "where the defamatory material is contained in a book or a magazine of nationwide distribution."

Ciolino v. Simon, 2021 IL 126024, ¶ 38 (2021). The single-publication rule protects the publisher such that they "will not be subject to a separate suit for each individual who reads the defamatory material following the release of the first edition or particular issue." *Id.*

In contrast to the Act, "the heart" of which is about securing informed consent, *see Bryant*, 958 F.3d at 626, defamation and related torts are about damage done to a person's reputation by information publicized to the public. *Kolegas v. Heftel Broad. Corp.*, 154 Ill. 2d 1, 10 (1992) (a defamatory statement is one that "tends to cause such harm to the reputation of another that it lowers that person in the eyes of the community or deters third persons from associating with him"). And unlike these privacy torts, as set forth in Section I.B, *supra*, the Act does not provide redress for the harms that occur as a result of an individual's biometrics being *actually compromised*. Rather, the Act "impos[es] safeguards" designed to prevent such problems from occurring in the first place. *Rosenbach*, 2019 IL 123186, ¶ 36.

These distinctions are fundamental, but that has not stopped White Castle from arguing that depriving someone of the choice to say no to the dissemination of their fingerprints to third parties is no different than airing a commercial allegedly assuming the likeness of the world record holder for hacky sack (*Martin v. Living Essentials, LLC*, 160 F. Supp. 3d 1042, 1044-1045 (N.D. Ill. 2016), *aff'd*, 653 F. App'x 482 (7th Cir. 2016)) or re-posting a product demonstration video allegedly using a person's likeness (*Troya Int'l, Ltd. v. Bird-X, Inc.*, No. 15 c 9785, 2017 WL 6059804, at *2-3 (N.D. Ill. Dec. 7, 2017)). These glaring factual differences make apparent that nothing in the text of the Act concerns "mass-produced, defamatory publication" such that the single-publication rule applies here. *Pippen*, 734 F.3d at 615. Even adopting—for argument's sake—White Castle's

application of the single-publication rule to fingerprint collection, Cothron has not alleged that her biometrics were mass produced to a general or national audience, nor could she state a cause of action under the Act if it was. *See Blair v. Nevada Landing Partnership*, 369 Ill. App. 3d 318, 326 (2d Dist. 2006) (finding that the photo at issue was "delivered to a mass sector of the public");[5] *Winrod v. Time, Inc.*, 334 Ill. App. 59, 60 (1st Dist. 1948) (noting that the issue of *Life* magazine was distributed "throughout the United States").

This Court's recent decision in *Ciolino* does not help White Castle, but instead further illustrates why the single-publication rule cannot apply to Section 15(d) claims. In *Ciolino*, the Court analyzed whether separate screenings of a documentary in different cities were re-publications of defamatory material that retriggered the statute of limitations. 2021 IL 126024, ¶¶ 36-46. The Court declined to apply the single-publication rule and held that each separate and limited screening to new and distinct audiences constituted a new publication. *Id.* ¶ 40. The Court observed that application of the single-publication rule in such circumstances would not serve the rule's purpose to "prevent ungovernable piecemeal liability and a potentially endless tolling of the statute of limitations." *Id.* ¶ 43 (internal quotation omitted).

Likewise, there is no "endless tolling" of the statute of limitations under the Act that necessitates application of White Castle's proposed "one and done" accrual rule, which it likens, erroneously, to the single-publication rule. There is no danger that White Castle will be endlessly subject to separate suits for future violations of Section 15(d) because it

[5] *Watson* also distinguished *Blair* on the basis that it involves a completely different statute, the Right of Publicity Act, which provides that "[t]he rights under this Act are property rights that are freely transferable," unlike biometric rights that are inherently *not* transferable. 2021 IL App (1st) 210279, ¶ 70 (quoting 765 ILCS 1075/15).

has complete power to toll the statute on its own. All it must do is cease to disclose individuals' biometrics or comply with the straightforward, easy-to-follow informed consent requirements of the statute.

II. So-Called Constitutional Concerns Over Hypothetical Future Damage Awards and Other "Practicalities" Are Not Reasons to Invalidate the Plain Text.

White Castle and its *amici* pay lip service to the plain text, but then implore the Court to do anything but follow it. In what has become a recurring theme, considerations they say take precedence over the plain and ordinary meaning of the Act, stretched across 90 pages of combined briefing, include: (1) the absence of a "guarantee" the trial court won't enter an unconstitutional damages award if it finds liability (ignoring the federal and state Constitutions, the Due Process Clause of the Fourteenth Amendment, the Eighth Amendment, decades of binding federal and state precedent, and the trial court's presumed familiarity with these documents); (2) public safety (rather than ask individuals to sign an informed consent form, providers of biometric devices in the vehicle, home security, hazardous material storage, and other critical sectors will refuse to sell, develop or implement biometric technology in Illinois); (3) the need to discourage future litigation (claiming, without evidence, that the vast majority of plaintiffs with valid claims under the Act are anxiously awaiting this Court's ruling to decide whether to file suit); (4) how biometric technology works (which the jurists on the Appellate Court and Federal district court "misapprehended");[6] and (5) the need to prevent a statute of limitations that never

[6] It is not the Court's role to analyze, at the pleading stage, White Castle's defenses on the merits by researching how its devices capture biometrics and rule in accordance with its findings. *See* Def.'s Br. at 29 (criticizing the Appellate Court for "misapprehending" and "never so much as mention[ing]" how biometric devices operate); *see also id*. at 8-9 (White Castle stating, in its Statement of Facts, that the courts are "confused.") Cothron alleges

tolls (which can happen only if a biometric collector repeatedly and perpetually breaks the law rather than come into compliance with the Act). *See generally* Br. of Ill. Chamber of Commerce et al. as Amici Curiae; Br. of Ill. Manufacturers' Ass'n et al. as *amici curiae*; Br. of Retail Litig. Ctr., Inc. et al. as *amici curiae*.

Variations on these sentiments were previously raised to this Court in *Rosenbach*[7] and *McDonald*,[8] the Appellate Court in *Watson*,[9] the Seventh Circuit in this case[10] and again here, each time with progressively more hyperbolic assertions, theories, and prognostications. But as all these courts have made clear, courts don't decide constitutional or other questions in the abstract. *See Watson*, 2021 IL App (1st) 210279, ¶ 66 n.4 ("Questions relating to damages are not before us."); *McDonald*, 2022 IL 126511, ¶¶ 48-

---

that White Castle collected and disclosed her biometrics at each fingerprint scan. (A014 at ¶ 31; A016 at ¶ 41; A018 at ¶ 55; A019 at ¶ 57.)

[7] *See* Br. of Illinois Chamber of Commerce as Amicus Curiae at 10, *Rosenbach v. Six Flags Ent. Corp.*, No. 123186 (Ill. Sept. 10, 2018) (charting potential damages of $5 billion for an employer with 1,000 employees that scan their fingerprints four times per workday), *available at* https://epic.org/wp-content/uploads/amicus/bipa/rosenbach/ Rosenbach-v-Six-Flags-Illinois-Chamber-of-Commerce-Amicus.pdf (last visited Apr. 7, 2022). Rather than entertain these premature damages arguments, the *Rosenbach* Court analyzed only the question before it on the preliminary dispositive motion and made the point that the Act was designed to expose violators "to substantial potential liability." 2019 IL 123186, ¶ 36.

[8] *See McDonald*, 2022 IL 126511 at ¶ 47 (noting that *amici* supporting Bronzeville's position suggest that the Court's decision "stands to expose employers to potentially devastating class actions that can result in financial ruin").

[9] *See Watson*, 2021 IL App (1st) 210279 at ¶ 66 (denying two of White Castle's amici leave to file briefs addressing damages because the question was not before the Court).

[10] *See generally* Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae, *Cothron v. White Castle Sys., Inc.*, No. 20-3202 (7th Cir. Apr. 5, 2021); Br. of LeadingAge Illinois as Amicus Curiae, *Cothron v. White Castle Sys., Inc.*, No. 20-3202 (7th Cir. Apr. 5, 2021); Br. of Internet Ass'n as Amicus Curiae, *Cothron v. White Castle Sys., Inc.*, No. 20-3202 (7th Cir. Apr. 5, 2021).

49 ("It is not our role to inject a compromise, but, rather, to interpret the act as written.") (quoting *Folta v. Ferro Engineering,* 2015 IL 118070, ¶ 43). The parade of horribles conjured by White Castle and its *amici*—which every court has rejected in the last two years—are not only irrelevant when construing a plain and unambiguous statute, but none have come to pass, and none ever will. The intent of the General Assembly, which enacted the statute to address very concrete and serious threats to privacy and public policy reasons, reinforces the need to interpret the Act exactly as written.

A. A Statute's Plain Text is Not Invalidated Because of Hypothetical Absurdities

While White Castle and its *amici* stop short of saying *this* Court will violate the Constitution if it rules in Cothron's favor (or that the Appellate Court and district court already have), they theorize that reading the plain text must be rejected because *the trial court* will later rely upon the ruling to disregard the Constitution by awarding astronomical damages. White Castle calls this a "constitutional problem" the Court should discern from the plain text not by using a dictionary, but with a calculator. *See, e.g.*, Def's. Br. at 45 (forecasting damages against White Castle of $17.1 billion "or more", up from the $1 billion figure mentioned at the Seventh Circuit); Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 15 n.6 (claiming an "average" restaurant chain is subject to a $84-$420 billion judgment per month);[11] Br. of Ill. Chamber of Commerce et al. as Amici Curiae at 16 (claiming, without evidence, that an employer with 100 employees is "easily" subject to a $250 million judgment); Br. of Ill. Manufacturers' Ass'n et al. as Amici Curiae at 17

[11] In this theoretical world, a court awards "Allie," an employee of the restaurant, $10 million for every month of her employ. Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 15 n.5.

(claiming, without evidence, the same employer is actually subject to a $500 million judgment).[12] Presenting damage awards like these as an "inevitable" problem requiring a present solution, White Castle warns that a constitutionally indefensible judgment is both certain and imminent, Def.'s Br. at 39-40, 42-45, 48-48, and the only way to prevent its entry is to preemptively rule in White Castle's favor on the accrual issue.

According to White Castle, this is simply a routine application of "constitutional avoidance." Def.'s Br. at 42. However, constitutional avoidance, like other canons of statutory interpretation, "comes into play only when, after the application of ordinary textual analysis, the statute is found to be susceptible of more than one construction," which, as explained in Section I.A, *supra*, the Act is not. *See Nielsen v. Preap*, 139 S. Ct. 954, 972 (2019) (internal quotation omitted). What White Castle really proposes is an approach to statutory interpretation where the plain text is barely an afterthought, and the primary tool of construction is a crystal ball. This attack on a damages award no trial court has entered (or will ever enter) is exactly the kind of hypothetical absurdity not considered when interpreting the plain text. *See, e.g.*, *Petersen v. Wallach*, 198 Ill. 2d 439, 447 (2002) (the Court's duty is to construe the text without regard to "hypothetical absurdities"). Indeed, even the existence of "bad consequences" from a reading of a statute which, unlike

[12] If calculating damages this way seems well-rehearsed, that's because ***defendants*** *are the only parties who have ever asked a court to calculate damages on a "per scan" basis*. They concocted the theory to justify the $5,000,000 "amount in controversy" threshold required under the Class Action Fairness Act ("CAFA"), 28 U.S.C. §1332(d)(2), in order to remove cases from Illinois state courts, and are now projecting it onto a plaintiff's bar which has expressly disavowed it. *See, e.g.*, *Nosal v. Rich Prods. Corp.*, No. 1:20-cv-04972, D.E. 1, at ¶¶ 6, 13 (N.D. Ill. Aug. 24, 2020) (defendant introducing "per scan" theory of damages to justify the amount in controversy requirement and CAFA threshold on removal); *Coleman v. Greenwood Hospitality Management, LLC*, No. 1:21-cv-00806, D.E. 1, at ¶ 8 (N.D. Ill. Feb. 12, 2021) (same).

here, are not rooted in hypotheticals, is not a basis to disregard the plain text. *See, e.g.*, *id.* ("The possibility of an unjust or absurd result is generally not enough to avoid the application of a clearly worded statute."); *Jaskolski v. Daniels*, 427 F.3d 456, 461 (7th Cir. 2005) (the command to avoid absurd statutory readings is not license to ignore the plain text, or apply creative interpretation to improve statutes "so that their outcomes accord more closely with judicial beliefs about how matters ought to be resolved"). Any other approach is to effectively rewrite the statute, which exceeds the Court's role. *See McDonald*, 2022 IL 126511, ¶¶ 48-49.

Needless to state, a court cannot assess whether Cothron's damages are "excessive" until an actual controversy arises (*i.e.*, the question of damages is litigated, ascertained, and awarded). Because that will not happen, if at all, until the completion of discovery, motion practice, and a liability finding, the *Watson* appellate and *Cothron* trial courts correctly rejected White Castle's request to construe the statute through the lens of a hypothetical future. The courts rightly recognized that they could not accept White Castle's "one and done" accrual rule simply because applying the law as written might one day result in a damages award rather than the get out of jail free card White Castle seeks.[13] "We are cognizant of the substantial consequences the legislature intended as a result of Privacy Act violations." *McDonald*, 2022 IL 126511, ¶ 48.

[13] White Castle's claim that its best possible outcome is a $9,500,000 judgment even if its accrual theory is accepted is extraordinarily disingenuous. Def.'s Br. at 45. White Castle first started harvesting Cothron's biometrics in violation of the Act immediately after it went into law in 2008. Because the Act is subject to a maximum five-year limitations period, acceptance of White Castle's accrual theory means dismissal of Cothron's action with her recovering nothing.

B. Should the Need to Calculate Cothron's Damages Arise, the Trial Court Will Award, and (If Necessary) the Appellate Courts Will Review, Damages Within Constitutional Guidelines.

White Castle posits that unless the Court embraces its "one and done" accrual rule, then the way White Castle and its *amici* calculate damages—the way which results in billions in damages—is the trial court's *only* option. Def.'s Br. at 44. But when the need to calculate damages for Cothron ripens, any honest assessment of how the trial court will approach damages quickly exposes White Castle's feigned hysteria. First, as the Appellate Court observed (and one of White Castle's *amici* concedes, albeit buried in a single footnote),[14] "damages [under the Act] are discretionary not mandatory." *Watson*, 2021 IL App (1st) 210279, ¶ 66 n.4. Second, courts have consistently held that the Act is not a penal statute. *See, e.g.*, *Haywood v. Flex-N-Gate*, No. 2019-CH-12933, at 3 (Ill. Cir. Ct. Apr. 8, 2021) (SA004-SA009); *Burlinski v. Top Golf USA Inc.*, No. 19-cv-06700, 2020 WL 5253150, at *7 (N.D. Ill. Sept. 3, 2020). Third, even absent an express admonition against construing the Act as a penal statute, it is also fair to presume the trial court would read the well-established appellate guidance on how to award constitutionally-sound damages, including the decades of binding precedential decisions referenced by White Castle and its *amici*. *See, e.g.*, *Cent. Mut. Ins. Co. v. Tracy's Treasures, Inc.*, 2014 IL App (1st) 123339, ¶ 72 ("A trial court presiding over a class action—a creature of equity—would certainly possess the discretion to fashion a damage award that (1) fairly compensated claiming class members and (2) included an amount designed to deter future violations, without destroying defendant's business."); *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 953-54

[14] *See* Br. of Ill. Manufacturers' Ass'n et al. as Amici Curiae at 17 n.7.

(7th Cir. 2006); *Soprych v. T.D. Dairy Queen, Inc.*, No. 08 C 2694, 2009 WL 498535, at *1 (N.D. Ill. Feb. 26, 2009). In other words, the "guardrails" to the damages question already absolutely exist. Br. of Ill. Chamber of Commerce et al. as Amici Curiae at 18.

Finally, while an exhaustive analysis is premature, there are several methods by which a trial court, exercising the discretion expressly afforded by the Act, could calculate damages. For example, the trial court could decide to calculate damages on a per-aggrieved person basis, as under the Fair and Accurate Credit Transactions Act ("FACTA"). *See Stillmock v. Weis Markets, Inc.*, 385 F. App'x 267, 271-72 (4th Cir. 2010) (statutory damages under FACTA properly awarded on a per-consumer instead of "per-receipt" basis). Or the trial court could award damages on a per-biometric identifier basis (*i.e.*, fingerprint versus hand geometry scan), as is done under the Copyright Act. *Chicago Bldg. Design, P.C. v. Mongolian House, Inc.*, 770 F.3d 610, 618 (7th Cir. 2014) (observing that an award of statutory damages under 17 U.S.C. § 504(c)(1) is cumulative in nature, covering "all infringements involved in the action, with respect to any one work," even though a claim accrues on each discrete infringing act). Or the trial might decide to award damages on a per-provision basis, as suggested by one of White Castle's *amici* at the Seventh Circuit. *See* R155; Br. for Internet Ass'n as Amicus Curiae at 6, *Cothron v. White Castle Sys. Inc.*, No. 20-3202 (7th Cir. Apr. 5, 2021).

Under any of these already-established approaches, the relevant liability question is: Did White Castle fail to secure Cothron's informed consent before collecting [or disseminating] her fingerprints at any time during the statute of limitations period? If yes, the trial court has the discretion to award damages on a per-aggrieved person or per-identifier basis (for a maximum of $1,000 or $5,000 in liquidated damages) or on a per

provision basis (for a maximum of $2,000 or $10,000 in liquidated damages), or any other basis which is consistent with Cothron's allegations in her complaint, seeking damages for violations of precisely two provisions of the Act during the statutory period. (A025-A027 at ¶¶ 86-88, 96-97.)

Particularly because discovery has not yet commenced, the trial court never suggested, "euphemistically" or otherwise, that it already analyzed how to assess damages, let alone that it was determined to calculate them on a "per scan" basis or enter a multibillion-dollar award. All the court did was note, in *dicta*, that applying the text as written "may" lead to a "large" damages award, a result dictated not by any misreading of the statute, but solely by White Castle's conduct in repeatedly collecting and disclosing Cothron's biometrics year after year without bothering to obtain her informed consent. As recently stated by one court, "[s]omeone whose maximum penalty reaches the mesosphere only because the number of violations reaches the stratosphere can't complain about the consequences of its own extensive misconduct." *United States v. Dish Network, L.L.C.*, 954 F.3d 970, 980 (7th Cir. 2020). Indeed, depending on whether a culpable party's conduct was negligent or reckless, the Act provides for damages of $1,000 or $5,000 for each "violation" (which is undefined by the statute). 740 ILCS 14/20. In the privacy context, a statutory award of $5,000 is fairly described as "large." Thus, while liability accrued every time White Castle collected or disseminated Cothron's fingerprints before securing her informed consent, it does not follow that the trial court is under a mandate to stack damages for each occurrence.

Although White Castle and its fear-mongering *amici* assert that applying the plain text is tantamount to millions in individual damage awards, the reality is revealed by the

relatively "nominal" settlement results in the real world, including examples they cite. Br. of Ill. Chamber of Commerce et al. as Amici Curiae at 19. For example, proclaiming small businesses are facing "annihilative liability" in lawsuits brought under the Act, White Castle and its *amici* reference a case against Gurtler Chemicals, Inc., which settled for $69,000 ($1,000 per person), and one against Four Seasons Heating and Air Conditioning Inc., which settled for even less (tiered structure of $800, $525, $262 per person). *See* Pl.'s Mot. and Memo. of Law for Atty's Fees, Expenses, and Incentive Award, *Lopez-McNear v. Sup. Health Linens, LLC*, No. 19-cv-2390 (N.D. Ill. Mar. 23, 2021) (noting that *Kirby v. Gurtler Chems., Inc.*, No. 2019-CH-09395 (Cir. Ct. Cook Cty.), settled for $1,000 per class member for 69-member class); *Truss v. Four Seasons Heating & Air Conditioning, Inc.*, JND Legal Administration *available at* https://www.jndla.com/cases/class-action-administration (last visited Apr. 7, 2022). *Lark v. McDonald's USA, LLC* illustrates this point equally saliently, where the parties negotiated a recently-approved settlement, more than a year after the *Cothron* trial court decision, providing for a net recovery of $190 or $375 per person. Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 22; *see also* Def.'s Br. at 49 (noting a settlement in *Rosenbach* providing for a net recovery of $200 per person); Br. of Ill. Manufacturers' Ass'n et al. as Amici Curiae at 7 (stating the average gross payout, before reductions for fees and costs, is $877 per person). As White Castle and its *amici* must begrudgingly acknowledge, settlement values like these are the norm because they naturally result from a straightforward reading of the Act.

C. Unsubstantiated Threats of "Annihilative Liability" Do Not Relieve White Castle From Accountability for Its Conduct or Obligation to Comply with the Act.

Peeking behind the histrionics, one unassailable fact emerges: White Castle, along with some of the largest and most sophisticated corporations in the world, collected sensitive, valuable, and immutable biometrics from millions of Illinois citizens for many years without making any effort to comply with the law. These aren't mere "technical violations," no matter how many times they continue, in the face of *Rosenbach*, being characterized as such. *See, e.g.*, Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 3-4, 6, 16, 23-25; *Rosenbach*, 2019 IL 123186, ¶ 34 ("This is no mere 'technicality.' The injury is real and significant."). Desperate for a distraction, White Castle and its allies resort to fictionalized accounts of "destroyed businesses," rampant bankruptcies, mass unemployment, and worse they say are the result of adverse rulings against private entities illegally harvesting biometrics.[15] They argue that the Court should excuse their conduct not on legal grounds, but on their self-generated propaganda, while placing the blame for their failure to follow the law onto the district court, the Appellate Court, this Court, Cothron, and everyone else whose rights they violated. *See* Def.'s Br. at 47; Br. for Retail Litig. Ctr., Inc. et al. as Amici Curiae at 4, 6-7, 11-12, 25; Br. of Ill. Chamber of Commerce et al. as Amici Curiae at 20-25; Br. of Ill. Manufacturers' Ass'n et al. as Amici Curiae at 2, 13-18.

[15] It is reasonable to expect parties who make such eye-opening representations to this Court to back them up with facts. But the "facts" cited by White Castle do not come from authoritative works, reputable media outlets or other reliable sources, but from what are essentially op-ed pieces authored by themselves and other defense counsel for the benefit of current and prospective clients and industry groups. No evidence exists that the rulings in *Rosenbach*, *Watson*, *Cothron* trial court (or any other ruling) has resulted in a single bankruptcy, destroyed a business, caused a company to stop selling, innovating, or deploying biometric technology.

White Castle and its *amici* can't seem to decide whether there are too many lawsuits brought under the Act or not enough lawsuits and which court rulings are to blame for their conduct. All say too many were filed, foisting blame squarely on the *Rosenbach* court,[16] yet all simultaneously say the district court and *Watson* court rulings actually had the opposite effect, incentivizing potential claimants, *before filing suit*, to clock-in and out on their employer's timeclock as often as possible to maximize potential damages. Br. of Ill. Manufacturers' Ass'n et al. as Amici Curiae at 13; Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 19-22, 25; Br. of Ill. Chamber of Commerce et al. as Amici Curiae at 24. Indeed, one amicus goes so far as to claim the overwhelming majority of meritorious lawsuits have ***not*** been filed, and the only thing holding them back is the possibility this Court will embrace the "one and done" accrual theory. Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 22.

These assertions, made by associations representing employers of more than 3.7 million Illinois residents, are both offensive and chilling. *Id.* at 2; Br. of Ill. Manufacturers' Ass'n et al. as Amici Curiae at 3. These groups advise the Court that their members ***will break the law until one of their employees files suit***, the only thing which might "encourage compliance," but they are concerned that the employee will intentionally delay in order to rack up more damages. Br. of Ill. Manufacturers' Ass'n et al. as Amici Curiae at 13. Suffice it to say, employees are not responsible for policing their employer's conduct, and hourly-paid employees do not strategically clock-in and out for work every day, hoping and waiting for years of noncompliance before taking action. White Castle, which unlike

[16] One amicus openly blames "several court decisions." Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 4.

its employees, is deemed to have knowledge of the laws to which employers are subject, is solely responsible for its conduct and its consequences.

Equally outlandish is the claim that applying the text as written will bring research and deployment of biometric technology to a screeching halt, as companies will find any profits they can earn or efficiencies they can achieve outweighed by the "risks" of securing informed consent, which they claim is all-but-impossible. The specter of dangerous roads, home invasions, hazardous waste spills, and threats to child safety all loom large. Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 16; Br. of Ill. Chamber of Commerce et al. as Amici Curiae at 5, 25. To its credit, White Castle itself does not suggest it has any plans to pull the plug on its biometric technology, likely because it continues to use it today just like has for at least 18 years (only attempting to comply with the Act within the last four years).

And as White Castle correctly notes, the Act doesn't outlaw biometric technology. Def.'s Br. at 47. What it does is provide biometrics collectors with the "strongest possible incentive to conform to the law and prevent problems before they occur." *Rosenbach*, 2019 IL 123186 at ¶ 37. Yet White Castle (and other entities that are not exactly "small businesses" like McDonald's, ADP, Facebook, Amazon, and IBM), apparently decided those incentives were not compelling enough, and far from undertaking their "best efforts to comply," they, like White Castle, did *nothing*.

The reality is that after affording corporate and other lobbying groups—including White Castle's current and former *amici*—every opportunity to evaluate and provide feedback on the proposed legislation, the General Assembly passed the Act by unanimous vote "to allay the fears of and provide protections for 'thousands of' people who had

provided their biometrics for use as identifiers and who were now left 'wondering what will become of' this data." *Watson*, 2021 IL App (1st) 210279, ¶ 64 (quoting the 95th Ill. Gen. Assem., House Proceedings, May 30, 2008 at 249). The law was not passed in secret but unveiled to the public in the usual course. 95th Ill. Gen. Assembly, House Proceedings, May 30, 2008, at 249-50. As noted by one *amici*, legislators considered whether the Act needed any modification in 2021, and the General Assembly concluded it should remain intact exactly as enacted. *See* Br. of Retail Litig. Ctr., Inc. et al. as Amici Curiae at 7 n.3.

The Act's requirements are straightforward, easy-to-follow, and can be effectuated at nominal cost, as shown by the countless entities which have done exactly that. *Rosenbach*, 2019 IL 123186, ¶ 37. "Compliance should not be difficult; 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; and the public welfare, security, and safety will be advanced." *Id.* But for over ten years, White Castle could not be bothered. It has no excuse and no one other than itself to blame.

Moreover, nothing about the accrual question affects the ease with which an entity can comply with the Act. In the employment setting, where the employer has direct access and control over the employee, employers can quickly, easily, and efficiently provide notice and secure informed consent with their onboarding documents (or with the subsequent rollout of new policies). *See e.g., Cothron I*, 477 F. Supp. 3d at 733 (explaining, "[t]o comply with Section 15(b), White Castle could have provided Ms. Cothron with a release informing her of 'the specific purpose and length of term' for which he information was being used and requiring her consent to all future scans consistent with those uses as

a condition of employment," and "as with Section 15(b), it is consistent with the statutory language to obtain consent for multiple future disclosures through a single written release."). Or they can simply place a notification on the enrollment device itself and require employees to indicate consent by clicking a button. Requirements like these hardly mean biometric devices are effectively outlawed, or that these results could not have been intended by the General Assembly. Quite the contrary, a requirement to get employees to sign a form before extracting their biometrics furthers the statute's goal of encouraging the responsible use of biometric technology and prevent irreversible harms before they occur while imposing no burden whatsoever.

CONCLUSION

For all the reasons stated above, the Court should answer certified question by holding that Section 15(b) and 15(d) claims accrue under the Act each time a private entity collects a person's biometrics and each time a private entity discloses their biometrics to a third party.

Respectfully submitted,

/s/ James B. Zouras

Ryan F. Stephan
James B. Zouras
Andrew C. Ficzko
Teresa M. Becvar
STEPHAN ZOURAS, LLP
100 North Riverside Plaza, Suite 2150
Chicago, Illinois 60606
(312) 233-1550
rstephan@stephanzouras.com
jzouras@stephanzouras.com
aficzko@stephanzouras.com
tbecvar@stephanzouras.com

Counsel for Appellee Latrina Cothron, individually and on behalf of others similarly situated

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 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), contains 41 pages.

/s/ James B. Zouras
James B. Zouras

SUPPLEMENTAL APPENDIX

SUPPLEMENTAL APPENDIX TABLE OF CONTENTS

SUPREME COURT OF ILLINOIS

SUPREME COURT BUILDING
200 East Capitol Avenue
SPRINGFIELD, ILLINOIS 62701-1721

CYNTHIA A. GRANT
Clerk of the Court

(217) 782-2035
TDD: (217) 524-8132

December 23, 2021

FIRST DISTRICT OFFICE
160 North LaSalle Street, 20th Floor
Chicago, IL 60601-3103
(312) 793-1332
TDD: (312) 793-6185

Hon. Christopher G. Conway
Clerk of the United Stated Court of Appeals
for the Seventh Circuit
219 South Dearborn Street, Room 2722
Chicago, Illinois 60604

In re: Cothron v. White Castle System, Inc.
128004

Dear Mr. Conway:

Enclosed is a certified order entered December 23, 2021, by the Illinois Supreme Court in the above-captioned cause.

Very truly yours,

Cynthia A. Grant

Clerk of the Supreme Court

cc: Andrew Christopher Ficzko
Erin Bolan Hines
James B. Zouras
Melissa A. Siebert
Ryan Francis Stephan
Teresa Marie Becvar
William F. Northrip

State of Illinois
Supreme Court

I, Cynthia A. Grant, Clerk of the Supreme Court of the State of Illinois, and keeper of the records, files and Seal thereof do hereby certify the following to be a true copy of an order entered December 23, 2021, in a certain cause entitled:

128004

Latrina Cothron,
behalf of all others similarly situated,

Plaintiff-Appellee

v.

White Castle System, Inc.,

Defendant-Appellant

Filed in this office on the 20th day of December A.D. 2021.

IN TESTIMONY WHEREOF, I have set my hand and affixed the seal of said Supreme Court, in Springfield, in said State, this 23rd

Cynthia A. Grant

Clerk,
Supreme Court of the State of Illinois

128004

IN THE

SUPREME COURT OF ILLINOIS

Latrina Cothron, individually and on behalf of all others similarly situated,	)	
Plaintiff-Appellee	)	Certif. 7th Cir.
v.	)	Federal Court, Seventh Circuit
White Castle System, Inc.,	)	20-3202
Defendant-Appellant	)	

O R D E R

Pursuant to Supreme Court Rule 20, this Court will answer the question of law certified to this Court by the United States Court of Appeals for the Seventh Circuit in Cothron v. White Castle System, Inc., No. 20-3202. The brief of the appellant is due January 27, 2022. Remaining briefs shall be filed according to Supreme Court Rule 343.

Order Entered by the Court.

FILED
December 23, 2021
SUPREME COURT
CLERK

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

SEYON R. HAYWOOD and ROBERT STEWART, individually and on behalf of all others similarly situated, *Plaintiffs*,	Case No. 19 CH 12933
v.	Judge Celia Gamrath
FLEX-N-GATE LLC; FLEX-N-GATE PLASTICS, LLC; FLEX-N-GATE CHICAGO, LLC, *Defendants*.	Calendar 6

ORDER DENYING DEFENDANTS' 2-619 MOTION TO DISMISS

This matter came to be heard on Defendants' Flex-N-Gate LLC, Flex-N-Gate Plastics, LLC, and Flex-N-Gate Chicago, LLC (collectively "Flex-N-Gate") 2-619 Motion to Dismiss Plaintiffs' Seyon R. Haywood and Robert Stewart (collectively "Haywood") Amended Class Action Complaint. For the following reasons, Flex-N-Gate's 2-619 Motion to Dismiss based on Illinois and United States constitutional violations is denied. Flex-N-Gate's 2-619 Motion to Dismiss based on the Illinois Workers' Compensation Act is continued generally pending the Illinois Supreme Court's decision in *McDonald v. Symphony Bronzeville Park LLC*.

BACKGROUND

Plaintiffs' Amended Class Action Complaint against Flex-N-Gate arises out of the Biometric Privacy Act ("BIPA"). Flex-N-Gate is an auto parts manufacturer and supplier of components for the automotive industry. Plaintiffs are, with several exceptions, all residents of the State of Illinois who had their fingerprints collected, captured, received, otherwise obtained, or disclosed by Flex-N-Gate while residing in Illinois.

When employees begin their jobs at Flex-N-Gate, they are required to scan their fingerprint in its biometric time tracking system as a means of authentication. As this involves the use of biometric data, BIPA must be contemplated. Plaintiffs allege Flex-N-Gate has violated BIPA because it has not:

1. Properly informed Plaintiffs in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, and used, as required by BIPA;
2. Provided a publicly available retention schedule and guidelines for permanently destroying Plaintiffs' fingerprints, as required by BIPA; nor
3. Received a written release from Plaintiffs to collect, capture, or otherwise obtain fingerprints, as required by BIPA.

Plaintiffs allege they have "continuously and repeatedly" been exposed to the risks created by Flex-N-Gate's violations of BIPA. Plaintiffs seek liquidated damages for each violation under BIPA.

Flex-N-Gate has brought this 2-619 Motion to Dismiss on two constitutional grounds. First, Defendants claim BIPA is unconstitutional under the Illinois Constitution because it arbitrarily discriminates against similarly situated employers and employees. Second, they claim BIPA is unconstitutional under the United States Constitution because it establishes grossly excessive civil damages out of proportion to the alleged offensive conduct. For the following reasons, the court rejects both propositions.

LEGAL STANDARD

A motion to dismiss pursuant to 735 ILCS 5/2-619 raises affirmative defenses. *Urbaitis v. Commonwealth Edison*, 143 Ill. 2d 458 (1991). It provides for "involuntary dismissal based on certain defects or defenses," which include, among others, where "the claim asserted against defendant is barred by other affirmative matter avoiding the legal effect of or defeating the claim." 735 ILCS 5/2-619(a)(9). When considering a motion under 2-619, the pleadings must be construed in the light most favorable to the nonmoving party and the court must view the facts alleged in the complaint as true.

ANALYSIS

a. Section 2-619 Motion to Dismiss as an Excessive Fine

Defendants contend BIPA's liquidated damages clause is so fundamentally excessive that it violates the Eighth Amendment of the United States Constitution. According to Defendants, a statute violates the Eighth Amendment when it imposes a penalty or fine "so severe and oppressive as to be wholly disproportionate to the offense and obviously unreasonable." *St. Louis, I.M & S.R. Co. v. Williams*, 251 U.S. 63, 66-67 (1919). However, BIPA's liquidated damages clause is neither a fine nor a penalty per se.

Courts have understood the word "fine" to mean "a payment to a sovereign as punishment for some offense." *Browning-Ferris Indus. v. Kelco Disposal*, 492 U.S. 257, 265 (1989). Liquidated damages paid to an aggrieved private party are not a fine. Generally, they do not serve as punishment. Rather, they serve to compensate an aggrieved party where actual damages are difficult to ascertain or prove. They may also serve to incentivize private parties to enforce BIPA and encourage private businesses to comply. But regardless, they clearly serve more than a punitive purpose and are not the same as a fine or penalty paid to the government.

Defendants point to no case that has categorized a statutory liquidated damages clause as a fine, forfeiture, or penalty. Nor do they point to any case that has analyzed a liquidated damages provision under the Eighth Amendment. To the Court's knowledge, all challenges to similar statutory schemes have been under the 14th Amendment Due Process Clause and analyzed under the rational basis test, not strict scrutiny. Even *Williams*, upon which Defendants rely, analyzed the penalty under the 14th Amendment Due Process Clause, not the Eighth Amendment Excessive Fines Clause. Moreover, the penalty at issue in *Williams* was an unequivocal penal penalty

designed to punish the wrongdoer. It bore no relation to damages, either actual or liquidated, that the aggrieved party suffered.

Defendants go on to argue that the legislature has identified no public interest in subjecting an Illinois company to BIPA's "ruinous" damages, even though there is no evidence the damages indeed would be ruinous to Defendants. Defendants also argue there is no uniform adherence required as nearly all private financial institutions and government contractors are exempted. Further, Defendants argue that BIPA allows for a windfall disproportionate to any injury Plaintiffs might have suffered as Plaintiffs need not prove actual injury to recover. Accordingly, Defendants believe the liquidated damages are so penal and grossly disproportionate relative to the gravity of the offense as to be unconstitutional as a matter of law.

However, as Plaintiffs point out, the purpose of BIPA is remedial, not penal. It was enacted for a legitimate purpose to protect rights and impose regulations for the public good. In *Burlinski*, the court clearly stated that BIPA is not penal, but rather remedial in considering the question of whether BIPA could be considered penal for purposes of the two-year statute of limitations. *Burlinski v. Top Golf USA, Inc.*, 2020 U.S. Dist. LEXIS 161371 at *21. The goal of BIPA is not to penalize, but rather set up a regulatory framework to protect biometric privacy. *Id*.

Additionally, in *Rosenbach*, the Illinois Supreme Court strongly suggested BIPA has a remedial purpose. The Supreme Court held that violations of BIPA are not mere technicalities; there is a real and significant injury to those aggrieved. *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 ¶ 34. The Supreme Court further stated the legislature intended the liquidated damage provisions in BIPA to have substantial force. *Id.* at ¶ 37. It would be the opposite of BIPA's purpose to require plaintiffs to wait until they have some compensable injury before they could bring a claim as their biometric data would be compromised at that point. *Id*.

BIPA bears a resemblance to the Telephone Consumer Protection Act ("TCPA") and other statutes that impose liquidated damages for a violation. In *Lay*, for instance, the Illinois Supreme Court found the $500 per violation liquidated damages provision of TCPA as remedial, not penal. *Standard Mutual Insurance Co. v. Lay*, 2013 IL 114617 ¶ 33. The Supreme Court found TCPA to both protect rights and incentivize private parties to enforce the statute. *Id*. at ¶ 32. This court finds TCPA comparable to BIPA's remedial scheme, which promotes the enforcement of the statute and protects private parties rights without requiring them to wait until they are actually harmed by the possible release of their biometric information. *See Rosenbach*, 2019 IL 123186 ¶¶ 34, 37.

All told, the court is unwilling at the pleadings stage to find as a matter of law that BIPA imposes an excessive fine that violates the Excessive Fines Clause of the Eighth Amendment of the United States Constitution. First, the court questions whether this is even the correct analysis since it does not believe the BIPA liquidated damages provision amounts to a fine, forfeiture, or penalty. Despite the number of times Defendants call the liquidated damages provision a "fine," it simply is not. Second, even if it could be characterized as a fine, the determination of whether a fine is excessive is a fact intensive inquiry that cannot be decided in a vacuum on this 2-619 Motion to Dismiss.

Notably, BIPA provides for recovery of the greater of actual or liquidated damages. The liquidated damages provision was enacted to ensure a simple way of computing damages in response to identity theft crises inherent with biometric data. Although the amount of liquidated damages may seem harsh, it is not so when considered with regard to the privacy interests of the public at stake. Such damages were designed not to punish, but rather, to compensate aggrieved parties and incentivize businesses to conform to the law and prevent problems before they occur. *See Id*. Accordingly, and due to the factual nature of this question and dubious contention that BIPA's liquidated damages provision amounts to a fine, the court rejects Defendants' assertion that it is violative of the Excessive Fines Clause as a matter of law. The court denies the 2-619 Motion to Dismiss on this basis.

b. Section 2-619 Motion to Dismiss as Special Legislation

Defendants also seek dismissal on the basis BIPA violates the Special Legislation Clause as creating arbitrary classifications by exempting financial institutions and government contractors. The Special Legislation Clause of the Illinois Constitution states:

> "The General Assembly shall pass no special or local law when a general law is or can be made applicable. Whether a general law is or can be made applicable shall be a matter for judicial determination." Ill. Const. art. IV, § 13.

The purpose of the Special Legislation Clause is to prevent arbitrary legislative classifications that discriminate in favor of select groups without a reasonable basis. *Best v. Taylor Mach. Works*, 179 Ill. 2d 367, 391 (1997). Plaintiffs' response brief sets forth a myriad of reasonable bases as to why the legislature distinguished between certain business entities in BIPA. This suffices to defeat Defendants' constitutional challenge to the legislative classifications in BIPA.

In their reply, Defendants argue that a strict scrutiny analysis should apply to this question as opposed to the rational basis test. However, the case law they cite does not support this. Moreover, the court is far from convinced that a fundamental right is at issue here. When a fundamental right, suspect class, or quasi-suspect classification is not involved, the rational basis test, not strict scrutiny, shall apply.

Defendants' reliance on *Timbs* and *Williams* is misplaced, for BIPA's liquidated damages provision does not remotely resemble the penal forfeiture and penalties at issue in those cases. In *Timbs,* the fine at issue was a forfeiture to the state of a vehicle used to transport heroin and commit a crime. *Timbs v. Indiana,* 139 S. Ct. 682, 686-87 (2019). There is no question the forfeiture amounted to a fine or penalty subject to the Excessive Fines Clause. In contrast, BIPA's liquidated damages award is paid to private aggrieved parties, not the government. It is not a per se penalty or fine within the meaning of the Eighth Amendment.

In *Williams*, 251 U.S. 63, although the penalty was paid to a private aggrieved party, it was a penal penalty designed to punish the wrongdoer and, thus, implicated due process concerns under the 14th Amendment. In contrast, as discussed above and at oral argument, the court seriously doubts Defendants' characterization of BIPA's liquidated damages as a penal penalty that would

give rise to a strict scrutiny analysis. The court's opinion is bolstered by the recent California decision of *Amy v. Curtis*, 2021 U.S. Dist. LEXIS 43092 (N.D. Cal. 2021), where the court rejected an Eighth Amendment constitutional challenge to liquidated damages paid to private individuals, noting that it was damages paid to private parties and not a fine paid to the government to which the Excessive Fines Clause applied.

Moreover, courts have already rejected the special legislation challenge against BIPA using the rational basis test. For example, in *Bryant*, the Court considered the special legislation challenge on a motion to dismiss. The court found that the exclusion of certain entities from BIPA's coverage is eminently rational. *Bryant v. Compass Group USA, Inc.*, 2020 U.S. Dist. LEXIS 222219 at *8. The court found the exclusion of financial institutions was likely due to the fact they are already subject to a comprehensive privacy protection regime under the Gramm-Leach Bliley Act. *Id.* at *9. Further, the court found the exclusion of governmental agencies and contractors rational for a number of reasons. First, governmental agencies are generally entitled to sovereign immunity. *Id*. at *8. The court also found that governmental agencies have no profit motive to exploit individuals' biometric information, so the perceived dangers are less severe with regards to governmental agencies and government contractors that are subject to their supervision. *Id*. at *8-9. The court ultimately ruled that both financial institutions and government contractors already had privacy safeguards in place, so imposing additional obligations to them under BIPA would have had minimal effect. *Id.* at *9.

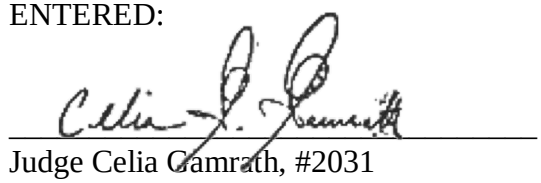
Additionally, on a motion to dismiss in *Bruhn v. New Albertson's Inc.*, Cook County Circuit Court Judge Loftus provided similar reasoning to *Bryant* in upholding BIPA under the rational basis test. In that case, defendant's Application for Leave to Appeal was denied by the First District Appellate Court on the grounds "the question of law at issue does not present a question of law as to which there is a substantial ground for difference of opinion." The court sees no reason to depart from these well-reasoned decisions or take the extraordinary measure to dismiss Plaintiffs' Amended Class Action Complaint under Defendants' novel strict scrutiny Eighth Amendment analysis.

IT IS ORDERED:

1. Defendants' 2-619 Motion to Dismiss as a violation of the Excessive Fines Clause of the Eighth Amendment of the United States Constitution is denied.
2. Defendants' 2-619 Motion to Dismiss with respect to their Special Legislation challenge as a violation of the Illinois Constitution is denied.
3. Defendants' 2-619 Motion to Dismiss arguing Plaintiffs' BIPA claims are barred by the Exclusivity Provision of the Illinois Workers' Compensation Act is continued pending the Illinois Supreme Court's decision in *McDonald v. Symphony Bronzeville Park LLC*. Defendants' time to answer the Amended Class Action Complaint is held in abeyance until such time as the Court rules.
4. This matter is set for status on the *McDonald* decision to August 23, 2021, at 9:00 AM.

Judge Celia G. Gamrath
APR 08 2021
Circuit Court - 2031

ENTERED:



Judge Celia Gamrath, #2031
Circuit Court of Cook County, Illinois
County Department, Chancery Division

NOTICE OF FILING and PROOF OF SERVICE

In the Supreme Court of Illinois

LATRINA COTHRON, individually and on behalf of all others similarly situated, *Plaintiff-Appellee,* v. WHITE CASTLE SYSTEM, INC., *Defendant-Appellant.*	)	No. 128004

The undersigned, being first duly sworn, deposes and states that on April 7, 2022, there was electronically filed and served upon the Clerk of the above court the Brief and Supplemental Appendix to of Plaintiff-Appellee. On April 7, 2022, service of the Brief will be accomplished by email to the following counsel of record:

Melissa A. Siebert
William F. Northrip
Matthew C. Wolfe
SHOOK, HARDY & BACON L.L.P.
masiebert@shb.com
wnorthrip@shb.com
mwolfe@shb.com

Within five days of acceptance by the Court, the undersigned states that thirteen copies of the Brief bearing the court's file-stamp will be sent to the above court.

/s/ James B. Zouras
James B. Zouras

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

/s/ James B. Zouras
James B. Zouras