No. 128004

IN THE SUPREME COURT OF ILLINOIS

LATRINA COTHRON, *Plaintiff-Appellee*,

v.

WHITE CASTLE SYSTEM, INC., *Defendant-Appellant*.

Question of Law Certified by the United States District Court of Appeals
for the Seventh Circuit, Case No. 20-3202

Question of Law ACCEPTED on December 23, 2021 under Supreme Court Rule 20

On appeal from the United States District Court for the Northern District of Illinois under
28 U.S.C. § 1292(b), Case No. 19 CV 00382
The Honorable Judge John J. Tharp, Judge Presiding

REPLY BRIEF OF DEFENDANT-APPELLANT WHITE CASTLE SYSTEM, INC.

ORAL ARGUMENT SET FOR MAY 17, 2022

Melissa A. Siebert
William F. Northrip
Matthew C. Wolfe
SHOOK, HARDY & BACON L.L.P.
111 South Wacker Drive, Suite 4700
Chicago, Illinois 60606
Tel: (312) 704 7700
masiebert@shb.com
wnorthrip@shb.com
mwolfe@shb.com

Counsel for Defendant-Appellant
White Castle System, Inc.

POINTS AND AUTHORITIES

Page(s)

INTRODUCTION

In Illinois, a claim accrues when a defendant invades a plaintiff's interest and inflicts injury. *Feltmeier v. Feltmeier*, 207 Ill. 2d 263, 279 (2003). This case asks the Court to determine when Privacy Act claims accrue, which necessarily involves determining the nature of the interest the Privacy Act protects from invasion, and when an invasion of that interest causes injury. The Court's precedent, the Privacy Act's text, and well-established canons of statutory interpretation provide the answer.

Prior Court decisions have interpreted the Privacy Act's text, explaining that it protects a privacy or secrecy interest in one's biometric data. *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 33; *West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978, ¶ 46. The unauthorized loss of data privacy or secrecy—the relinquishment of control over the data—inflicts a "personal and societal" and "real and significant" injury, which occurs at the "precise" point that the individual's privacy "vanishes." *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶ 43; *Rosenbach*, 2019 IL 123186, ¶ 34; *see West Bend*, 2021 IL 125978, ¶ 46. Applying the Court's prior decisions interpreting the Privacy Act, Court precedent of claim accrual, and canons of statutory interpretation yields one conclusion: a Privacy Act claim accrues the first time that biometric data is collected or disclosed.

Plaintiff argues the text of the Privacy Act is clear, and that the Court, with dictionaries in hand, can simply follow the federal district court's

decision. Had the Seventh Circuit found the Privacy Act's text so clear, the certified question would not be before the Court for it to answer anew, using all of the tools at its disposal. After all, the Court's role is to construe Illinois statutes in a manner consistent with legislative intent, which includes reference to the Court's precedent and the use of canons of statutory construction that favor consistency, rationality, and constitutionality. *See Int'l Ass'n of Fire Fighters, Local 50 v. City of Peoria*, 2022 IL 127040, ¶ 19 ("Fundamentally, this court is always concerned with discerning legislative intent.").

Single-claim accrual is not "atextual," as Plaintiff contends. Rather, single-claim accrual is the only outcome consistent with the Privacy Act's text, this Court's precedent interpreting the text, and the Act's intended purpose. This is a statute with the term "privacy" in its title, which is intended to protect data privacy rights. The injury is thus a privacy right invasion; it is not an injury caused by the mechanism (notice and consent) designed to prevent the injury. Indeed, *Rosenbach* firmly rejected any such reading of the Privacy Act.

Singular accrual does not render the Privacy Act a "one and done" privacy protection regime. White Castle and all Illinois employers remain subject to *all* of the Privacy Act's provisions. This includes the requirement that White Castle obtain consent under Section 15(b) for all newly hired employees at its Illinois restaurants; its obligation to all of its Illinois

employees (including Plaintiff under Section 15(d)) not to disclose data to additional entities without consent; and all other provisions of Section 15. If it fails to meet any of its ongoing Privacy Act obligations, White Castle faces significant, potential liability under the Privacy Act with respect to its entire Illinois workforce.

Nor is White Castle's position an attempt to avoid Privacy Act compliance. White Castle is not a Privacy Act villain, but it has been inaccurately miscast in that role by Plaintiff. *Since 2004*, when it first began using biometric technology in Illinois, White Castle has obtained employee consent (including Plaintiff's) prior to collecting any purported biometric information. (A005). White Castle also continuously has permitted its employees (including Plaintiff) to opt-out of providing their data, even though the Privacy Act does not so require. (A005-06); *see also* 740 ILCS 14/10 (release can be a condition of employment).

Plaintiff spends considerable time telling the Court not to concern itself with how its opinion here will be applied by Illinois courts. Ignoring the impact of its decisions is something this Court simply does not do. As the Court recently noted, it "consider[s] the reason for the law, the problems sought to be remedied, the purposes to be achieved, and the *consequences of construing the statute one way or another." McDonald*, 2022 IL 126511, ¶ 18.[1] This is critical—"after this court has construed a statute, that construction

[1] Emphasis added unless otherwise noted.

becomes, in effect, a part of the statute" and can only be changed by legislative amendment. *Int'l Ass'n of Fire Fighters*, 2022 IL 127040, ¶ 17 (citation omitted). The decision now before the Court implicates fundamental Illinois accrual principles, upon which only this Court can provide "authoritative guidance." *Cothron II*, 20 F.4th 1156, 1166 n.2 (7th Cir. 2021) (A078).[2] Put simply, the Court's precedent has the "force of law" and must be clear so lower courts may follow. *Int'l Ass'n of Fire Fighters*, 2022 IL 127040, ¶ 19.

White Castle respectfully requests that the Court answer this important certified question by finding that Section 15(b) and Section 15(d) claims accrue once, upon the first collection (scan) or disclosure (transmission) of biometric data.

ARGUMENT

I. A Privacy Act claim under Section 15(b) and (d) accrues once.

A. Under the Court's precedent, Privacy Act injuries occur once under Sections 15(b) and (d), and thus claims accrue once.

Almost two decades ago in *Feltmeier*, 207 Ill. 2d at 279, the Court set forth basic principles of claim accrual. Where there is a "single overt act" from which subsequent damages may flow, a claim accrues "on the date the defendant invaded the plaintiff's interest and inflicted injury." *Id.*

[2] White Castle uses the same short terms here as in its opening brief.

Yet Plaintiff deems *Feltmeier* "inapposite," without citing case law to support a different claim accrual method. Pl. Br. at 21. She premises her misdirected argument on the "discovery rule," rejected as inapplicable in *Feltmeier*, regarding when a party reasonably should know they have been injured and have a claim. *See Feltmeier*, 207 Ill. 2d at 284-85. Like *Feltmeier*, this appeal does not involve the discovery rule; it involves *Feltmeier*'s holding that a claim accrues based on a "single overt act," when an interest is invaded, and an injury occurs. *Id.* at 279. The claim accrues once, even if the effects of the injury may be ongoing. *Id*.

This Court has consistently and repeatedly defined the nature of a Privacy Act injury in alignment with *Feltmeier*'s single-claim accrual analysis. *Rosenbach* articulates that the Privacy Act "codified" a "right to privacy in and control over" one's biometric data. *Rosenbach*, 2019 IL 123186, ¶ 33. Biometric privacy rights are invaded when control of the data is lost non-consensually, at which point the "right of the individual to maintain his or her biometric privacy *vanishes into thin air*." *Id.* ¶ 34. At this point, the "precise harm the Illinois legislature sought to prevent is then realized." *Id.*; *see also McDonald*, 2022 IL 126511, ¶ 24. Under *Rosenbach*, a Privacy Act injury occurs when the right to privacy in and control over biometric data is lost.

West Bend confirms this conclusion, holding that the Act "protects a *secrecy interest*—here, the right of an individual to keep his or her personal

identifying information like fingerprints secret." *West Bend*, 2021 IL 125978, ¶ 46. Once biometric information is obtained or disclosed, an individual's "right to keep certain information confidential" is violated, and the data's "secrecy" is lost. *Id.* ¶ 45.

The Court's opinions thus lead to one conclusion—a Privacy Act injury occurs the first time the data is either non-consensually collected or disclosed. At that point, the individual has lost control of their data, and it is no longer secret or private. *Rosenbach*, 2019 IL 123186, ¶ 34.

The injury defined in *Rosenbach* is a "precise harm" which cannot be undone. *See McDonald*, 2022 IL 126511, ¶ 43 (describing a singular "lost opportunity to say no" to collection of biometrics). One cannot be reinjured by subsequent use or disclosure of the same biometric data between the same parties for the same purpose. Once White Castle allegedly obtained Plaintiff's first scan, no secret remained. And, once White Castle allegedly disclosed her first scan to purported third-party vendors, they also knew the secret. It was then, under *Rosenbach*, that any arguable injury occurred and claim accrued. Plaintiff's right to privacy in and control over her biometric data, which was codified in 2008, "vanished into thin air" 14 years ago, following her first, post-Act scan and White Castle's first purported automatic disclosure to its third-party vendors.

B. Plaintiff cannot avoid single-claim accrual by mischaracterizing the nature of Privacy Act injuries.

Plaintiff contends Privacy Act injuries have nothing to do with a loss of control over or privacy in one's biometric data. Pl. Br. at 20-21. Her position cannot be squared with *Rosenbach*'s holding that the Privacy Act "codifie[s] that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 2019 IL 123186, ¶ 33. It is, as *Rosenbach* stated, "the right of the individual to maintain [his or] her biometric privacy" that "vanishes into thin air," and the injury flows therefrom. *Id.* ¶ 34.

Contrary to *Rosenbach*'s clear language, Plaintiff deems the fact that the injury results from loss of privacy and control a "faulty" or "false" argument. Pl. Br. at 18, 20. She insists Privacy Act injuries are "informational" and arise from the failure to provide the correct "mechanism" of notice and consent. *Id.* at 21. *Rosenbach* forecloses this argument. The *Rosenbach* defendants did not contest that they had collected the plaintiff's biometrics "without first following the statutorily prescribed protocol." *Rosenbach*, 2019 IL 123186, ¶ 22. They argued, however, that their violation of the Act (the failure to provide notice and obtain consent) was non-substantive and purely procedural, not resulting in actual harm. *Id.*

The Court firmly rejected the "procedural" argument, noting that "such a characterization . . . misapprehends the nature of the harm our legislature is attempting to combat through this legislation." *Id.* ¶ 34; *see also Bryant v.*

Compass Group USA, Inc., 958 F.3d 617, 624 (7th Cir. 2020) (Because plaintiff asserted a "violation of her own rights" in "her private information," her injury "was no bare procedural violation."). Although *Rosenbach* set a low pleading bar to bring a Privacy Act claim, it also clarified that a "real and significant injury" occurs, the nature of which is the key to the claim-accrual question before the Court. *See Rosenbach*, 2019 IL 123186, ¶ 34. The "precise harm" is the loss of the right to privacy in and control over biometric data. *Id.*

Plaintiff's insistence that her purported injury flows solely from the Privacy Act's technical notice and consent procedures literally elevates forms over substance. It is not possible to read *Rosenbach* as creating a right, over and over, to receive forms containing "magic words" and to be injured repeatedly by the absence of such "magic words." The Privacy Act's procedural duties merely serve to "define the contours" of the privacy right, but they are not the right itself. *Id.* ¶ 33. It is the loss of the right to retain control over and privacy in one's biometric data that results in the "precise harm the Illinois legislature sought to prevent," and which is a "real and significant" injury. *Id.* ¶ 34; *see also West Bend*, 2021 IL 125978, ¶¶ 45-46; *McDonald*, 2022 IL 126511, ¶ 43 (Privacy Act injuries are "personal and societal"); *Bryant*, 958 F.3d at 626 (injury is "substantive and personal"). The loss-of-control injury is "real and significant" because loss of privacy and secrecy in biometric information also happens once and has unalterable consequences. The data (as between the same parties) can never be private or

secret again—the privacy right has vanished forever. *Rosenbach*, 2019 IL 123186, ¶¶ 33-34.

In effect, Plaintiff is asking the Court to ignore *Rosenbach* because it suits her position in this case. Moreover, applying Plaintiff's "informational injury" claim accrual theory leads to the same outcome—her Section 15(b) claim still accrues only once. Without the information, she gave up her privacy and secrecy interest in the data, lost control of it, and her claim accrued. *See Rosenbach*, *supra*. The Court should follow its previous decisions in *Rosenbach*, *McDonald*, and *West Bend* by holding that the initial loss of privacy and control is the only injury. There is no subsequent injury contemplated by the Privacy Act.

C. Single-claim accrual applies to analogous privacy-based claims.

Because a loss of privacy or control cannot be undone, single accrual principles that apply to traditional privacy actions likewise apply to Privacy Act claims. In *Bank of Ravenswood*, which Plaintiff does not address but White Castle discusses at length in its opening brief, the City of Chicago constructed a subway tunnel in 1988, but the subway did not begin to run until 1993. *Bank of Ravenswood v. City of Chicago*, 307 Ill. App. 3d 161, 168 (1st Dist. 1999). Despite this, the "single overt act" resulting in the plaintiff's privacy injury was the construction of the tunnel. *Id.* The claim did not accrue anew each day the tunnel continued to exist or each time the train ran beneath plaintiff's property. *Id*. The claim accrued when the tunnel was built,

and the plaintiff's right to privacy was initially lost. *Id*. The same principles apply here. Plaintiff's claim also accrued at the point when she lost privacy and control of her biometric data.

In the context of privacy claims premised on transmission of private information to a third party, the injury occurs, and the claim accrues, when private information is disclosed to a specific group or audience. Repeated disclosure of the same private data to the same group or audience does not result in additional injury—the injury occurs when the information is first disclosed, and is no longer a secret from that group. *See Ciolino v. Simon*, 2021 IL 126024, ¶ 38. The rule serves an important policy objective in our increasingly digital world: prevention of an endless limitations period. *Pippen v. NBCUniversal Media, LLC*, 734 F.3d 610, 616 (7th Cir. 2013).[3] The Privacy Act's purpose of preventing problems before they occur (*see Rosenbach*, 2019 IL 123186, ¶ 37) cannot be served by an endless tolling of the statute of limitations.

Respectfully, Plaintiff's contention that Privacy Act claims are singularly important does not justify ignoring claim accrual rules. A stale claim is untimely, no matter how important the right at issue may be. Were it otherwise, a host of claims would not have any limitations period at all. Claim accrual and resulting statutes of limitations apply equally to Privacy Act defendants and defendants facing similar privacy claims.

---

[3] *See* White Castle Br. at 37 (collecting cases).

II. The plain text of the Privacy Act statute supports a single-accrual rule.

Of course, in addition to its precedent interpreting the Privacy Act, the Court must consider the text of the Act itself. Plaintiff suggests the Court cannot consider legislative intent absent ambiguity. Pl. Br. at 14-15. However, it is a "basic principle[] of statutory construction" that "[w]hen construing a statute, [the Court's] primary objective is to ascertain and give effect to the legislature's intent." *Rosenbach*, 2019 IL 123186, ¶ 24. Whatever statute needs interpretation, the Court looks "to canons of statutory construction to glean [the legislature's] intent." *Int'l Ass'n of Fire Fighters*, 2022 IL 127040, ¶ 19.

As the Court recognizes repeatedly, Illinois courts interpret statutory language by looking to the text itself and determining the plain and ordinary meaning of the statute's words, as well as by considering "the reason for the law, the problems sought to be remedied, the purposes to be achieved, and the consequences of construing the statute one way or another." *McDonald*, 2022 IL 126511, ¶ 18. The Court has done this when interpreting the Privacy Act by turning to reliable dictionary definitions (*e.g.*, *Rosenbach*, 2019 IL 123186, ¶ 32), looking at how other statutes use the same language (*id.* ¶ 25), applying relevant canons of construction (*id.* ¶ 29), consulting its relevant prior interpretations (*id.* ¶¶ 30-31), and evaluating the purpose of the statute (*id.* ¶ 37). *See West Bend*, 2021 IL 125978, ¶¶ 39-42 (considering how other

courts, dictionaries, and legal literature have defined "publication"). Those tools should be equally utilized here.

A. Plaintiff's reliance on *Watson* to interpret Section 15(b)'s text is misplaced.

Plaintiff relies heavily on *Watson v. Legacy Healthcare Financial Services, LLC*, 2021 IL App (1st) 210279, to suggest Section 15(b) claims accrue with each scan. *Watson* involved an appeal following the circuit court's dismissal of Section 15(a) and (b) claims on statute of limitations grounds. The circuit court, relying on *Feltmeier*, held the Privacy Act claims accrued, and damages flowed, from the initial act of collection and storage of plaintiff's handprint without "first complying with the statute." (*See* A052). By contrast, the First District relied exclusively on its own analysis of the text and the lower federal court decision in *Cothron I*, declining to acknowledge the circuit court decisions that disagreed with *Cothron I*. *Watson*, 2021 IL App (1st) 210279, ¶ 45 n.2; *see also* A029-56 (circuit court decisions). Other than citing *Rosenbach* in passing for the proposition that dictionary definitions are appropriately considered in textual analysis, *Watson* failed to rely on the Court's Privacy Act decisions. The First District's interpretation is wrong. Neither Section 15(b)'s text nor this Court's Privacy Act opinions support it.

1. *Watson*'s interpretation of Section 15(b) is faulty.

The *Watson* court erred because the definitions it adopted do not match its conclusion. *Watson* considered dictionary definitions of "capture" and "collect." As discussed in White Castle's opening brief, those verbs, and the

others in Section 15(b), mean to gain control of something—here, biometric information. *See* White Castle Br. at 23-27. *Watson* came close to reaching that correct conclusion. It acknowledged that "capture" means "to record in a permanent file (as in a computer)" or "to take by force or stratagem; take prisoner; seize." *Watson*, 2021 IL App (1st) 210279, ¶ 58. *Watson* further noted that "collect" means "to gather or exact from a number of persons or sources" or "to gather together; assemble," as in "[t]he professor collected the students' exams." *Id.* ¶ 59. But it then missed the mark.

Applying the First District's textual analysis, Section 15(b)'s terms "capture" and "collect" mean to obtain control. Specifically, the professor collects exams from students with the intent of keeping them. The professor could not collect those exams a second time; they would already be collected and in her control. Similarly, on its face, the definition of "capture" requires establishing control, as in the creation of a permanent file or a seizure of property. Reading these terms together, then, would lead to the following interpretation of Section 15(b): before gaining control of a user's biometric information, an entity must first inform the user of its actions. *See also McDonald*, 2022 IL 126511, ¶ 21 (Privacy Act "mandates that, *before* obtaining an individuals' fingerprint, a private entity must" provide notice and "must also obtain a signed 'written release' from an individual *before* collecting her biometric" data (citing 740 ILCS 14/15(b)).

Yet the First District—relying on *Cothron I*, but without further analysis of its own—held that "the dictionary definitions confirm our reading of the plain language of the statute that its obligations applied to each and every hand scan." *Watson*, 2021 IL App (1st) 210279, ¶ 60. This is wrong. The dictionary definitions point in the exact opposite direction.

2. *Watson* disregards this Court's Privacy Act precedent.

Moreover, *Watson*'s conclusion is contrary to *Rosenbach*. Despite acknowledging that the plain meanings of the verbs in Section 15(b) indicate or mean to gain control, the *Watson* court nonetheless declared that every collection and capture constitutes a new injury. *Id.* ¶ 69. This makes no sense in light of the Court's definition of a Privacy Act injury as the loss of control over and privacy in biometric data. Once control is lost, it is lost. It "vanishes." *Rosenbach*, 2019 IL 123186, ¶ 34.

The First District held that "before collection or capture, an entity must 'first' inform a subject and receive a release." *Watson*, 2021 IL App (1st) 210279, ¶ 53. But it interpreted the use of "first" in Section 15(b) as meaning "unless it first each time." Such a reading is inconsistent with how *Rosenbach* defines what it means to be aggrieved under the Privacy Act. In reaching this faulty conclusion, the First District relied heavily on *Cothron I*, which misquoted *Rosenbach* to reach the same faulty conclusion.

Cothron I cited *Rosenbach* for the proposition that "a person is 'aggrieved within the meaning of Section 20 of the [BIPA] and entitled to seek

recovery under that provision' *whenever* 'a private entity fails to comply with one of section 15's requirements.'" *Cothron I*, 477 F. Supp. 3d 723, 730 (N.D. Ill. 2020) (A064) (quoting *Rosenbach*, 2019 IL 123186, ¶ 33). *Rosenbach* does not use the term "whenever." *Rosenbach* actually held that "*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 or customer whose [biometrics] is subject to the breach." *Rosenbach*, 2019 IL 123186, ¶ 33. "When" indicates a specific point in time, and has a very different connotation than the term "whenever," which indicates multiple instances. *Cothron I*'s change of the term "when" to "whenever" forms the premise for its conclusion that claim accrual occurs with each collection, which is not what *Rosenbach* held.

McDonald emphasizes the incongruity between *Cothron I* and *Watson*, and this Court's Privacy Act precedent. In *McDonald*, the Court explained that the invasion at issue is "*the* lost opportunity 'to say no.'" *McDonald*, 2022 IL 126511, ¶ 43. Section 15(b) notice and consent must occur "*before* collecting" to avoid the singular lost opportunity. *Id.* ¶¶ 5, 43. As between one individual and one entity, there is a singular lost opportunity to say no, and that happens at the first collection. Said differently, an entity must obtain informed consent *before* it first collects biometrics—not *whenever* it collects biometrics.

B. Under Section 15(d), no new injury is created by redisclosure of the same information to the same third party.

Section 15(d) provides that a private entity may not "disclose, redisclose, or otherwise disseminate" biometrics without consent. 740 ILCS 14/15(d). Plaintiff argues that "redisclose" must mean the same biometric data is "disclosed again" to the same entity. Pl. Br. at 12-13. This is incorrect. "Redisclose" means to newly make known, which must implicate a new entity. *See Cothron II,* 20 F.4th at 1163 (A076) ("[R]epeated transmissions of the same biometric identifier to the same third party are not new revelations.").

To this end, the principle of *noscitur a sociis* is instructive. A "word is known by the company it keeps." *Corbett v. Cty. of Lake*, 2017 IL 121536, ¶ 31. Accordingly, "[i]t is a general rule that words grouped in a list should be given related meaning." *Dynak v. Bd. of Educ. of Wood Dale Sch. Dist.*, 2020 IL 125062, ¶ 22 (citing *Corbett*, 2017 IL 121536, ¶ 31). Thus, as the Seventh Circuit suggested, "disclose, redisclose, or otherwise disseminate" is simply a way to ensure that all disclosure-like acts are covered. *See Cothron II*, 20 F.4th at 1164 (A076).

In addition, to the extent the Court has any doubt about the plain meaning of "redisclose," it is appropriate to look to other Illinois statutes to see how the legislature used the term there—just as the Court has done to interpret the Privacy Act and the Seventh Circuit did in certifying the question. *See Rosenbach*, 2019 IL 123186, ¶ 25; *Cothron II*, 20 F.4th at 1164

n.1 (A076); *see also State v. Mikusch*, 138 Ill. 2d 242, 247-48 (1990) (Legislature presumed to act "rationally and with full knowledge of all previous enactments."); *Christ Hosp. & Med. Ctr. v. Ill. Comprehensive Health Ins. Plan*, 295 Ill. App. 3d 956, 961 (1st Dist. 1998) (Legislative intent may be discerned from use of the same term in "other Illinois statutes.").

The word "redisclose" appears 16 times in Illinois statutes. Every time, it means an individual or an entity is prohibited from disclosing information already received to a new or downstream individual or entity. *See, e.g.*, 210 ILCS 45/3-801.1 (under Nursing Home Care Act, no state agency may "redisclose" records of a person with a disability without advance written notice); 210 ILCS 47/3-801.1 (same prohibition for ID/DD Community Care Act); 405 ILCS 45/3(C) (same prohibition in Mentally Ill Persons Act). The Mental Health and Developmental Disabilities Confidentiality Act uses "redisclose" throughout to mean new or downstream entities. Certain agencies are permitted to disclose an individual's "record or communications, without consent" to certain institutions for research and treatment purposes. 740 ILCS 110/9.1. Those institutions, however, "shall not *redisclose* any personally identifiable information, unless necessary for treatment of the identified recipient." *Id.* Similarly, a person to whom a disclosure is made under the "Therapist's disclosure" section "shall not *redisclose* any information except as provided in this Act." 740 ILCS 110/9.

It would make no sense in the context of any of the statutes above that a confidential-information violation occurs by disclosing the same confidential information to the same person who initially received it. The same is true for the Privacy Act. Repeat disclosure of the same biometric information to the same third party for the same purpose does not result in a new loss of control or secrecy. It is not a new injury.

C. "One and done" is not White Castle's position, and such a statement is not supported by the Privacy Act's text.

Plaintiff proffers a mistaken description of White Castle's interpretation of BIPA's text as "one and done." According to Plaintiff, the single-claim accrual rule would mean that there are "no limit[s] on what [White Castle] 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." Pl. Br. at 19 (emphasis omitted). This significantly misunderstands White Castle's position for four reasons.

First, single accrual is not a "one-and-done" theory. White Castle is not "done" with its duty to comply with the Privacy Act after an initial scan or disclosure. White Castle continues to owe duties under the Act. White Castle must continue to obtain consent from every Illinois-based new employee prior to scanning their data, each of whom would have a timely claim now if White Castle failed to comply with its notice and consent practices. If Plaintiff's claim is considered untimely, White Castle still faces potential liability to

employees who assert their biometric data was first scanned within the last year or five years without notice and consent.[4]

Second, the Privacy Act itself contains numerous provisions that serve its prophylactic goals even after the first collection or disclosure. Specifically, White Castle has a duty to safeguard information it has collected. 740 ILCS 14/15(a), (e). White Castle has an ongoing duty to destroy any biometric data that current employees have already scanned, once the data's purpose is fulfilled. *Id.* at 15(a). Section 15(c) prohibits the sale of biometrics, so any sale of biometrics would give rise to a new claim. *Id.* at 15(c). Section 15(d) prohibits the disclosure of biometrics to a third party without consent. *Id.* at 15(d). So disclosure of biometrics to a *new third party* would give rise to a new claim—a straightforward reading of the statute that has *always* been White Castle's position, no matter how many times Plaintiff and her *amici* try to twist it.

Third, to the extent a party surreptitiously collects or discloses biometrics, numerous doctrines protect against a statute of limitations running before the plaintiff learns of misconduct that she could not have learned about with reasonable inquiry. For example, the discovery rule prohibits a plaintiff's cause of action from accruing until a party knows or reasonably should know of an injury and that the injury was wrongfully

[4] The question of whether a one-year or five-year statute of limitations applies to Privacy Act claims is before the Court in *Tims v. Black Horse Carriers, Inc.*, No. 127801 (Ill.).

caused. *Clay v. Kuhl*, 189 Ill. 2d 603, 608 (2000). Also, if a defendant fraudulently conceals unlawful conduct, the plaintiff has five years to file suit after discovering the cause of action. 735 ILCS 5/13-215. Illinois recognizes equitable tolling as well, which is appropriate if a defendant actively misleads a plaintiff or takes certain extraordinary measures to prevent a plaintiff from asserting her rights. *Clay*, 189 Ill. 2d at 614.

Fourth, Plaintiff ignores that her conduct also matters. This is not a case where White Castle surreptitiously collected Plaintiff's biometrics. To the contrary, it is uncontroverted that Plaintiff affirmatively *chose* to scan her finger. (*See* A005). To the extent Plaintiff had concerns that her biometric privacy rights were being violated, she had ample opportunity to raise such concerns and to investigate her rights. *Pyle v. Ferrell*, 12 Ill. 2d 547, 555 (1958) ("[I]gnorance of the law or legal rights will not excuse delay in bringing suit."); *People v. Lander*, 215 Ill. 2d 577, 588 (2005) (all citizens "charged with knowledge of the law").

III. The continuing-violation doctrine does not apply.

In a footnote, Plaintiff suggests—without explanation or authority—that the continuing-violation doctrine could apply to Privacy Act violations. Pl. Br. at 21 n.4. This argument is waived. Ill. S. Ct. R. 341(h)(7); *id.* at 341(i) ("Points not argued are forfeited."); *Young America's Found. v. Doris A. Pistole Revocable Living Tr.*, 2013 IL App (2d) 121122, ¶ 23 (citing Rule 341(h)(7), refusing to consider argument raised in footnote that contained "no citation to legal authority").

If considered, the continuing-violation doctrine does not apply here. The continuing-violation doctrine does not apply to "continual ill effects from an initial violation." *Feltmeier*, 207 Ill. 2d at 278. Instead, it "involves viewing the defendant's conduct as a continuous whole for prescriptive purposes," as in an "ongoing scheme." *Id.* at 279-80. For these reasons, the Seventh Circuit has called the doctrine "misnamed" because its purpose is to "allow [a] suit to be delayed until a series of wrongful acts *blossoms* into an injury on which suit can be brought . . . [i]t is thus a doctrine not about a continuing, but about a *cumulative*, violation." *Limestone Dev. Corp. v. Vill. of Lemont, Ill.*, 520 F.3d 797, 801 (7th Cir. 2008); *see also Feltmeier*, 207 Ill. 2d at 282 (applying continuing-violation doctrine to claim for intentional infliction of emotional distress because "repetition of the behavior may be a critical factor in raising offensive acts to actionably outrageous ones . . . whereas one instance of such behavior might not be" (citations omitted)).

Privacy Act violations do not need time to "blossom" to be actionable. *Rosenbach* instructs that the initial failure to comply with Section 15, without more, "is sufficient to support the individual's . . . statutory cause of action." *Rosenbach*, 2019 IL 123186, ¶ 33. No "blossoming" of the claim from "repetition of the behavior" is required. *See Limestone Dev. Corp.*, 520 F.3d at 801; *Feltmeier*, 207 Ill. 2d at 282.

IV. If claims accrue with each scan or disclosure of biometric data, there will be unacceptable policy and constitutional implications.

Policy and constitutional implications matter, and this Court properly considers them. *E.g.*, *McDonald*, 2022 IL 126511, ¶ 18 (Courts consider "the consequences of construing the statute one way or another."); *People v. Nastasio*, 19 Ill. 2d 524, 529 (1960) (Courts have a duty to "interpret [a] statute as to . . . avoid, if possible, a construction that would raise doubts about its validity."). Despite Plaintiff's response, White Castle's and the *amici*'s damages concerns are neither hypothetical nor unlikely, and necessitate the Court's guidance to avoid confusion and potentially "staggering damages awards," as stated in *Cothron II*, 20 F.4th at 1165 (A077).

A recent Privacy Act case involving the railway BNSF is a prime example. Just this March, a federal district court followed *Cothron I*, holding that "a private entity violates the law *each time* it fails to comply with the statute through one of the triggering terms, rather than only the first time." *Rogers v. BNSF Ry. Co.*, No. 19 C 3083, 2022 WL 787955, at *8 (N.D. Ill. Mar. 15, 2022) (emphasis in original). A week later, the same court certified a class of over 44,000 truck drivers, each of whom now can assert numerous Privacy Act claims based on the court's accrual holding, and set the case for trial this September. *Rogers v. BNSF Ry. Co.*, No. 19 C 3083, 2022 WL 854348, at *4 (N.D. Ill. Mar. 22, 2022); *Id.* at Dkt. 144.

BNSF submitted a petition to appeal the ruling to the Seventh Circuit, wherein it freely admitted that the district court, in adopting *Cothron I*, had forced it to consider settling the case because of "potentially staggering liability." *BNSF Ry. Co. v. Rogers*, No. 22-8003 (7th Cir. Apr. 5, 2022). BNSF is confronting potentially millions of dollars in liability "measuring at least $1,000 for each time each of the more than 44,000 class members provided fingerprint information." *Id.* at 8. And, "the magnitude of this potential liability caused by the district court's 'grant of class status can put considerable pressure on the defendant to settle, even when the plaintiff's probability of success on the merits is slight.'" *Id.* at 21 (citation omitted).

This is not surprising. As the district court noted in *Cothron I*, damages are tied to accrual; that court freely acknowledged its accrual method could lead to catastrophic results for Privacy Act defendants. *Cothron I*, 477 F. Supp. 3d at 733 (A066). Illinois circuit court judges have acknowledged the same, and have not left the damages resulting from a per scan/disclosure claim accrual for another day, as suggested by *Watson*. (A029-56). Plaintiff still offers no cogent way to correlate her proposed per scan/disclosure claim accrual method with the Privacy Act's damages provisions, such that a trial court could reasonably implement them. And ignoring these damages consequences, as Plaintiff suggests, leaves serious constitutional questions unanswered. White Castle Br. at 42-46.

Moreover, the real-world implications of the *Cothron I* holding do not align with the real-world use of biometric technology. Plaintiff alleges she enrolled her "fingerprint" in 2007, and since then, White Castle has continued to use the original data as an "authentication method" to verify that she is who she says she is. White Castle Br. at 18-21 (citing A013-16). Subsequent scans merely compare a new scan to previously collected data. Any loss of control occurs only upon the first collection of and first disclosure of biometrics, and that is when a Privacy Act claim accrues.

Contrary to Plaintiff's assertions, the single-accrual approach does not let Privacy Act violators get off scot-free. As a practical matter, all Privacy Act suits are brought as class actions, and given the statutory damages available, any class-wide settlement or judgment will surely send a significant message. *See* White Castle Br. at 49; *see also, e.g.*, Br. of *Amici* Illinois Manufacturers' Ass'n, et al. at 14-15.

Simply put, the real-world consequences of repeated accrual on a class-wide basis are not theoretical. They are happening right now. The BNSF case serves as a real, unfolding example that underscores White Castle's damages calculations. White Castle Br. at 44-45, 49. The Court has an opportunity here to consider and ensure that the Privacy Act's interpretation and application are consistent with real-world liability and damages outcomes.

CONCLUSION

For the reasons above and those stated in White Castle's opening brief, the answer to the certified question is that Privacy Act Section 15(b) and

Section 15(d) claims accrue once, upon the first scan or collection, or the first disclosure or transmission, of purported biometric identifiers or biometric information.

Dated: May 10, 2022

Respectfully submitted,

WHITE CASTLE SYSTEM, INC.

By: */s/Melissa A. Siebert*

Melissa A. Siebert
William F. Northrip
Matthew C. Wolfe
SHOOK, HARDY & BACON L.L.P.
111 South Wacker Drive
Suite 4700
Chicago, Illinois 60606
Tel: (312) 704 7700
Fax: (312) 558-1195
masiebert@shb.com
wnorthrip@shb.com
mwolfe@shb.com

Counsel for Defendant-Appellant White Castle System, Inc.

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 5,979 words.

Dated: May 10, 2022 */s/ Melissa A. Siebert*

NOTICE OF FILING AND CERTIFICATE OF SERVICE

I, Melissa A. Siebert, an attorney, hereby certify that on **May 10, 2022**, I caused a true and complete copy of the foregoing **REPLY BRIEF OF DEFENDANT-APPELLANT WHITE CASTLE SYSTEM, INC.** to be filed electronically with the Clerk's Office of the Illinois Supreme Court, using e-filing provider **Odyssey eFileIL**, which sends notification and a copy of this filing by electronic mail to all counsel of record.

I further certify I caused an additional courtesy copy of this filing to be served by electronic mail upon the following:

Ryan F. Stephan
(rstephan@stephanzouras.com)
James B. Zouras
(jzouras@stephanzouras.com)
Andrew C. Ficzko
(aficzko@stephanzouras.com)
Teresa M. Becvar
(tbecvar@stephanzouras.com)
STEPHAN ZOURAS, LLP
100 North Riverside Plaza, Suite 2150
Chicago, IL 60601
Tel: (312) 233-1550

Attorneys for Plaintiff-Appellee Latrina Cothron, Individually, and on Behalf of All Others Similarly Situated

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

/s/ Melissa A. Siebert