No. 127801

IN THE SUPREME COURT OF ILLINOIS

JOROME TIMS and ISAAC WATSON, individually and on behalf of others similarly situated,

Plaintiffs-Appellees,

v.

BLACK HORSE CARRIERS, INC.,

Defendant-Appellant.

Petition for Leave to Appeal FILED on October 22, 2021

Petition for Leave to Appeal ACCEPTED on January 26, 2022

On appeal from the Appellate Court of Illinois, First District

BRIEF OF *AMICUS CURIAE* ILLINOIS CHAMBER OF COMMERCE IN SUPPORT OF DEFENDANT-APPELLANT BLACK HORSE CARRIERS, INC.

Melissa A. Siebert (ARDC #6210154)
Matthew C. Wolfe (ARDC #6307345)
Ian M. Hansen (ARDC #6329781)
SHOOK, HARDY & BACON LLP
111 South Wacker Drive, Suite 4700
Chicago, Illinois 60606
(312) 704-7700
masiebert@shb.com
mwolfe@shb.com
ihansen@shb.com

Counsel for Amicus Curiae *Illinois Chamber of Commerce*

TABLE OF CONTENTS AND POINTS AND AUTHORITIES

INTEREST OF *AMICUS CURIAE*

In recent years, businesses across Illinois have endured a wave of hundreds of lawsuits filed under the Illinois Biometric Information Privacy Act (the "Privacy Act"). The targets of Privacy Act lawsuits are Illinois businesses that span multiple industries and vary in size. They include community hospitals, small, family-owned grocery stores, nursing homes and rehabilitation centers, restaurants, food service companies, retailers, hotels and airlines, and other, well-respected Illinois-based businesses—industries that form the backbone of the Illinois economy and provide essential employment and services to Illinois citizens. The vast majority of Privacy Act lawsuits consist of putative class actions with hundreds, if not thousands, of members alleging technical violations of the statute due to the use of timekeeping systems that purportedly rely on finger, hand, or face scanners. With statutory damages of up to $5,000 per violation, these lawsuits have the potential to impose devastating damages on Illinois businesses across the state.

Amicus Illinois Chamber of Commerce (the "Chamber") is the voice of the business community in Illinois. The Chamber is a statewide organization with more than 1,800 members in virtually every industry, including manufacturing, retail, insurance, construction and finance. The Chamber advocates on behalf of its members to achieve an optimal business environment that enhances job creation and economic growth.

The Chamber's interest in this case is substantial. At least 32 members of the Chamber have been sued in Privacy Act lawsuits in the last four years. The litigation surge shows no signs of slowing down. Some 1,486 Privacy Act lawsuits have been filed in state and federal courts since fall 2017. Since January 2021, no fewer than 549 new Privacy Act lawsuits have been filed, 116 of which have been filed since the beginning of 2022.

The key question before the Court—whether the statute of limitations for Privacy Act claims is one year, five years, or both depending upon the subsection allegedly violated—has the potential to dramatically expand the onslaught of Privacy Act class action lawsuits that have demanded, and continue to demand, enormous resources from Illinois businesses. Illinois businesses, especially smaller businesses, will be negatively impacted if the appellate court's decision applying the five-year catchall statute of limitations to certain Privacy Act claims is upheld. Such would result in larger putative class sizes, costlier discovery, and larger amounts sought in damages. A five-year statute of limitations for any section of the Privacy Act would also contravene the Act's preventative purpose.

What businesses need now more than ever is certainty. The COVID-19 pandemic has created unprecedented economic challenges, leaving many businesses simply struggling to survive. Allowing five years for plaintiffs to bring some Privacy Act claims will create an even more uncertain climate for businesses. It will increase exposure to class actions seeking massive (and

potentially catastrophic) damages. Overturning the appellate court's decision and applying the one-year statute of limitations for privacy claims to *all* Privacy Act claims is necessary to promote the legislative objectives of both the Privacy Act and statutes of limitations generally. This brief will assist the Court by addressing the implications of the appellate court's decision for the Illinois business community.

INTRODUCTION

This appeal presents an issue of critical importance: whether the one-year statute of limitations for privacy claims or the five-year catchall statute of limitations applies to Privacy Act claims. The scope and viability of hundreds of Privacy Act class actions turns on the answer to this question.

In its three prior decisions interpreting the Privacy Act, the Court has made clear that the purpose of the Privacy Act is to "prevent problems" resulting from the compromise of biometric data[1] before they occur." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 37. Like privacy torts that involve publication, the Privacy Act "*protects a secrecy interest*—here, the right of an individual to keep his or her personal identifying information like fingerprints secret." *West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan*, 2021 IL 125978, ¶ 46. (emphasis added). The Privacy Act accomplishes its protective purpose by establishing "*prophylactic measures*" that work together to "*prevent*

[1] The Privacy Act regulates "biometric identifiers" and "biometric information," as defined by the Act. For convenience, this brief refers to them collectively as "biometric data" or "biometrics."

compromise of an individual's biometrics." *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶ 48. (emphasis added).

Statutes of limitations exist to provide the maximum timeframe within which a suit must be brought, and they vary based on the purpose of the statute involved. A one-year statute of limitations applies to privacy claims asserting "slander, libel, or publication of matter violating the right of privacy." 735 ILCS 5/13-201. Because the Privacy Act does not provide a statute of limitations, the maximum timeframe in which to bring a lawsuit should be determined by reviewing the nature of liability under the Privacy Act, rather than the particular relief sought. *Travelers Cas. & Sur. Co. v. Bowman*, 229 Ill. 2d 461, 469 (2008). Moreover, the statute of limitations for all Privacy Act claims should be "governed by one spirit and a single policy." *Uldrych v. VHS of Ill., Inc.*, 239 Ill. 2d 532, 540 (2011).

The appellate court failed to undertake the analysis set forth in *Travelers* or *Uldrych*, and instead relied on a hyper-technical analogy to a Second District ruling—a ruling that this Court never has endorsed. In doing so, the appellate court reached an odd result that splits the Privacy Act in two: claims brought under Sections 15(c) and (d) are governed by the one-year privacy statute of limitations, but claims brought under Sections 15(a), (b), and (e) are governed by the five-year "catchall" statute of limitations.

Under the appellate court's ruling, a plaintiff whose data is sold to a third party for a profit (in violation of Section 15(c)), or whose data is re-

disclosed by a third-party to yet another third party, has less time to sue than an individual who, as here, knowingly uses a biometric time clock on a daily basis, and is thus fully aware their data is being collected, stored, used and disclosed for timekeeping purposes. Other courts assessing Privacy Act claims have indicated that the risk of data compromise increases when data is stored without notice and not destroyed (in violation of Section 15(a) and (b)), yet those portions of the Privacy Act have a five-year statute of limitations under the appellate court's ruling. And, it just stands to reason that the data compromise problems the Privacy Act seeks to prevent can be more promptly addressed and remediated by a one-year statute of limitations, not a five-year period (or in the case of Section 15(a), as long as eight years, given the time frame for data destruction already built into the statute). The extended statute of limitations proposed by the appellate court for some claims subverts the Privacy Act's purpose—which is to protect against unauthorized or otherwise wrongful disclosure of biometric data. *Rosenbach*, 2019 IL 123186, ¶ 37.

The practical result of the appellate court ruling is that Privacy Act class sizes will dramatically increase while actually working against the preventative purpose of the Privacy Act. More time to allow a situation of non-compliant notice and consent to continue to exist before requiring suit will not prevent problems from occurring in the first instance, but it will grow large classes for settlement or trial, result in expanded litigation and discovery, and

increase attorneys' fees. A one-year statute of limitations is an important restraint on potential for abuse.

The appellate court's ruling produces another discordant result: it subjects alleged violators of the procedural requirements in Sections 15(a), (b) or (e) to *five times the financial penalty* of alleged violators of Sections 15(c) or (d)—even though violators of Sections 15(c) and (d) allegedly have *actually disclosed* individuals' biometric information to unauthorized parties (the precise and ultimate harm the Privacy Act aims to prevent).

The Privacy Act's purpose is to protect against the improper disclosure of individuals' private information. Particularly in cases such as this one that involve the voluntary use of a time clock, the purpose is best served by requiring individuals to bring claims promptly. The sooner individuals file suit, the sooner businesses become aware of alleged violations, and the sooner businesses can get compliant with the statute (if necessary). The result of an earlier resolution is that fewer individuals' privacy rights are at risk of compromise—the Act's entire point. In contrast, the appellate court's decision creates a countervailing incentive to manipulate pleadings to avoid the shorter one-year statute of limitations and create greater fees and larger settlements, while doing nothing to further the Privacy Act's purpose. The Court should reverse the decision below.

ARGUMENT

I. The one-year statute of limitations for privacy claims applies to *all* causes of action under the Privacy Act.

A. The Privacy Act aims to prevent the unauthorized publication of biometric data.

The Court's three prior decisions made clear the Privacy Act aims to prevent unauthorized or otherwise wrongful publication of biometric data. *Rosenbach*, 2019 IL 123186, ¶¶ 33-34; *West Bend*, 2021 IL 125978, ¶ 46; *McDonald*, 2022 IL 126511, ¶ 48. The Court's teachings in those cases are dispositive of this appeal: because the Privacy Act's requirements are "prophylactic measures" designed to "prevent compromise of an individual's biometrics," *McDonald*, 2022 IL 126511, ¶ 48, the one-year statute of limitations "for publication of matter violating the right of privacy" applies to *all* claims under the Privacy Act.

First, *Rosenbach* explains that the Privacy Act "imposes numerous restrictions on how private entities collect, retain, disclose, and destroy biometric identifiers" and made clear that the purpose of these restrictions is to "prevent problems before they occur." *Rosenbach*, 2019 IL 123186, ¶¶ 1, 37. *West Bend* further described the Act's protections, noting 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. *West Bend* further explained that "disclosing a person's biometric identifiers or information without their consent or knowledge necessarily violates that person's right to privacy in biometric information." *Id*. And, once

biometric data is allegedly obtained by or disclosed to a third party, the individual's "right to keep certain information confidential" is violated, and the data's "secrecy" is lost. *Id.* ¶ 45. Secrecy cannot be recreated: once information has been shared, it is no longer secret. As *Rosenbach* puts it, once lost through a violation of any of the rights conferred by the Privacy Act, the right to control biometric data—that is, to maintain its confidentiality and secrecy—"vanishes into thin air." *Rosenbach*, 2019 IL 123186, ¶ 34.

In *McDonald*, the Court further stated: "The Privacy Act involves prophylactic measures to prevent compromise of an individual's biometrics." *McDonald*, 2022 IL 126511, ¶ 43 (citing *Rosenbach*, 2019 IL 123186, ¶ 36). *McDonald* thus reaffirms *Rosenbach*'s conclusion that the Act's ultimate aim is to "prevent problems before they occur." *Rosenbach*, 2019 IL 123186, ¶ 37.

Rosenbach, *West Bend*, and *McDonald* therefore show that the purpose of the Privacy Act is to prevent the unauthorized compromise of biometrics. The "determination of the applicable statute of limitations is governed by the type of injury at issue." *Travelers*, 229 Ill. 2d at 469 (citing *Armstrong v. Guigler*, 174 Ill. 2d 281, 286 (1996)). The "focus of the inquiry is on the nature of the liability." *Id*. In the context of the Privacy Act, the injury at issue is the unauthorized publication of biometric data. But the appellate court's opinion did not consider that the Act's entire purpose, and thus the nature of any liability arising from the Act, is the prevention of the wrongful publication of biometric data.

Instead, the appellate court first set out the "two types of privacy interests in the right to privacy": "secrecy," on the one hand, and "seclusion" on the other. *Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st) 200563, ¶ 21. Then, relying on "[its] decision in *Benitez*," the appellate court held that the one-year statute of limitations "does not encompass all privacy actions but only those where publication is an element or inherent part of the action"—*i.e.*, those aimed at protecting individuals' "secrecy" privacy interest. *Id.* ¶ 30. The appellate court then sliced the Privacy Act through the middle: because Sections 15(c) and (d) include what it called "an element" of "publication or disclosure," the one-year statute applies. *Id.* ¶ 32. The five-year statute applies to Sections 15(a), (b), and (e), however, because according to the appellate court, none of them involves publication or disclosure. *Id.* ¶ 31.

Such reflexive analysis is flawed. At the outset, its key rule—that the one-year statute applies only if the claim includes a formal publication element—is not the law of Illinois. It derives from a Second District case, *Benitez v. KFC National Management Co.*, 305 Ill. App. 3d 1027 (1999), and this Court has never endorsed such a hard line, nor should it. Rather, the Court's precedent makes utterly clear that the Privacy Act's provisions are "prophylactic measures" that *work together* to preserve the "power to say no" to the collector of biometrics, *Rosenbach*, 2019 IL 12386, ¶ 33, "prevent compromise of an individual's biometrics," *McDonald*, 2022 IL 126511, ¶ 43, and *all* thereby "protect[] a secrecy interest." *West Bend*, 2021 IL 125978, ¶ 46.

Each of the Privacy Act's subsections is aimed at the same ultimate goal: to prevent unauthorized dissemination of an individual's biometrics. *First*, the Act expressly prohibits the precise conduct it sets out to prevent: dissemination of biometrics without individuals' consent. 740 ILCS 14/15 (c), (d). *Second*, it requires that entities observe certain procedures in collecting and handling biometric data—*i.e.*, procuring informed consent prior to collection, establishing and following retention policies, and handling data with reasonable care—that further protect secrecy and privacy by making unauthorized or accidental disclosure less likely to occur. 740 ILCS 14/15(a), (b) and (e). Indeed, this Court and others consistently have recognized that the Privacy Act's provisions serve to further its primary, data-protection objective. *See Rosenbach*, 2019 IL 123186 at ¶¶ 33-36; *West Bend*, 2021 IL 125978, ¶ 46; *McDonald*, 2022 IL 126511, ¶ 43. *See also Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 620 (7th Cir. 2020), *as amended on denial of reh'g and reh'g en banc* (June 30, 2020) (noting that the Privacy Act is concerned with "the sensitivity of biometric information and the risk of identity theft or other privacy or economic harm that may result from its dissemination"); *Figueroa v. Kronos Inc.*, 2020 WL 1848206, *3 (N.D. Ill. Apr. 13, 2020) (the denial of plaintiffs' "opportunity to withhold their consent to the collection or dissemination of their data" was "no mere technicality, for without being informed that Kronos or outside data hosts would obtain their data, Plaintiffs were denied entirely an opportunity to object, in any fashion, to the way their

data was handled"); *Howe v. Speedway LLC*, 2018 WL 2445541, at *5 (N.D. Ill. May 31, 2018) ("BIPA's notice and consent provisions do not create a separate interest in the right-to-information, but instead operate in support of the data protection goal of the statute.")

The appellate court's opinion also is flawed from the perspective of practical consequences. The appellate court's decision subjects alleged violators of the procedural requirements in Sections 15(a), (b) or (e) to *five times the financial penalty* of alleged violators of Sections 15(c) or (d)—even though violators of Sections 15(c) and (d) allegedly have *actually disclosed* individuals' biometric data to unauthorized parties (the precise and ultimate harm the Privacy Act aims to prevent). But the point of the Privacy Act is to prevent problems before they occur, which is shown by the plain text of the statute. Sections 15(a), 15(b), and 15(e) all serve to protect biometric data from disclosure by requiring a biometrics policy and compliance with that policy (Section 15(a)); notice and consent before collection (15(b)); and secure storage and transmission of biometric data (15(e)). The whole purpose of the policy, collection, and security requirements in Sections 15(a), 15(b) and 15(e) accordingly is to prevent unauthorized disclosure before it occurs; all of the subsections of Section 15 work together to achieve the Privacy Act's overarching goal of preventing the unauthorized disclosure of biometric data.

B. The one-year statute of limitations applies to claims intended to prevent and remedy wrongful "publication" of personal information.

The one-year statute of limitations "for publication of [a] matter violating the right of privacy," 735 ILCS 5/13-201, applies to virtually every privacy common law and statutory claim, including defamation, false light, public disclosure of private facts, misappropriation of an individual's likeness, and violation of the Illinois Right of Publicity Act ("IRPA"). *See Bryson v. News Am. Publications, Inc.*, 174 Ill. 2d 77, 105 (1996) ("[t]he limitations period for invasion of privacy claims and for defamation claims is one year after the cause of action accrues"); *Leopold v. Levin*, 45 Ill. 2d 434, 444 (1970) (the one-year statute of limitations applies to claims for misappropriation of an individual's likeness); *Blair v. Nevada Landing P'ship*, 369 Ill. App. 3d 318, 323 (2006) (the one-year statute of limitations applies to claims under IRPA); *Poulos v. Lutheran Soc. Servs. of Illinois, Inc.*, 312 Ill. App. 3d 731, 745 (2000) (same as to false light); *Johnson v. Lincoln Christian College*, 150 Ill. App. 3d 733, 745-46 (1986) (same as to public disclosure of private facts); *Founding Church of Scientology of Washington, D.C. v. Am. Med. Ass'n*, 60 Ill. App. 3d 586, 589 (1978) (same as to libel); *Bakalis v. Bd. of Trustees of Cmty. Coll. Dist. No. 504, Cty. of Cook, State of Ill. (Triton Coll.)*, 948 F. Supp. 729, 736 (N.D. Ill. 1996) (same for libel).

All of these claims share the same ultimate goal as the Privacy Act: to prevent or remedy the unauthorized or otherwise wrongful publication of personal information. *See Kolegas v. Heftel Broad. Corp.*, 154 Ill. 2d 1, 17–18

(1992) (false light claim shows that plaintiff was "placed in a false light before the public"); *Trannel v. Prairie Ridge Media, Inc.*, 2013 IL App (2d) 120725, ¶ 18 (IRPA claims address the "public use" *or* "holding out" of an individual's identity"); *Poulos*, 312 Ill. App. 3d at 745 ("[a]n action for public disclosure of private facts provides a remedy for the dissemination of true, but highly offensive or embarrassing, private facts"); *Ainsworth v. Century Supply Co.*, 295 Ill. App. 3d 644, 648 (1998) (misappropriation of likeness claims are "designed to protect a person from having his name or image used for commercial purposes without consent.")

Very little is required to establish that a claim involves "publication." In fact, publication can occur when private information is disclosed to a single third party. For instance, in *Poulos*, the Court held that the one-year statute of limitations applies to the common-law privacy tort of public disclosure of private facts even though the private facts need not be communicated "to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Poulos*, 312 Ill. App. 3d at 740. To that end, courts have held that an action as minor as sending an intra-office communication from one employee to another constitutes publication. *Popko v. Cont'l Cas. Co.*, 355 Ill. App. 3d 257, 265–66 (2005); *accord West Bend*, 2021 WL 2005464, ¶ 43 (holding that "the term publication has at least two definitions and means both the communication of information to a single party and the communication of information to the public at large").

Here, the Privacy Act protects against the loss of control of privacy in biometric data, which necessarily involves publication to another. *West Bend* makes this exact point. In *West Bend*, the Court analyzed the nature of the interest the Act itself protects, and concluded 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.[2] Secrecy cannot be recreated. By definition, a loss of secrecy, or control of privacy, occurs equally when data is collected by another entity (and thus published to it), and upon publication, or disclosure, to a new party. Accordingly, all claims within the Privacy Act fit comfortably within the types of privacy claims to which the one-year statute of limitations applies.

C. The Privacy Act's purpose and legislative history further support that the one-year statute of limitations applies to all claims.

The Privacy Act's purpose and legislative history confirm that its aim is to prevent and remedy the wrongful disclosure, or publication, of private information—just like the other claims that are subject to the one-year statute of limitations.

---

[2] Although *West Bend* was construing the term "publication" as used in an insurance policy, the Court expressly drew on "dictionaries, treatises, and the Restatement" in concluding that "publication" includes a "communication of information to a single party." *Id.* Accordingly, *West Bend's* holding is not limited to the insurance context. Rather, it reaffirms the general proposition of law stated in *Poulos* and *Popko*.

The Illinois General Assembly enacted the Privacy Act to protect against the disclosure and sale of individuals' biometric data. *Rosenbach*, 2019 IL 123186 at ¶ 34 (stating that the General Assembly enacted the Privacy Act in light of assessing the "difficulty in providing meaningful recourse *once a person's biometric identifiers or biometric information has been compromised*.") (emphasis added). As the legislative findings and intent of the statute expressly state, biometrics present unique risks to individuals' privacy because they are unique and therefore, unlike a social security number, cannot be changed once compromised. 740 ILCS 14/5. Accordingly, "the purpose of the BIPA is to ensure that, when an individual engages in a biometric-facilitated transaction, *the private entity protects the individual's biometric data*, and does not use that data for an improper purpose, especially a purpose not contemplated by the underlying transaction." *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 504 (S.D.N.Y. 2017) (emphasis added), *vacated in part on other grounds*, 717 F. App'x 12 (2d Cir. 2017). The statute was enacted in the wake of the Pay By Touch bankruptcy, in which a court approved the sale of a defunct company's database of biometric data. *See Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175 at ¶¶ 63, 115. Lawmakers' chief concern was that individuals' biometric data would be sold or otherwise disclosed to third parties. The legislature made this concern explicit in the preamble to the statute. 740 ILCS 14/5(c) ("Biometrics, however,

are biologically unique . . . therefore, *once compromised*, the individual has no recourse") (emphasis added).

When determining what statute of limitations applies, the Court has a "singular concern": "to ascertain and give effect to the legislature's intent." *Uldrych v. VHS of Ill., Inc.*, 239 Ill. 2d 532, 540 (2011) (*citing Moore v. Green*, 219 Ill. 2d 470, 488 (2006)). "When the spirit and intent of the legislature are clearly expressed and the objects and purposes of a statute are clearly set forth, courts are not bound by the literal language of a particular clause of the statute that might defeat such clearly expressed legislative intent." *Id.* (citing *In re Application of the Cty. Treasurer*, 214 Ill. 2d 253, 259 (2005)). A court "must presume that *several statutes relating to the same subject . . . are governed by one spirit and a single policy*, and that the legislature intended the several statutes to be consistent and harmonious." *Id.* (emphasis added).

In this case, the Privacy Act's several subsections "are governed by one spirit and a single policy" (*see id.*): to prevent "*publication* of matter violating the right of privacy." *See* 735 ILCS 5/13-201 (emphasis added). The overarching purpose of the statute does not change depending on the specific provision allegedly violated. As recognized by the court in *Rosenbach*, *West Bend*, and *McDonald*, as well as by the Seventh Circuit in *Bryant*, the Privacy Act's provisions work in tandem toward the same purpose: to prevent the wrongful publication of private information. That purpose, in turn, determines the proper limitations period. Accordingly, the one-year statute of limitations

applies to Privacy Act actions irrespective of which particular provision allegedly was violated.

Notably, the appellate court "[did] not address . . . legislative history" in concluding that two separate statutes of limitations apply to different Privacy Act subsections. *Tims*, 2021 IL App (1st) 200563, ¶ 35. This was a critical error because the Privacy Act's legislative history informs the entire statute and makes clear that all of its subsections are intended to work together in service of the same purpose: preventing and remedying the unauthorized or otherwise wrongful disclosure of biometric data. The appellate court's decision to split the Privacy Act in two thus strikes an oddly dissonant chord.

D. The one-year statute of limitations applies to claims that closely resemble Privacy Act claims.

The Privacy Act's similarity to other statutes governed by the one-year statute of limitations further supports the same limitations period here. Again, the Court must look to the nature of the liability. *See Travelers*, 229 Ill. 2d at 469. Furthermore, where "two statutes of limitation arguably apply to the same cause of action, the one which more specifically relates to the action must be applied."[3] *SPSI Res. LLC v. MB Fin. Bank, Nat. Ass'n*, 55 N.E.3d 186, 195 (1st Dist. 2016).

---

[3] A two-year statute of limitations for "[a]ctions for damages for an injury to the person," 735 ILCS 5/13-202, is another potentially applicable limitations period to Privacy Act claims. Indeed, in *McDonald*, the Court characterized Privacy Act injuries as "personal and societal injuries caused by violating [the Privacy Act's] prophylactic requirements." *McDonald*, 2022 IL 126511, ¶ 43. The applicability of the two-year statute of limitations to Privacy Act claims is currently before the Appellate Court for the Third District in *Marion v. Ring*

Looking to the nature of the liability at issue and considering which statute of limitation should apply, it is instructive that the Illinois Right to Privacy Act ("IRPA") applies the one-year statute of limitations. *See Blair*, 369 Ill. App. 3d at 323. Like the Privacy Act, the IRPA codifies privacy rights. "IRPA grants to each individual the 'right to control and to choose whether and how to use [his or her] identity for commercial purposes,' and prohibits use of 'an individual's identity for commercial purposes during the individual's lifetime without having obtained previous written consent.'" *Troya Int'l, Ltd. v. Bird-X, Inc.*, No. 15 C 9785, 2017 6059804, at *13 (N.D. Ill. Dec. 7, 2017) (citing 765 ILCS 1075/10, 1075/30). Under the Privacy Act, "individuals possess a right to privacy in and control over their biometric identifiers and biometric information," which the Act regulates by "requiring notice before collection and giving them the power to say no by withholding consent." *Rosenbach*, 2019 IL 123186, ¶ 34.

The statutes also operate in very similar ways. Plaintiffs suing under IRPA can recover the greater of "(1) actual damages, profits derived from the unauthorized use, or both; or (2) $1,000." 765 ILCS 1075/40(a). Punitive damages are available against a person who willfully violates IRPA. *Id.* at 1075/40(b). Similarly, the Privacy Act permits courts to choose to award

---

Container Technologies, LLC, No. 3-20-0184. Because the two-year statute of limitations is another potential statute of limitations that "more specifically relates to the action" than the five-year catch-all statute of limitations, the Court should limit its holding in this case to deciding whether the one-year statute of limitations applies to Privacy Act claims.

prevailing plaintiffs the greater of actual damages or liquidated damages of up to $1,000 for negligent violations and up to $5,000 for intentional or reckless violations. 740 ILCS 14/20. Both statutes codify rights to privacy. Both provide courts the discretion to award varying amounts of statutory damages according to differing levels of culpability. Both are concerned with preventing the disclosure or publication of a person's information.

Like the Privacy Act, IRPA does not supply its own statute of limitations. *Blair*, 369 Ill. App. 3d at 322. Rather, the one-year privacy statute of limitations applies to IRPA claims because they involve the disclosure of private facts. *Id*. This point is particularly important because it establishes that publication does not need to be a specific element of a claim in order to come within the purview of the one-year statute of limitations. Claims under IRPA simply require "[1] an appropriation of one's name or likeness, [2] without one's consent, [3] for another's commercial benefit." *Blair*, 369 Ill. App. 3d at 322 (recognizing that to state a claim under IRPA, a plaintiff must essentially meet the same three elements as its common-law antecedent). Publication is not an express element of IRPA claims, but the one-year statute of limitations applies nonetheless. Likewise, although it is possible to plead certain Privacy Act claims without alleging publication to a third party, publication is central to the Act's purpose and the nature of liability.

As explained *supra*, this Court's holdings emphasize that the nature of liability—not the particular relief sought—is determinative in assessing

whether the one-year statute of limitations applies. *Travelers*, 229 Ill. 2d at 469. Privacy Act claims involve the same type of liability as other claims falling within the one-year statute of limitations. Specifically, Privacy Act claims protect the right to control information about oneself and deter wrongful or unauthorized disclosure of such information, and so do other claims governed by the one-year statute of limitations. *See*, *e.g.*, *CBS, Inc. v. Partee*, 198 Ill. App. 3d 936, 945, (1990) (privacy is "the individual's right to control dissemination of information about himself"). And liability occurs when a third party interferes with that control, whether by disclosing private facts to a third party (the basis of public disclosure of private facts claims) or profiting off a person's image without their consent, such as with misappropriation of likeness claims. *See, e.g., Poulos*, 312 Ill. App. 3d at 745 ("[a]n action for public disclosure of private facts provides a remedy for the dissemination of true, but highly offensive or embarrassing, private facts"); *Ainsworth*, 295 Ill. App. 3d at 648 (misappropriation of likeness claims are "designed to protect a person from having his name or image used for commercial purposes without consent.")

The Act's structure, the legislative history, and its objectives demonstrate that Privacy Act lawsuits are "[a]ctions for . . . publication of matter violating the right of privacy," and therefore are governed by the one-year statute of limitations of 735 ILCS 5/13-201. Plaintiff, and all other Privacy Act claimants, cannot escape the legislature's intent to create a statutory cause of action that closely resembles other claims falling within the purview of the

one-year statute of limitations. The one-year statute of limitations applies to Privacy Act claims.

II. A one-year statute of limitations is essential to achieve the Privacy Act's intended purpose by incentivizing plaintiffs to come forward promptly and thereby expediting any needed remediation.

A short statute of limitations is consistent with the Privacy Act's policy prerogatives. Lawmakers designed the Act to incentivize compliance and "to try to head off [] problems before they occur." *Rosenbach*, 2019 IL 123186, ¶ 36. This legislative intent is evident in the duties imposed by the Privacy Act, which focus primarily on safeguards companies must enact before collecting biometrics. It is also evident in the statute's enforcement mechanism. *Id.*

The Act's private right of action plays a particularly critical role in incentivizing companies to comply with the statute. *Id.* ¶ 37. "When private entities face liability for failure to comply with the law's requirements without requiring affected individuals or customers to show some injury beyond violation of their statutory rights, those entities have the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone." *Id.* Because the Act is enforced solely through private actions, a company may not discover the existence of alleged violations until it is served with a lawsuit, at which point measures may be taken to get compliant. 740 ILCS 14/20. Allowing plaintiffs five years to bring Privacy Act claims will effectively delay compliance with the statute and risk compromising *more* individuals' privacy rights. In contrast, a one-year statute

advances the Act's principal objective: claims will be brought sooner, thus companies that are not compliant already will become compliant sooner, and fewer individuals' privacy rights will potentially be compromised.[4]

Rosenbach likewise confirmed that plaintiffs should bring claims expeditiously. When assessing the impact of potential delays associated with requiring plaintiffs to allege an actual injury in addition to a violation of the statute, the Court found: "[t]o require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse . . . would be completely antithetical to the Act's *preventative and deterrent purposes*." *Rosenbach*, 2019 IL 123186, ¶ 37 (emphasis added). A five-year statute of limitations would be equally antithetical to those purposes.

III. A one-year statute of limitations promotes the legislative policy goals underpinning statutes of limitations.

Statutes of limitations provide vital "security and stability to human affairs." *Gabelli v. SEC*, 568 U.S. 442, 448-49 (2013). Courts throughout the

---

[4] Other privacy statutes have statutes of limitations of similar duration. For instance, the Fair Credit Reporting Act of 1970 has a two-year statute of limitations and a five-year statute of repose. 15 U.S.C. § 1681. The Privacy Act of 1974 also has a two-year statute of limitations. 5 U.S.C. § 552a(g)(5). Additionally, actions under the Illinois Personal Information Protection Act and Illinois Consumer Fraud and Deceptive Business Practices Act have three-year statutes of repose. 815 ILCS 530/20 (violations of the Illinois Personal Information Protection Act are violations of the Illinois Consumer Fraud and Deceptive Business Practices Act); 815 ILCS 505/10a(e)(any claim under the Illinois Consumer Fraud and Deceptive Business Practices Act "shall be forever barred unless commenced within 3 years after the cause of action accrued").

country have consistently recognized the importance of statutes of limitations "to allow more certainty and reliability" in civil litigation—policy goals that "are a necessity in a marketplace where stability and reliance are essential components of valuation and expectation for financial actors." *California Pub. Employees' Ret. Sys. v. ANZ Sec., Inc.*, 137 S. Ct. 2042, 2055 (2017).

This Court has recognized and respected the General Assembly's prerogative to adopt statutes of limitations, which "represent society's recognition that predictability and finality are desirable, indeed indispensable, elements of the orderly administration of justice." *Sundance Homes, Inc. v. Cty. of DuPage*, 195 Ill. 2d 257, 265–66 (2001). Statutes of limitations exist to "discourage the presentation of stale claims and to encourage diligence in the bringing of actions." *Id*.

In the context of Privacy Act claims, the one-year privacy statute of limitations promotes the policy goals behind statutes of limitations in several ways. *First*, the claims are of the precise type that can and should be brought at an early stage. As is the case here, the vast majority of Privacy Act claims are brought by employees who knowingly and voluntarily scan their fingers, hands, or faces for timekeeping and pay purposes. Courts have noted the obvious: individuals who scan their fingers are aware that their information is being collected and stored. *See*, *e.g.*, *Bryant*, 958 F.3d at 620 (plaintiff "voluntarily created a user account for the Smart Market vending machines and regularly made use of the fingerprint scanner to purchase items from the

machines"); *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017) (explaining that "[n]o reasonable person, however, would believe that the MyPlayer feature was conducting anything other than [] a [facial] scan"); *McGinnis v. United States Cold Storage, Inc.*, 382 F. Supp. 3d 813, 819 (N.D. Ill. 2019) (plaintiff "knew his fingerprints were being collected because he scanned them in every time he clocked in or out of work, and he knew they were being stored because the time-clock-scanned prints were obviously being compared to a stored set of prints"); *Howe v. Speedway LLC*, 2018 WL 2445541, at *6 (N.D. Ill. May 31, 2018) (employee's "fingerprints were collected in circumstances under which any reasonable person should have known that his biometric data was being collected"); *Goings v. UGN, Inc.*, 2018 WL 2966970, at *4 (N.D. Ill. June 13, 2018) (noting that the plaintiff-employee "was aware that he was providing his biometric data to defendants" for timekeeping purposes); *McCollough v. Smarte Carte, Inc.*, 2016 WL 4077108 at *1 n.1 (N.D. Ill. Aug. 1, 2016) ("This Court assumes that a customer would understand that Smarte Carte collects and retains their fingerprint data for at least the duration of the rental. The system would not work otherwise.") In other words, the facts giving rise to many alleged Privacy Act violations, including the one at issue here, are apparent at the first scan.[5]

[5] Where it is not obvious that biometrics are potentially being collected, discovery and tolling doctrines could help mitigate any concern about a plaintiff not realizing she has a claim until it is too late.

Nor are Privacy Act claims difficult to file, as evidenced by the many lawsuits pending all over Illinois. Most Privacy Act complaints are copied and pasted from previously filed complaints that simply substitute the parties. *See*, *e.g.*, *Colon v. Dynacast, LLC*, 2019 WL 5536834, at *4 (N.D. Ill. Oct. 17, 2019) (noting that the case was "virtually identical" to several other Privacy Act cases); *see also A Bad Match: Illinois and the Biometric Information Privacy Act*, Institute for Legal Reform (Oct. 12, 2021), available at https://instituteforlegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf (discussing the "massive wave" of Privacy Act class actions). Little, if any, investigation into the facts of each case is done before the case is filed. Moreover, plaintiffs "need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act . . . to seek liquidated damages and injunctive relief." *Rosenbach*, 2019 IL 123186, ¶ 40. Given these low barriers to filing suit, courts should apply "relatively short time limits for types of claims that are readily recognizable early in their existence and that would be expected to bring about litigation soon after their arising." David Crump, *Statutes of Limitations: The Underlying Policies*, 54 U. Louisville L. Rev. 437, 443 (2016) (pointing to the one-year statute of limitations for defamation claims as an example).

Second, allowing a longer limitations period is unfair to Privacy Act defendants. Courts have emphasized that statutes of limitations "embody a policy of repose, designed to protect defendants by eliminating stale claims."

Lozano v. Montoya Alvarez, 572 U.S. 1, 14, (2014) (internal quotations omitted). Businesses using biometric technology, whether for timekeeping purposes to ensure their employees are paid properly or to make consumer transactions more secure, are entitled to the "security and stability to human affairs" that are "vital to the welfare of society" and should not be "surprise[d] through the revival of claims that have been allowed to slumber." *Gabelli v. SEC*, 568 U.S. 442, 448, 449 (2013). The appellate court's decision unfairly forces Privacy Act defendants to litigate claims over alleged violations that occurred long ago—even though no actual harm ever resulted from them.

Extending the statute of limitations comes with real costs. Privacy Act lawsuits are time-consuming, expensive to litigate, and potentially ruinous. Privacy Act lawsuits have reached nearly every major sector of the Illinois economy, including healthcare, technology, transportation, manufacturing, and retail. Class action lawsuits, in particular, inherently carry heavy discovery costs, and the threat of that financial burden alone can be enough to force a Privacy Act defendant to settle, regardless of the merits of the case. *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011) ("faced with even a small chance of a devastating loss, defendants will be pressured into settling questionable claims"); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 559 (2007) ("the threat of discovery expense will push cost-conscious defendants to settle even anemic cases before reaching [summary judgment]"). That threat

becomes much more potent when facing larger classes resulting from a longer statute of limitations.

In summary, a one-year statute of limitations would prevent the unintentionally detrimental results occasioned by the onslaught of Privacy Act litigation in our state. Such would enable Illinois businesses to focus on hiring employees, keeping stores and warehouses open, and staying in business, as opposed to litigating expensive class actions.

CONCLUSION

The Court should reverse the decision below and, instead, apply the statute of limitations set forth in Section 13-201 to claims under the Privacy Act.

Dated: March 23, 2022

Respectfully submitted,

ILLINOIS CHAMBER OF COMMERCE

By: */s/ Matthew C. Wolfe*

Melissa A. Siebert (ARDC #6210154)
Matthew C. Wolfe (ARDC #6307345)
Ian M. Hansen (ARDC #6329781)
SHOOK, HARDY & BACON L.L.P.
111 South Wacker Drive, Suite 4700
Chicago, Illinois 60606
(312) 704-7700
masiebert@shb.com
mwolfe@shb.com
ihansen@shb.com

Counsel for Amicus Curiae
Illinois Chamber of Commerce

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 27 pages.

Dated: March 23, 2022 */s/ Matthew C. Wolfe*

NOTICE OF FILING AND CERTIFICATE OF SERVICE

I, Matthew C. Wolfe, an attorney, hereby certify that on **March 23, 2022**, I caused a true and complete copy of the foregoing **BRIEF OF *AMICUS CURIAE* ILLINOIS CHAMBER OF COMMERCE IN SUPPORT OF DEFENDANT-APPELLANT BLACK HORSE CARRIERS, 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)
Catherine T. Mitchell (cmitchell@stephanzouras.com)
STEPHAN ZOURAS, LLP
100 North Riverside Plaza, Suite 2150
Chicago, IL 60606
Attorneys for Appellee Jorome Tims

David M. Schultz (dschultz@hinshawlaw.com)
John P. Ryan (jryan@hinshawlaw.com)
Adam R. Vaught (avaught@hinshawlaw.com)
Louis J. Manetti, Jr. (lmanetti@hinshawlaw.com)
HINSHAW & CULBERTSON LLP
151 North Franklin Street, Suite 2500
Chicago, Illinois 60606
Attorneys for Appellant Black Horse Carriers, Inc.

Under penalties by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certified that the statements set forth in this notice of filing and certificate of service are true and correct.

/s/ Matthew C. Wolfe