No. 123186

IN THE ILLINOIS SUPREME COURT

STACY ROSENBACH, as Mother and Next Friend of Alexander Rosenbach, individually and as the representative of a class of similarly situated persons, Petitioner/Plaintiff, v. SIX FLAGS ENTERTAINMENT CORP. and GREAT AMERICA LLC, Respondents/Defendants.	On Appeal from the Appellate Court of Illinois, Second Judicial District, No. 2-17-317 There on Appeal from the Circuit Court of Lake County, Illinois No. 2016-CH-13 The Hon. Luis A. Berrones, Judge Presiding

Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC) in Support of Petitioner/Plaintiff Urging Reversal

Marc Rotenberg
Alan Butler
Natasha Babazadeh
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave. NW
Suite 200
Washington, D.C. 20009
(202) 483-1140

Adam J. Levitt
Amy E. Keller
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
(312) 214-7900

Counsel for Amicus Curiae

July 5, 2018
Re-filed July 11, 2018

E-FILED
7/19/2018 1:30 PM
Carolyn Taft Grosboll
SUPREME COURT CLERK

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

TABLE OF AUTHORITIES iii

INTEREST OF THE AMICUS 1

SUMMARY OF ARGUMENT 4

ARGUMENT 4

I. Biometric information, which is uniquely personal data, is the target of hackers and identity thieves. 6

II. Strict application of BIPA is necessary to limit unlawful collection of biometric information. 13

CONCLUSION 20

TABLE OF AUTHORITIES

CASES

ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) 17

Eichenberger v. ESPN, 876 F.3d 979 (9th Cir. 2017) 18

FEC v. Akins, 524 U.S. 11 (1998) 18

In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003) 16

Lawlor v. North American Corp. of Illinois, 983 N.E.2d 414 (Ill. 2012) 17

Morris v. Harvey Cycle and Camper, Inc., 911 N.E.2d 1049 (Ill. App. Ct. 2009) 19

Perry v. CNN, 854 F.3d 1336 (11th Cir. 2017) 18

Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618, 623 (7th Cir. 2014) 18

Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996) 16

STATUTES

11 Del. C. Ann. § 2401(1) 17

18 Pa. Cons. Stat. § 5702 (2017) 16

18 U.S.C. § 2511 16

18 U.S.C. § 2701 16

18 U.S.C. § 2707 16

18 U.S.C. § 2710 ..... 17, 18

815 Ill. Comp. Stat. 505 / 2RR (2012) 19

Biometric Information Privacy Act, 740 ILCS 14/ 5

BIPA 14/5(c) 5

BIPA 14/5(d) 5

BIPA 14/5(e) 5

BIPA 14/5(g) 6

S.C. R. Crim. P. §17-30-15 17

OTHER AUTHORITIES

Aadhaar, *Unique Identification Authority of India* (June 30, 2018) 9

About Aadhaar (2018) 9

Banco Bilbao Vizcaya Argentaria, *BBVA, the First Bank with Access to Its Mobile App via Iris Scanning, Thanks to Samsung* (Nov. 16, 2017) 13

Comments of EPIC, *In re: FACT Act Biometric Study*, Treas. No. R411005 (Apr. 1, 2004) 3

Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 So. Cal. L. Rev. 241 (2007) 12, 14, 15

EPIC, *Bankruptcy of Verified Identity Pass and the Privacy of Clear Registered Traveler Data* (2018) 11, 12

EPIC, *Biometric Identifiers* (2018) 3

EPIC, *Theme Parks and Your Privacy* (2018) 1

Illinois House Transcript, 2008 Reg. Sess. No. 276 (statement of Illinois state Rep. Kathy Ryg) 19, 20

Isaac Ehrlich & Richard A. Posner, *An Economic Analysis of Legal Rulemaking*, 3 J. Legal Stud. 257 (1974) 16

Israel: Police Looking at Chareidim In Theft Of Population Database, Yeshiva World (Oct. 24, 2011) 10

Mastercard, *Mastercard Biometric Card* (2018) 12

Nat'l Res. Council, Nat'l Academies, *Biometric Recognition* (Joseph N. Pato & Lynette I. Millett, eds. 2010). 7

OPM: Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform, 114th Cong. (2015) 7

Press Release, Nat'l Academies of Sci., Engineering, & Medicine (Sept. 24, 2010) 6

Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018) 9

Restatement (Second) of Torts § 163 (1965) 15

Restatement (Second) of Torts § 652B cmt. b (1977)..... 17

Statement of Sam Schumach, Press Secretary, U.S. Off. of Personnel Mgmt.,on Background Investigations Incident (Sept. 23, 2015) 8

Tomer Zarchin, *Authorities Find Source That Leaked Every Israeli's Personal Information Online*, Haaretz (Oct. 24, 2011) 10

U.S. Dep't of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* XX-XXIII (1973) 14

U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018)..... 7

Unique Identification Authority of India, *Use of Aadhaar* (2018)..... 10

INTEREST OF THE AMICUS

In 2005, the Electronic Privacy Information Center ("EPIC") first identified the risk to privacy resulting from the collection of biometric data at amusement parks in the United States. EPIC, *Theme Parks and Your Privacy* (2018).[1] EPIC noted that it is disproportionate and unnecessary for theme parks to collect biometric identifiers from attendees. At the very least, EPIC explained, "Theme park visitors should have knowledge of the practice of collecting fingerprint information so they may act to protect their privacy and their children's privacy." *Id*. EPIC further stated, "Knowing as much as possible whenever personally identifiable information is being collected from you or your family is your best defense. It is not in your privacy interest to fail to ask questions or challenge requests for personally identifiable information. It is important to ask questions and assert your right to protect you and your children's privacy." *Id*.

The State of Illinois subsequently enacted the Illinois Biometric Information Privacy Act to establish safeguards for the collection of biometric data, including specific requirements for the collection of this information. Now before this Court is a person whose child's biometric data was unlawfully obtained in violation of the Act. EPIC has submitted many

[1] *Available at* https://epic.org/privacy/themepark/.

amicus briefs in federal and state courts concerning emerging privacy issues, including four briefs for the U.S. Supreme Court during the past term, and a brief in the D.C. Circuit concerning the massive OPM data breach, that included the compromise of 5.1 million fingerprints, precisely the same digital data gathered by Six Flags. *See* Br. of *Amici Curiae* EPIC et al., *Carpenter v. United States*, No. 16-402 (June 22, 2018); Br. of *Amici Curiae* EPIC et al., *Byrd v. United States*, 138 S. Ct. 1318 (2018) (No. 16-1371); Br. of *Amicus Curiae* EPIC, *Dahda v. United States*, 138 S. Ct. 1491 (2018) (No. 17-43); Br. of *Amici Curiae* EPIC et al., *Microsoft v. United States*, 138 S. Ct. 1186 (2018) (No. 17-2); Br. of *Amici Curiae* EPIC et al., *In re OPM Data Security Breach Litigation*, 266 F. Supp. 3d 1 (D.D.C. 2017), *appeal docketed*, No. 17-5217 (D.C. Cir. Sept. 27, 2017). This case is of particular concern. If companies are allowed to collect biometric information on children in violation of the Illinois law, then the cornerstone of the Act will be gone, and the statute will quickly collapse.

EPIC has long advocated for strict limits on use of biometric data. Biometric data is personally identifiable information that cannot be changed, even if compromised. Improper collection of this information can contribute to identity theft, inaccurate identifications, and infringement on

constitutional rights. *See* EPIC, *Biometric Identifiers* (2018);[2] Comments of EPIC, *In re: FACT Act Biometric Study*, Treas. No. R411005 (Apr. 1, 2004).[3] Strict limits on collection of biometric data is the best practice to prevent abuse. *See, e.g.*, Br. of *Amici Curiae* EPIC et al., *In re OPM*, *supra* (arguing that the constitutional right to informational limits the personal data that federal agencies may collect); Br. of *Amicus Curiae* EPIC, *Attias v. Carefirst*, Inc., 865 F.3d 620 (D.C. Cir. 2017) (No. 16-7108) (arguing that courts should not limit consumers ability to seek redress when their social security numbers have been breached); Br. of *Amicus Curiae* EPIC, *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359 (M.D. Penn. 2015), *appeal docketed*, No. 15-3690 (3d Cir. Nov. 6, 2015) (arguing that breaches of SSNs and other identifiers create a substantial risk of fraud and identity theft).

[2] *Available at* https://epic.org/privacy/biometrics/.
[3] *Available at* https://www.epic.org/privacy/biometrics/factabiometrics.html.

SUMMARY OF ARGUMENT[4]

There is no requirement that companies collect and store biometric identifiers, such as fingerprints, from young children. Companies that choose to collect this sensitive personal data of Illinois residents are subject to the Illinois Biometric Information Privacy Act. The Act recognizes the unique threats associated with the collection of biometric identifiers—over 5 million digital fingerprint records were stolen from the Office of Personnel Management in 2015—and sets out clear limitations on companies' collection of this data. And when a company has failed to follow these explicit requirements prior to collection of this uniquely personal data, it should be unnecessary for a consumer to prove they have suffered an *additional* harm before they can enforce their rights under the Act. In these circumstances, judicial second-guessing of legislative determinations will come at an enormous cost to Illinois residents.

ARGUMENT

The Illinois Biometric Information Privacy Act ("BIPA") imposes clear responsibilities on any private entity that collects or possesses biometric identifiers. This includes strict limitations on not only disclosure

[4] EPIC would like to thank its Summer 2018 Clerks, Allison Gilley, Sherry Safavi, and F. Mario Trujillo, for their assistance in preparing this brief.

of that data, but also on collection. In particular, the law prohibits collection of biometric information absent (1) disclosure in writing notifying the data subject of the collection, (2) disclosure in writing detailing both the "specific purpose" and "length of term" for which the data will be "collected, stored, and used," and (3) obtaining a "written release" from the data subject. Biometric Information Privacy Act, 740 ILCS 14/15 ("BIPA"). The Illinois legislature made clear the purpose of the Act:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

BIPA 14/5(c). Reflecting widespread public concern at the time of enactment, the legislature found that "[a]n overwhelming majority of members of the public are wary of the use of biometrics when such information is tied to finances and other personal information," and are "deterred from partaking in biometric identifier-facilitated transactions." BIPA 14/5(d), (e). And the legislature made clear that the act of collection was explicitly regulated:

> 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.

BIPA 14/5(g).

Strict enforcement of these rules is necessary to ensure that unlawful collection and retention do not occur, and that individuals' identities are not put at risk.

I. Biometric information, which is uniquely personal data, is the target of hackers and identity thieves.

The collection of biometric information raises profound concerns about privacy, safety and security. A report by the National Academy of Sciences found that the technique was "inherently fallible" and recommended strict control of biometric data:

> careful consideration is needed when using biometric recognition as a component of an overall security system. The merits and risks of biometric recognition relative to other identification and authentication technologies should be considered. Any biometric system selected for security purposes should undergo thorough threat assessments to determine its vulnerabilities to deliberate attacks. Trustworthiness of the biometric recognition process cannot rely on secrecy of data, since an individual's biometric traits can be publicly known or accessed. In addition, secondary screening procedures that are used in the event of a system failure should be just as well-designed as primary systems.

Press Release, Nat'l Academies of Sci., Engineering, & Medicine (Sept. 24, 2010). The National Academy emphasized in particular the risk of unregulated collection of biometric data, stating that "privacy protections required to facilitate data collection from and about biometric systems need

to be clearly established." Nat'l Res. Council, Nat'l Academies, *Biometric Recognition* 136 (Joseph N. Pato & Lynette I. Millett, eds. 2010).

But in many parts of the country, the call from the National Academies has gone unheeded. In 2015, a data breach at the United States Office of Personnel Management (OPM) exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018).[5] The records breached included the Standard Form 86, completed by those seeking national security positions, and over five million digitized fingerprints, collected precisely for the purpose of authenticating identity. As a result of the breach, the risks of identity theft, financial fraud, and extortion faced by federal employees and others have increased significantly. The Chairman of the House Committee on Oversight and Government Reform noted during his investigation this may have been "the most devastating cyber attack in our Nation's history." *OPM: Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (2015).[6]

[5] *Available at* https://www.opm.gov/cybersecurity/cybersecurity-incidents.
[6] *Available at* https://oversight.house.gov/wp-content/uploads/2015/06/2015-06-16-FC-OPM-Data-Breach.GO167000.pdf.

The breach of fingerprint data held by OPM was especially damaging, as the agency itself conceded. *See* Statement of Sam Schumach, Press Secretary, U.S. Off. of Personnel Mgmt., on Background Investigations Incident (Sept. 23, 2015).[7] In the immediate aftermath of the breach, OPM could not accurately estimate how many biometric identity records had been compromised. Their first estimate was that fingerprint data from "approximately 1.1 million" individuals had been breached, but they later discovered that estimate was woefully inadequate. *Id*. Their subsequent assessment found that approximately 5.6 million individuals' fingerprints were compromised. The agency acknowledged that the likelihood this data will be misused "could change over time as technology advances." *Id*. The OPM left unsaid the obvious point—the risk of misuse of fingerprint data will increase over time if fingerprints become a routine method of authentication, not only for sensitive accounts but remarkably for access to theme parks in the United States.

The risks of improper collection of biometric data are not unique to the United States. Hackers and identity thieves have also targeted Aadhaar, the largest biometric database in the world. Vidhi Doshi, *A Security Breach*

[7] *Available at* https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

in India Has Left a Billion People at Risk of Identity Theft, The Washington Post (Jan.4, 2018). [8] In 2018, an Indian newspaper reported that the information housed in India's national ID database, Aadhaar, was available for purchase for less than $8 and in as little as ten minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018).[9] There was even an option for third parties to print an Aadhaar card for any enrolled individual. *Id.* The Aadhaar database contains the personal and biometric information, including fingerprints, iris scans, and a facial photograph, Unique Identification Authority of India of over a billion Indian citizens. *About Aadhaar* (2018);[10] Aadhaar, *Unique Identification Authority of India* (June 30, 2018).[11] An Aadhaar breach has far-reaching implications as Aadhaar cards and related personal information are used by citizens in almost every aspect of daily life. Indians use Aadhaar when accessing publicly distributed food, in various employment and

[8] *Available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.
[9] *Available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.
[10] *Available at* https://uidai.gov.in/your-aadhaar/about-aadhaar.html.
[11] *Available at* https://uidai.gov.in/images/state-wise-aadhaar-saturation.pdf.

education programs, and for social security purposes. Unique Identification Authority of India, *Use of Aadhaar* (2018).[12]

Also, in 2006 the Israel Welfare Ministry's Population Registry was breached and the personal and familial information of over nine million Israeli citizens was exposed. Tomer Zarchin, *Authorities Find Source That Leaked Every Israeli's Personal Information Online*, Haaretz (Oct. 24, 2011).[13] Soon after the breach, the citizens' personal information was found for sale on criminal websites; this personal data included identification numbers and the identities of familial relations. *Id.* Israeli law enforcement attempted to find and delete online copies of the registry but only six people were arrested. *Id.* The Israeli breach illustrates the ease with which sensitive information can be disseminated amongst malicious actors and the relative powerlessness of law enforcement in regaining control over it. At the same time that this breach was uncovered, government officials in Israel were proposing to create a biometric database. *See Israel: Police Looking at Chareidim In Theft Of Population Database*, Yeshiva World (Oct. 24, 2011).[14] As opponents of the biometric database pointed out at that time, a

[12] *Available at* https://uidai.gov.in/your-aadhaar/faqs.html.
[13] *Available at* https://www.haaretz.com/1.5203015.
[14] *Available at* https://www.theyeshivaworld.com/news/headlines-breaking-stories/106550/israel-police-looking-at-chareidim-in-theft-of-population-database.html.

breach of the biometric database would be "far more catastrophic" than the breach of the population registry. *Id.*

Biometric information is at risk from the moment it is collected. The constant threat of a data breach is not the only risk that consumers face; companies that collect consumers' sensitive data might also sell that data like any other business asset. For example, Verified Identity Pass, Inc., the company whose service "Clear" is used by airport travelers to bypass Transportation Security Administration (TSA) screening at certain airports, collects biometric information from each of its users (including fingerprints and retinal scans). *See* EPIC, *Bankruptcy of Verified Identity Pass and the Privacy of Clear Registered Traveler Data* (2018).[15] The company lost control of sensitive data when an unencrypted laptop housing the personal information of 33,000 customers and applicants was stolen from a Clear office at the San Francisco Airport. *Id.* The at-risk data included names, addresses and birth dates, as well as some driver's license numbers and passport information. *Id.*[16] Verified Identity Pass declared bankruptcy in 2009, and given the sensitivity of the biometric data—including fingerprints

[15] *Available at* https://www.epic.org/privacy/airtravel/clear/.
[16] The stolen laptop was ultimately recovered, and the TSA conducted a review of the impact of the breach, but never released the results.

and retinal scans—the company promised to delete the biometric identifiers. Ryan Singel, *Clear Promises to Delete Sensitive Flier Data, But No Refunds*, Wired (Jun. 23, 2009).[17]

Experts have noted that "strict liability creates an incentive for actors engaging in ultrahazardous activities to 'cut back on the scale of the activity…to slow its spread while more is learned about conducting it safely." Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 So. Cal. L. Rev. 241, 266 (2007). Collecting biometric data is such an activity. Not only have the risks of breach increased, but the consequences of a breach of biometric data are severe. Many private companies already use biometrics for identification and authentication to access sensitive systems, including financial accounts and personal devices. *Id.* at 243. For example, Mastercard is developing a bank card that can be authenticated using a built-in biometric fingerprint scanner. Mastercard, *Mastercard Biometric Card* (2018).[18] Other financial institutions have begun using iris scanning to authenticate users in their mobile banking apps. Banco Bilbao Vizcaya Argentaria, *BBVA, the*

[17] *Available at* https://www.wired.com/2009/06/where-will-registered-traveler-fingerprints-go-its-un-clear/.
[18] *Available at* https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html.

First Bank with Access to Its Mobile App via Iris Scanning, Thanks to Samsung (Nov. 16, 2017).[19] Users can login without a password simply by looking at their phone. *Id.*

The rise in data breaches of biometric data and the increasing use of biometric identifiers for authentication makes clear the importance of following the recommendations of the National Academies. "The privacy protections required to facilitate data collection from and about biometric systems need to be clearly established." Nat'l Res. Council, Nat'l Academies, *supra*.

II. Strict application of BIPA is necessary to limit unlawful collection of biometric information.

Federal and state privacy laws have long recognized harms that stem from unlawful collection of sensitive personal data. Privacy laws impose strict obligations on data collectors to ensure that consumers do not bear the costs associated with the misuse of their personal information. To ensure compliance with these restrictions, privacy laws typically impose liability on any business that violates its statutory obligations. BIPA follows this tradition. Like other privacy laws, BIPA does not require a consumer to prove special damages to state a claim. Such a requirement would frustrate

[19] *Available at* https://www.bbva.com/en/bbva-first-bank-access-mobile-app-iris-scanning-thanks-samsung.

the purposes of the Act and make companies less likely to protect the data they collect.

Privacy laws give individuals control over their personal information and seek to protect that information by imposing strict limits on collection, use, and disclosure. *See* U.S. Dep't of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* XX-XXIII, at 40-44 (1973). These laws are not only meant to protect against pecuniary harm, but also to "eliminate misunderstanding, mistrust, frustration, and seeming unfairness." *Id.* at 46. The prohibition on collection (absent certain safeguards) in BIPA serves a similar purpose because it ensures that consumers will not be subject to collection of their biometric information without their knowledge and consent.

Consumers' right to control the flow of their biometric information also creates a prophylactic protection against data breaches, internal business misuse, unwanted secondary use, and government access. Modern privacy laws, including BIPA, address the most significant threat in the Information Age, "the release of sensitive personal information from computer databases into the hands of identity predators and corporate thieves." Citron, *supra*, at 243.

A private entity that chooses to collect biometric information in violation of BIPA should not be allowed to ignore its legal obligations. If that were the case, then any person caught speeding could simply argue to the officer they shouldn't be ticketed because they did not harm any pedestrians. BIPA seeks both to establish best practices for the use of biometric data, such as meaningful consent at the time of collection, and deter practices that place individuals at risk. The deterrence effect of a law like BIPA would be miniscule if private entities knew that they could only be held liable in the rare case where a victim can prove downstream harm.

Privacy laws incentivize businesses to limit collection of sensitive information and to therefore limit the risk of a breach. *See* Citron, *supra*, at 283–87 (discussing the "efficient deterrence" theory of liability as applied to entities collecting sensitive information). Similar per se liability rules are already found in the fields of trespass law and automobile speed limit infractions. *See* Restatement (Second) of Torts § 163 (1965) ("One who intentionally enters land in the possession of another is subject to liability to the possessor for a trespass, although his presence on the land causes no harm to the land, its possessor, or to any thing or person in whose security the possessor has a legally protected interest."); *see also* Isaac Ehrlich & Richard A. Posner, *An Economic Analysis of Legal Rulemaking*, 3 J. Legal

Stud. 257, 257 (1974) ("If we want to prevent driving at excessive speeds, one approach is to post specific speed limits and to declare it unlawful per se to exceed those limits.").

Privacy laws also limit collection of private communications and sensitive personal information because the unauthorized collection of such data, in and of itself, is a privacy harm. For example, the federal Wiretap Act prohibits the interception of calls, e-mails, and other communications, 18 U.S.C. § 2511, and the Stored Communications Act prohibits unauthorized access to e-mail and other stored data, 18 U.S.C. § 2701. These laws, like BIPA, give a private right of action to any individual whose communications have been intercepted, *Id*. § 2520(a), or who has been "aggrieved by any violation" of the SCA, *Id*. § 2707(a). *See also In re Pharmatrak, Inc.*, 329 F.3d 9, 12 (1st Cir. 2003). An entity can, for example, be held liable under those provisions for the unlawful collection of stored communications. *See Tucker v. Waddell*, 83 F.3d 688, 693 (4th Cir. 1996). Corresponding state wiretap laws similarly define "aggrieved person" as anyone whose communications were intercepted —or collected, requiring no further showing of harm. *See, e.g.*, 18 Pa. Cons. Stat. § 5702 (2017) (defining "aggrieved person" as "a person who was a party to any intercepted wire, electronic or oral communication or a person against whom the interception

was directed"); 11 Del. C. Ann. § 2401(1) (same); S.C. R. Crim. P. §17-30-15 (same).

The common law privacy tort of intrusion upon seclusion also prohibits the unauthorized collection of sensitive personal information. *See Lawlor v. North American Corp. of Illinois*, 983 N.E.2d 414, 425 (Ill. 2012); Restatement (Second) of Torts § 652B cmt. b, at 378–79 (1977) ("The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the. . . information outlined."). Similarly, in the Fourth Amendment context, courts have found that the mere unauthorized collection of metadata, by itself, creates a concrete privacy injury. *See ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (finding standing because "appellants challenge the telephone metadata program as a whole, alleging injury from the very collection of their telephone metadata").

Courts have held that other privacy laws with liability provisions similar to BIPA authorize broad liability for violations. The Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710, which prohibits the unauthorized disclosure of personally identifiable information of video rental customers has a right of action provision that is nearly identical to the section at issue in BIPA. The VPPA provides that "[a]ny person aggrieved by any act of a

person in violation of this section may bring a civil action in United States district court." *Id*. § 2710(c)(1). Courts have found this provision empowers any individual to bring suit against a company that violated their rights under the VPPA. *See Perry v. CNN*, 854 F.3d 1336 (11th Cir. 2017); *Sterk v. Redbox Automated Retail, LLC*, 770 F.3d 618, 623 (7th Cir. 2014). The Supreme Court has held that "[h]istory associates the word 'aggrieved' with a congressional intent to cast the standing net broadly." *FEC v. Akins*, 524 U.S. 11, 19 (1998) (interpreting a provision in the Federal Election Campaign Act similar to the section at issue in BIPA). The Ninth Circuit recently rejected a defendant's argument that the "aggrieved" provision in the VPPA "requires a showing of additional harm and that, without such a showing, a consumer does not have standing." *Eichenberger v. ESPN*, 876 F.3d 979, 983 (9th Cir. 2017). The court in *Eichenberger* flatly rejected that argument, citing the Supreme Court's broad reading of aggrieved in *Akins*. *Id*.

The legislators who enacted BIPA included in the liability provision the same broad language seen in other privacy statutes. And had they intended to limit the availability of civil liability to a narrower subset of plaintiffs, they would have included limiting language in the statute. For example, the Illinois Consumer Fraud and Deceptive Business Practices Act,

which prohibits a company from collecting a consumer's social security number over an unsecure Internet connection, 815 Ill. Comp. Stat. 505/2RR (2012), limits relief to those who have suffered "actual damages." *See Morris v. Harvey Cycle and Camper, Inc.*, 911 N.E.2d 1049, 1054 (Ill. App. Ct. 2009).

Given the purpose of privacy laws and the structure of the BIPA enforcement provision, this Court should recognize that an "aggrieved party" is any consumer whose biometric information was collected in violation of the statutory requirement. This interpretation of "aggrieved" is consistent with the legislatures findings in BIPA that individuals are "wary" of biometric collection and can "deterred from partaking" in transactions that involve the collection of biometric information absent strict safeguards.

The legislative history of BIPA suggests that an individual whose fingerprints were unlawfully collected is precisely the type of person who is entitled to bring suit. The Illinois legislature passed BIPA after the controversy spurred by the bankruptcy of a fingerprint scanning company, Pay By Touch. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276 (statement of Illinois state Rep. Kathy Ryg). The sponsor of BIPA specifically referenced the questions raised by the Pay By Touch bankruptcy, noting that residents were "wondering what will become of their

biometric and financial data." *Id.* The lawmakers recognized that it was necessary to impose strict collection restrictions to limit the amount of data that could be misused, resold, or breached.

* * *

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

CONCLUSION

EPIC respectfully requests that this Court reverse the lower court's judgment and remand the case for further consideration.

July 5, 2018
Re-filed July 11, 2018

Respectfully submitted,

/s/ Adam J. Levitt

Adam J. Levitt (A.R.D.C. No. 6216433)
Amy E. Keller (A.R.D.C. No. 6296902
DiCello Levitt & Casey LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
(312) 214-7900
alevitt@dlcfirm.com
akeller@dlcfirm.com

/s/ Alan Butler
Marc Rotenberg
Alan Butler (A.R.D.C. No. 6328985)
Natasha Babazadeh
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org
butler@epic.org
babazadeh@epic.org

Counsel for Amicus Curiae

RULE 341(c) CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Supreme Court Rules 345(b) and 341(a) and (b). The length of this brief, excluding the pages containing the Rule 341(d) cover, the Rule 341(h)(1) statement of points and authorities, the Rule 341(c) certificate of compliance, and the certificate of service, is 20 pages.

/s/ Adam J. Levitt
Adam J. Levitt

Dated: July 11, 2018

E-FILED
7/19/2018 1:30 PM
Carolyn Taft Grosboll
SUPREME COURT CLERK