No. 18-15982

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

In re Facebook, Inc. Biometric Information Privacy Litigation

CARLO LICATA, NIMESH PATEL & ADAM PEZEN,
Individually and on behalf of all others similarly situated,
Plaintiffs-Appellees,

v.

FACEBOOK, INC.,
Defendant-Appellant.

On appeal from the United States District Court
for the Northern District of California
No. 3:15-cv-03747-JD

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PLAINTIFFS-APPELLEES

MARC ROTENBERG
ALAN BUTLER
JOHN DAVISSON
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org
Counsel for Amicus Curiae

December 17, 2018

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c) and Local Rule 26.1, *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. No publicly held company has a direct financial interest in the outcome of this litigation by reason of a franchise, lease, other profit sharing agreement, insurance, or indemnity agreement.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Other Authorities

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy issues.[1] EPIC routinely participates as *amicus curiae* in federal cases concerning a plaintiff's standing to sue over the invasion of a privacy right. *See, e.g.*, Br. *Amici Curiae* EPIC et al., *In re OPM Data Security Breach Litigation*, No. 17-5217 (D.C. Cir. May 17, 2018); Br. *Amicus Curiae* EPIC, *Attias v. Carefirst*, 865 F.3d 620 (D.C. Cir. 2017) (No. 16-7108); Br. *Amici Curiae* EPIC et al., *Spokeo v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339). EPIC also submitted an *amicus* brief in the Illinois Supreme Court concerning the interpretation of the term "aggrieved" in the Illinois Biometric Information Privacy Act ("BIPA"). Br. *Amicus Curiae* EPIC, *Rosenbach v. Six Flags Entm't Corp.*, No. 123186 (Ill. July 5, 2018).

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, financial fraud, warrantless surveillance, and infringement on constitutional

[1] The parties consent to the filing of this *amicus curiae* brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

rights. *See* EPIC, *Biometric Identifiers* (2018);[2] Comments of EPIC, *In re: FACT Act Biometric Study*, Treas. No. R411005 (Apr. 1, 2004).[3] Placing strict limits on the collection of biometric data is the best practice to prevent abuse. *See, e.g.*, Br. *Amici Curiae* EPIC et al., *In re OPM*, No. 17-5217 (arguing that the constitutional right to informational privacy limits the personal data that federal agencies may collect); Br. *Amicus Curiae* EPIC, *Attias*, 865 F.3d 620 (arguing that courts should not limit consumers' ability to seek redress when their social security numbers are subject to a data breach); Br. *Amicus Curiae* EPIC, *Storm v. Paytime, Inc.*, No. 15-3690 (3d Cir. Apr. 18, 2016) (arguing that breaches of social security numbers and other identifiers create a substantial risk of fraud and identity theft).

EPIC has also focused public attention on Facebook's privacy practices and Facebook's use of facial recognition software. *See* EPIC, *Facebook Privacy*.[4] In 2011, EPIC and other consumer protection groups filed a complaint with the FTC about Facebook's face identifying software. Complaint, Request for Investigation, Injunction, Other Relief, *In re Facebook, Inc., and the Facial Identification of Users* (2011). In 2018, EPIC again warned the FTC about Facebook's use of facial recognition software and about the agency's failure to enforce its 2011 Facebook

[2] https://epic.org/privacy/biometrics/.
[3] https://www.epic.org/privacy/biometrics/factabiometrics.html.
[4] https://www.epic.org/privacy/facebook/.

consent order. Complaint, Request for Investigation, Injunction, and Other Relief, *In re Facebook, Inc., and Facial Recognition* (2018).

SUMMARY OF THE ARGUMENT

While "injury" and "harm" may be synonyms in everyday speech, the terms represent distinct concepts in law. Defendants in privacy cases have long conflated the terms in an attempt to confuse and persuade courts that injury, for purposes of Article III standing, also requires a showing of consequential harm. This argument ignores the well-established legal definitions of the terms and the Supreme Court's decision in *Spokeo v. Robins,* which made clear that a violation of a concrete and particularized legal right establishes legal injury, irrespective of any harm that may follow. There are many statutory and common law rights that require only a showing of a legal violation to establish standing. Article III simply requires plaintiffs to demonstrate that a defendant has invaded a concrete interest protected by the law—nothing more.

The Illinois Biometric Information Privacy Act imposes, by statute, legal obligations on companies that choose to collect and store individuals' biometric data. The Act recognizes the unique risks associated with the collection of biometric identifiers—including the risks and repercussions of theft, unauthorized use, and unauthorized disclosure—and sets out clear limitations on companies' collection of this data. When a company violates individuals' BIPA rights by

failing to obtain consent prior to collecting their biometric data, the company invades their legally protected interests, causing injury-in-fact—*legal injury*. If the injury is tied to the company's conduct and redressable by the court, it is unnecessary for a consumer to prove they have suffered an *additional* harm before they can enforce their rights under the Act. Judicial second-guessing of statutory protections for biometric data established by the state legislature, following a careful weighing of the public safety concerns, will come at an enormous cost to the privacy of Illinois residents.

ARGUMENT

Article III grants the federal courts "judicial power" over "cases" and "controversies." U.S. Const. art. III § 2. The Supreme Court has interpreted this to embody the "fundamental" principle that "federal-court jurisdiction" is limited "to actual cases or controversies." *Spokeo, Inc. v. Robins ("Spokeo I")*, 136 S. Ct. 1540, 1547 (2016). To effectuate this principle, the Court established the standing doctrine with its "injury-in-fact" requirement. *Id*. The standing doctrine helps ensure that in actions against the government, plaintiffs satisfy the requirements of Article III. *See, e.g*., *Lujan v. Def's of Wildlife,* 504 U.S. 555 (1992). But standing was never understood to limit the ability of private plaintiffs to seek redress against private defendants for otherwise-valid claims arising under federal law or for state and common law claims under ancillary or diversity jurisdiction. *See Spokeo I*, 136

S. Ct. at 1550–52 (Thomas, J., concurring) ("In a suit for the violation of a private right, courts historically presumed that the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded.").

Standing serves "to prevent the judicial process from being used to usurp the powers of the political branches," *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1146 (2013), and "confines the federal courts to a properly judicial role," *Spokeo I*, 136 S. Ct. at 1547. Standing also ensures the plaintiff has "such a personal stake in the outcome of the controversy as to warrant his invocation of federal-court jurisdiction." *Warth v. Seldin*, 422 U.S. 490, 498 (1975) (internal quotation marks omitted).

The statute at issue in this case, the Illinois Biometric Information Privacy Act, imposes clear obligations on any private entity that collects or possesses biometric identifiers. This includes limitations on both the collection and disclosure of biometric data. In particular, the law prohibits collection of biometric information absent (1) notification writing to the data subject of the collection; (2) notification in writing detailing both the "specific purpose" and "length of term" for which the data will be "collected, stored, and used"; and (3) a "written release" from the data subject. BIPA, 740 ILCS 14/15. Many courts have recognized that the violation of a legal right against the collection of personally identifiable information—such as the rights granted by BIPA—is sufficient to establish

standing under Article III. *See, e.g.*, *Heglund v. Aitken County*, 871 F.3d 572, 577 (8th Cir. 2017) (finding plaintiff had standing to sue under the DPPA because "[a]n individual's control of information concerning her person . . . was a cognizable interest at common law"); *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"). Strict enforcement of these rights is necessary to ensure that unlawful collection and retention do not occur, and that individuals' identities are not put at risk. Such rights and injuries are also similar to other rights and injuries recognized at common law.

In this case, Plaintiffs have alleged that Facebook violated their right to control their biometric data by collecting their "face templates" without obtaining prior consent or even disclosing the fact that it had collected this information. Consol. Class Action Compl. ¶¶ 21–52 (Aug. 28, 2015). The lower court was right to find that "[a] violation of the BIPA notice and consent procedures infringes the very privacy rights the Illinois legislature sought to protect by enacting BIPA. That is quintessentially an intangible harm that constitutes a concrete injury in fact." Order re Renewed Mot. Dismiss, Dkt. 227, at 6 (citing *Robins v. Spokeo, Inc. ("Spokeo II")*, 867 F.3d 1108, 1113 (9th Cir. 2017)). The lower court's decision should be affirmed.

I. Article III does not require plaintiffs to prove consequential harm to establish standing.

"Injury is the illegal invasion of a legal right; damage is the loss, hurt, or harm that results from the injury." 22 Am. Jur. 2d *Damages* § 2 (2018). Despite this clear and important distinction, courts across the United States routinely conflate injury-in-fact and consequential harm in their analysis of standing. This occurs frequently in privacy cases, where many defendants have exploited this semantic trick to avoid consideration of plaintiffs' claims on the merits.[5] Not only is this analysis wrong as a matter of law; the conflation has led to increasing confusion about the necessary requirements to bring a lawsuit in federal court.

Article III requires only that a plaintiff allege (1) an injury-in-fact (2) tied to defendant's conduct that is (3) redressable by the court. Injury-in-fact, *legal injury*, consists of an "*invasion* of a legally protected interest" that is (1) "concrete and particularized" and (2) "actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560 (emphasis added). When the law protects an interest, the law grants the owner of that interest a right. A right is a "legally enforceable claim that another will do or will not do a given act." *Right*, Black's Law Dictionary.

[5] In common English, the terms "injury" and "harm" are considered synonyms. Webster's Pocket Thesaurus of the English Language 134 (2001). However, in the legal analysis of standing, the terms are clearly distinguishable. A legal injury is the "violation of another's legal right, for which the law provides a remedy." *Injury*, Black's Law Dictionary (10th ed. 2014). Harm, by contrast, is "material or tangible detriment." *Harm*, *id.*

"[C]reated or recognized by law," *id.*, rights are granted through common law, statutory law, and constitutional law. *Tenn. Elec. Power Co. v. Tenn. Val. Auth.*, 306 U.S. 118, 137 (1939) ("[T]he right invaded is a legal right,—one of property, one arising out of contract, one protected against tortious invasion, or one founded on a statute which confers a privilege.").

The invasion of a right, *i.e.*, a "legal injury," is distinct from the "disadvantage that may flow from" the invasion. *Warth*, 422 U.S. at 503 n.13; *see, e.g.*, *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (finding that "[t]he VPPA [Video Privacy Protection Act] does not protect only against harms such as embarrassment and harassment" but also "privacy interests more generally by ensuring that consumers retain control over their personal information"). "[O]ur contemporary decisions have not required a plaintiff to assert an actual injury beyond the violation of his personal legal rights to satisfy the 'injury-in-fact' requirement." *Spokeo I*, 136 S. Ct. at 1552 (Thomas, J., concurring).

As the Supreme Court explained in *Spokeo I*, there are two ways to show that an intangible injury is concrete. First, an intangible legal injury can be concrete if it "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* at 1549 (using "harm" to refer to the invasion of the plaintiff's legal right). Second, a statute can elevate "concrete, *de facto* injuries that were previously inadequate at

law" to the "status of legally cognizable injuries." *Id.* (internal quotation marks omitted).

Legislatures have "the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before." *Id.* (internal quotation marks omitted). Justice Thomas stated the rule directly in his concurrence: "Congress can create new private rights and authorize private plaintiffs to sue based simply on the violation of those private rights." *Id*. at 1553 (Thomas, J., concurring). As the Court recognized more than four decades ago, "Congress may create a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in the absence of statute." *Warth*, 422 U.S. at 514. State legislatures, such as the Illinois General Assembly, also have "the power to create new interests, the invasion of which may confer standing." *Diamond v. Charles*, 476 U.S. 54, 65 n.17 (1986).

Rights established by legislatures are substantive and are therefore concrete. Indeed, privacy laws protect substantive rights. For example, Congress enacted the Video Privacy Protection Act of 1988, which prevents video service providers from disclosing personally identifiable information about their customers in order "to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials." Pub. L. No. 100-618, 102 Stat. 3195

(codified at 18 U.S.C. § 2710). Congress enacted the Telephone Consumer Protection Act of 1991 because banning nonconsensual "automated or prerecorded telephone calls" was the "only effective means of protecting telephone consumers" from the resulting "nuisance and privacy invasion." Pub. L. No. 102-243, § 2(12), 105 Stat. 2394, 2394–95 (codified at 47 U.S.C. § 227). Federal and state privacy statutes are based on an interconnecting framework of rights and responsibilities known as the Fair Information Practices and provide substantive protections against the misuse of personal data. *See* Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* 760–64 (2016).

Substantive law "creates, defines, and regulates the rights, duties, and powers of parties," while procedural law is "rules that prescribe the steps for having a right or duty judicially enforced." *Substantive Law*, Black's Law Dictionary; *Procedural Law*, Black's Law Dictionary. In other words, "substantive law defines the remedy and the right, while the law of procedure defines the modes and conditions of the application of the one to the other." John Salmond, *Jurisprudence* 476 (Glanville L. Williams ed., 10th ed. 1947); *see Shady Grove Orthopedic Assoc.'s, P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 407 (2010) (stating that procedural rights govern "only the manners and the means by which the litigants' rights are enforced").

But the Supreme Court in *Spokeo I* made clear that a violation of procedural rights also creates legal standing. Writing for the Court, Justice Alito said:

> Just as the common law permitted suit in such instances, the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified. *See Federal Election Comm'n* v. *Akins*, 524 U.S. 11, 20–25 (1998) (confirming that a group of voters' "inability to obtain information" that Congress had decided to make public is a sufficient injury in fact to satisfy Article III); *Public Citizen* v. *Department of Justice*, 491 U. S. 440, 449 (1989) (holding that two advocacy organizations' failure to obtain information subject to disclosure under the Federal Advisory Committee Act "constitutes a sufficiently distinct injury to provide standing to sue").

Spokeo I, 136 S. Ct. at 1549 (emphasis in original).

The Court explained that only a "bare procedural violation, divorced from any concrete harm" fails to confer standing. *Spokeo I*, 136 S. Ct. at 1549. Courts should not presume to second-guess complex laws which establish a legally protected interest. Legislators have likely undertaken extensive fact finding prior to the enactment of a public law, and the provisions of that law, when read together, may confer greater significance than when read in isolation. *See Lujan*, 504 U.S. at 580 (Kennedy, J., concurring in part and concurring in judgment) ("As Government programs and policies become more complex and far reaching, we must be sensitive to the articulation of new rights of action.").

Even in *Spokeo I*, the Court was careful in its discussion of what may constitute a "bare procedural violation." *Spokeo I*, 136 S. Ct. at 1550. In discussing

whether there was any violation of the Fair Credit Reporting Act that might not result in a concrete injury, the Court noted that ‘‘[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.’’ *Id.* at 1550. The Court was correct to add the qualifier "without more." A zip code is routinely used to establish identity, confirm a credit card payment, withdraw money from an ATM machine, and create profiles with legal consequences. *See, e.g.*, Shaunacy Ferro, *What Your Zip Code Says About You*, Fast Company Co. Design (Oct. 24, 2014);[6] Adam Tanner, *Never Give Stores Your ZIP Code. Here's Why*, Forbes (June 19, 2013).[7] Zip codes can also act as proxies for race, wealth, and consumer habits that can affect whether an individual is granted a loan or called in for an interview for a job. Cathy O'Neill, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* 146 (2016). The Court in *Spokeo I* added in a footnote: "We express no view about any other types of false information that may merit similar treatment. We leave that issue for the Ninth Circuit to consider on remand." *Spokeo I*, 136 S. Ct. at 1550 n.8. The caution is well advised. In laws that seek to protect the collection and use of personal data, false and aggregable information about the individual may produce concrete harms.

---

[6] http://www.fastcodesign.com/3037550/infographic-of-the-day/what-your-zip-code-says-about-you.

[7] http://www.forbes.com/sites/adamtanner/2013/06/19/theres-a-billion-reasons-not-to-give-stores-your-zip-code-ever/#3cfe08514e33.

On remand, this Court found that, to determine whether a concrete harm follows from a violation of a statutory right, a court must determine "(1) whether the statutory provisions at issue were established to protect his concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests." *Spokeo II*, 867 F.3d at 1113. This Court found that the inaccuracies in Robins' credit report—age, marital status, educational background, and employment history—were not "meaningless inaccurac[ies]" but rather "the type that may be important to employers or others making use of a consumer report," and thus the type of information the accuracy of which "seems directly and substantially related to FCRA's goals." This Court did not need to inquire further as to whether there was a consequential harm in addition to the legal injury.

II. Unlawful collection of an individual's biometric information in violation of the Illinois BIPA is an invasion of a legal right sufficient to establish a concrete injury under Article III.

This Court in *Eichenberger* recognized a concrete privacy interest in "consumers retain[ing] control over their personal information." *Eichenberger*, 876 F.3d at 983. In enacting BIPA, the Illinois General Assembly recognized that the public is wary not only of the possible disclosure of their biometric data to unauthorized users, but also of the simple *collection* of that data. It is the unlawful collection of biometric data that seizes control of that unique, personal information

from the consumer. Personal data, particularly biometric data, has proven to be an attractive target for identity thieves and foreign adversaries. For example, in the 2015 breach of records at the Office of Personnel Management, more than five million digitized fingerprint files were stolen.

The legislature thus sought to ensure that customers retained control of their biometric data by establishing a prohibition against collection of that data absent knowing consent. BIPA is not alone in recognizing unauthorized collection of data as a concrete injury; other privacy statutes, as well as common law privacy torts and other common law claims, protect similar interests and do not require a showing of consequential harm to establish standing.

A. The Illinois General Assembly created a clear prohibition against unlawful collection of customers' biometric data to protect customers' concrete interest in controlling who has access to their biometric identifiers.

In enacting BIPA, the Illinois General Assembly was not only concerned with disclosure of biometric data, but also with protecting consumers' control of that data. BIPA was passed after a 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). In her floor statement on the bill, BIPA's sponsor 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," *i.e.*, whether the data would be sold

like the company's other assets, who would obtain it, and what they would do with it. *Id.* The language, structure, and purpose of BIPA reflect this concern, creating a clear prohibition against the collection of consumers' biometric information absent knowledge and consent. The Act thus protects consumers' concrete interest in controlling access to their biometric identifiers.

Specifically, BIPA prohibits collection of biometric information absent (1) notification in writing to the data subject of the collection, (2) notification in writing detailing both the "specific purpose" and "length of term" for which the data will be "collected, stored, and used," and (3) a "written release" from the data subject. BIPA 14/15. In enacting BIPA, the Illinois legislature recognized that use of biometrics in commerce creates unique risks:

> 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). 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).

BIPA also contains a liability provision that provides "any person aggrieved by a violation" of the Act with "a right of action" under Illinois state law. BIPA 14/20. Courts have held that other privacy laws with liability provisions similar to BIPA authorize broad liability for violations. The Video Privacy Protection Act, 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 private right of action provision in BIPA. 18 U.S.C. § 2710(c)(1). 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." 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). This Court recently rejected a defendant's argument that the "aggrieved" provision in the VPPA "requires a showing of additional harm," citing the Supreme Court's broad reading of that term in *Akins*. *Eichenberger*, 876 F.3d at 983.

The legislators who enacted BIPA included in the liability provision the same broad language seen in other privacy statutes. Had the Illinois legislature intended to limit the availability of civil liability to a narrower subset of plaintiffs, it 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 & Camper, Inc.*, 911 N.E.2d 1049, 1054 (Ill. App. Ct. 2009).

The Illinois Supreme Court has yet to decide *Rosenbach v. Six Flags*, in which the court is expected to decide the meaning of the term "aggrieved" in BIPA. *Rosenbach v. Six Flags Entm't Corp.*, 2017 IL App (2d) 170317, *pet. granted,* 98 N.E.3d 36 (Ill. 2018). This Court is not bound by any of the Illinois intermediate courts' interpretations of the BIPA provision, *In re Kirkland*, 915 F.2d 1236, 1238 (9th Cir. 1990) ("When interpreting state law, a federal court is bound by the decision of the highest state court"), but it is bound by the Illinois

Supreme Court's broad interpretation of "aggrieved" in another statutory context. *Am. Sur. Co. v. Jones*, 384 Ill. 222, 229-30 (1943) (citing *Glos v. People*, 259 Ill. 332 (1913)) ("A person is prejudiced or aggrieved, in the legal sense, when a legal right in invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment.").

B. A company's collection of biometric data puts unique personal data at heightened risk of theft, unauthorized use, and unauthorized disclosure.

The collection of biometric information presents profound risks to privacy, safety, and security. A report by the National Academy of Sciences on biometric identifiers 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 of 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018).[8] The records breached included over five

[8] https://www.opm.gov/cybersecurity/cybersecurity-incidents.

million digitized fingerprints. *Id*. As a result of the breach, those whose data was stolen face a significantly increased risk of identity theft, financial fraud, and extortion. The Chairman of the House Committee on Oversight and Government Reform noted during his investigation that the OPM data breach 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).[9]

OPM conceded that the breach of fingerprint data was especially damaging. *See* Statement of Sam Schumach, Press Secretary, U.S. Off. of Personnel Mgmt., on Background Investigations Incident (Sept. 23, 2015).[10] In the immediate aftermath of the breach, OPM could not accurately estimate how many biometric identity records had been compromised. OPM's first estimate was that fingerprint data from "approximately 1.1 million" individuals had been breached, but the agency later discovered that estimate was woefully inadequate. *Id*. OPM's 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.

[9] https://oversight.house.gov/wp-content/uploads/2015/06/2015-06-16-FC-OPM-Data-Breach.GO167000.pdf.
[10] https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

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 in India Has Left a Billion People at Risk of Identity Theft*, Wash. Post (Jan.4, 2018).[11] The Aadhaar database contains the personal and biometric information—including fingerprints, iris scans, and a facial photograph—of over a billion Indian citizens. *About Aadhaar* (2018);[12] Unique Identification Authority of India, *Aadhaar* (June 30, 2018).[13] An Aadhaar breach has far-reaching implications: 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 education programs, and for social security purposes. Unique Identification Authority of India, *Use of Aadhaar* (2018).[14] In 2018, an Indian newspaper reported that the information housed in the Aadhaar database 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

[11] 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.
[12] https://uidai.gov.in/your-aadhaar/about-aadhaar.html.
[13] https://uidai.gov.in/images/state-wise-aadhaar-saturation.pdf.
[14] https://uidai.gov.in/your-aadhaar/faqs.html.

Tribune (Jan. 4, 2018).[15] There was even an option for third parties to print an Aadhaar card for any enrolled individual. *Id.*

In 2006, hackers breached the Israel Welfare Ministry's Population Registry, exposing the personal and familial information of over nine million Israeli citizens. Tomer Zarchin, *Authorities Find Source That Leaked Every Israeli's Personal Information Online*, Haaretz (Oct. 24, 2011).[16] Soon after the breach, 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 among 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 proposed creating a biometric database. *See Israel: Police Looking at Chareidim In Theft Of Population Database*, Yeshiva World (Oct. 24, 2011).[17] As opponents of the biometric database pointed out at that time, a breach of the biometric database would be "far more catastrophic" than the breach of the population registry. *Id.*

---

[15] http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.
[16] https://www.haaretz.com/1.5203015.
[17] https://www.theyeshivaworld.com/news/headlines-breaking-stories/106550/israel-police-looking-at-chareidim-in-theft-of-population-database.html.

Biometric information is at risk from the moment it is collected—not only from breach, but also from unauthorized use and sharing. Companies that collect consumers' sensitive data might sell that data like any other business asset. Facebook in particular has come under fire for its commodification of user data and its lax data sharing policies that allow third party apps to obtain and store user data without oversight or even Facebook's awareness. *See, e.g.,* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (Mar. 17, 2018).[18] Just last week, it was revealed that a bug had allowed third party apps to access the private photos of millions of Facebook users. Tony Romm, *Facebook says a new bug allowed apps to access private photos of up to 6.8 million users*, Wash. Post (Dec. 14, 2018).[19] Facebook staff have also discussed not notifying users of a new data collection practice that would be "a pretty high-risk thing to do from a PR perspective." Email from Michael LeBeau (Feb. 4, 2015) (discussing Facebook's plan to upload users' call and text logs from Android phones).[20]

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

[18] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[19] https://www.washingtonpost.com/technology/2018/12/14/facebook-says-new-bug-allowed-apps-access-private-photos-up-million-users.
[20] https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf.

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). The consequences of breach and unauthorized access make clear that prohibitions on collecting biometric data without knowledge or consent—like those in BIPA—must be strictly enforced.

C. Unlawful collection of biometric data is a concrete privacy injury akin to injuries recognized at common law and in federal and state statutes.

Federal and state privacy laws have long recognized concrete injuries 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 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. BIPA's prohibition on the collection of customers' biometric data absent certain safeguards serves a similar purpose because it ensures that consumers get to decide who has access to this unique personal information.

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. Privacy laws incentivize businesses to limit collection of sensitive information and to therefore limit the risk of a breach. *See id*. at 283–87 (discussing the "efficient deterrence" theory of liability as applied to entities collecting sensitive information). 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 could prove downstream harm.

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 concrete privacy injury. 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 ("SCA") 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. N. Am. Corp. of Ill.*, 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 Clapper*, 785 F.3d at 801 (finding standing because "appellants challenge the telephone metadata program as a whole, alleging injury from the very collection of their telephone metadata").

This Court should hold that the unauthorized collection of biometric data in violation of BIPA is a concrete injury that establishes standing under Article III. In *Lujan*, Justice Kennedy warned the courts not to second-guess legislators in areas of increasing complexity. "As Government programs and policies become more

complex and far-reaching, we must be sensitive to the articulation of new rights of action that do not have clear analogs in our common-law tradition." *Lujan*, 504 U.S. at 580 (Kennedy, J., concurring). Courts are not empowered to overrule legislative judgments as to which injuries should be legally protected simply because they are "out of harmony with a particular school of thought." *Williamson v. Lee Optical of Okla., Inc.*, 348 U.S. 483, 488 (1955). The Supreme Court has long rejected the view that the judiciary may "sit as super-legislature to judge the wisdom or desirability of legislative policy determinations[.]" *Metro. Life Ins. Co. v. Ward*, 470 U.S. 869, 901 (1985). If a court demands that a plaintiff prove harm in addition to the concrete injury that legislators have deemed actionable, it is impermissibly "substitut[ing] its own judgment for that of the legislature." *Whole Woman's Health v. Hellerstedt*, 136 S. Ct. 2292, 2310 (2016).

CONCLUSION

Amicus respectfully requests this Court to affirm the lower court's finding that Plaintiffs have standing to sue for violations of BIPA under Article III.

Respectfully submitted,

*/s/ Marc Rotenberg*_____
Marc Rotenberg
Counsel of Record
Alan Butler
John Davisson
Electronic Privacy Information Center

1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 18-15982

I am the attorney or self-represented party.

This brief contains 6283 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ○ it is a joint brief submitted by separately represented parties;
  - ○ a party or parties are filing a single brief in response to multiple briefs; or
  - ○ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Marc Rotenberg **Date** 12/17/2018

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of December 2018, the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center in Support of Plaintiff-Appellee was electronically filed with the Clerk of the Court, and thereby served upon counsel for the parties via electronic delivery.

Dated: December 17, 2018

*/s/ Marc Rotenberg*_____
Marc Rotenberg
Counsel of Record
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140