No. 123186

IN THE SUPREME COURT OF ILLINOIS

STACY ROSENBACH, as Mother and Next Friend of Alexander Rosenbach and on behalf of all others similarly situated, Plaintiff-Appellant, v. SIX FLAGS ENTERTAINMENT CORP. and GREAT AMERICA LLC, Defendant-Appellee.	On Appeal from the Appellate Court of Illinois, Second District, No. 2-17-317 There on appeal from the Circuit Court of Lake County, No. 16-CH-13 Honorable Luis A. Berrones, Judge Presiding

BRIEF OF *AMICI CURIAE* THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, THE CENTER FOR DEMOCRACY & TECHNOLOGY, THE CHICAGO ALLIANCE AGAINST SEXUAL EXPLOITATION, THE ELECTRONIC FRONTIER FOUNDATION, ILLINOIS PIRG EDUCATION FUND, INC., AND LUCY PARSONS LABS IN SUPPORT OF PLAINTIFF-APPELLANT

Rebecca K. Glenberg
ARDC No. 6322106
Roger Baldwin Foundation of ACLU, Inc.
180 N. Michigan Ave., Ste. 2300
Chicago, Illinois 60601

Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad St., 18th Fl.
New York, NY 10004

Joseph Jerome
Center for Democracy & Technology
1401 K St. NW, Ste. 200
Washington, DC 2005

Megan Rosenfeld
Chicago Alliance Against Sexual Exploitation
307 N. Michigan Ave., Ste. 1818
Chicago, IL 60601

Adam Schwartz
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109

Michael C. Landis
Illinois PIRG Education Fund, Inc.
328 S. Jefferson St., Ste. 620
Chicago, IL 60661

Attorneys for Amici Curiae

POINTS AND AUTHORITIES

INTERESTS OF AMICI CURIAE

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization of more than one million members dedicated to defending the civil liberties and civil rights guaranteed by the Constitution. The ACLU of Illinois is the Illinois state affiliate of the national ACLU. Both entities have been at the forefront of numerous cases addressing the right to privacy. The ACLU and its Illinois affiliate drafted BIPA and were instrumental to its passage.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on privacy, civil liberties, and human rights issues affecting the Internet, other communications networks, and associated technologies. CDT has long advocated for stronger privacy laws at both the state and federal level, and has been involved in the establishment of best practices for biometric data collection, including digital signage systems and research with wearable devices. CDT believes meaningful enforcement of violations of biometric privacy is important to protecting consumers from irresponsible data collection and use.

The Chicago Alliance Against Sexual Exploitation ("CAASE") is an Illinois-based non-profit dedicated to transforming the cultural, systemic, and individual responses that lead to, support, or profit from sexual harm. CAASE advocates for policies and practices that decrease vulnerabilities to sexual harm and give survivors of sexual harm more options for healing and safety. Fundamental pillars of survivor safety include the ability for the survivor to make informed decisions about release of their personal information, as well as the ability to individually enforce their rights after a violation.

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society. EFF has served as *amicus* in cases involving biometrics and other privacy issues, including *People v. Minnis*, 409 Ill. Dec. 60 (2016), *Riley v. California*, 134 S. Ct. 2473 (2014), *Maryland v. King*, 133 S. Ct. 1958 (2013), and *United States v. Jones*, 565 U.S. 400 (2012).

Illinois PIRG Education Fund, Inc. ("Illinois PIRG Education Fund") is an independent, non-partisan, 501(c)(3) organization that works for consumers and the public interest. Through research, public education, and outreach it serves as a counterweight to the powerful special interests that threaten our health, safety, and well-being. Illinois PIRG Education Fund has been an active defender of Illinois' Biometric Information Privacy Act in the legislature as opponents have tried to weaken it and was a leading advocate of updating the Illinois Personal Information Protection Act in 2015. Illinois PIRG Education Fund believes that consumers must be protected from violations of their biometric information privacy rights.

Lucy Parsons Labs ("LPL") is a digital rights non-profit composed of academics, transparency activists, artists, and technologists. LPL analyzes issues in technology particularly at the intersection of corporate and government surveillance. LPL has written extensively about the role of surveillance and its impact on civil society. Most recently, members of LPL wrote to the Telecommunications and Information Technology Committee about the technical impact of proposed amendments to Illinois' Biometric Information Privacy Act.

SUMMARY OF THE ARGUMENT

In 2008, the Illinois legislature enacted the Biometric Information Privacy Act ("BIPA") in order to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). The legislature found it necessary to protect biometric information because it is "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." 740 ILCS 14/5(c). In addition, the legislature found that the "use of biometrics is growing in the business and security screening sectors." 740 ILCS 14/5(a).

The ensuing decade has confirmed the wisdom and necessity of the legislature's action, as the collection and use of biometric information has proliferated and the privacy threats of nonconsensual collection and use of biometric information have become even clearer. Without reasonable limits, biometric technologies threaten to enable corporations and law enforcement to pervasively track people's movements and activities in public and private spaces, and risk exposing people to forms of identity theft that are particularly hard to remedy. Only with enforceable protections of the kind enshrined in BIPA can society hope to mitigate those risks.

This case concerns the interpretation of BIPA's provision allowing a person "aggrieved" by a violation of the statute to file a civil action in court. Although the defendants violated BIPA by collecting plaintiff's fingerprints without giving the requisite notice or receiving the requisite consent, the court below held that the plaintiff

was not aggrieved. That holding is inconsistent with the language, purpose, and structure of BIPA, and this Court should reverse.

First, the statute recognizes that the immutability of biometric information puts individuals at risk of irreparable harm in the form of identity theft and/or tracking when they are unable to control access to that information. Second, in order to allow individuals to protect such highly sensitive information, the statute creates substantive rights in receiving notice and giving informed consent. Specifically, the statute requires a private entity to (1) "inform[ ] the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored," 740 ILCS 14/15(b)(1); (2) "inform[ ] the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used," 740 ILCS 14/15(b)(2); and (3) obtain "a written release executed by the subject of the biometric identifier or biometric information or the subject's legal authorized representative," 740 ILCS 14/15(b)(3). Third, the protection of these substantive rights requires private enforcement when they are violated, as intended by the Illinois legislature.

A conclusion in this case that the plaintiff is not an "aggrieved person" would significantly undermine the private enforcement mechanism of the statute, depriving this particular plaintiff of relief and leaving no means to hold wrongdoers accountable for their violations of BIPA's notice and consent requirements. Accordingly, this Court should reverse the decision of the court below and conclude that the plaintiff is a "person aggrieved by a violation of [BIPA]."

ARGUMENT

I. IN THE DECADE SINCE BIPA'S ENACTMENT, ADVANCES IN BIOMETRIC COLLECTION AND STORAGE TECHNOLOGY HAVE MADE CLEAR THE IMPORTANCE OF ENFORCEABLE GUARANTEES OF NOTICE AND INFORMED CONSENT.

Biometric collection technologies have spread markedly since BIPA's enactment in 2008, now appearing in a dizzying array of everyday applications. Retail stores use facial recognition technology to "identify known shoplifters,"[1] and at least some companies are reportedly using such technology to track shoppers in their stores.[2] Employers collect biometrics for time tracking and attendance management, as well as to manage access to company phones, laptops, and cloud storage accounts.[3] Banks have invested in collecting customers' biometric data, including fingerprints, iris scans, and voiceprints, to authenticate those customers' identities.[4] Churches have adopted fingerprint collection technology "to accurately track attendance for various events like Bible studies, worship services and Sunday school."[5] Many schools now collect fingerprints to manage attendance, cafeteria purchases, library services, and security,[6] and

---

[1] Lowe's US Privacy Statement, Lowe's, Nov. 20, 2017, https://www.lowes.com/l/privacy-and-security-statement.html.

[2] Annie Lin, *Facial Recognition is Tracking Customers as They Shop in Stores, Tech Company Says*, CNBC, Nov. 23, 2017, https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html.

[3] Kronos Touch ID Plus, Kronos, https://www.kronos.com/resource/download/20106; Selena Larson, *Beyond Passwords: Companies Use Fingerprints and Digital Behavior to ID Employees*, CNN Tech, Mar. 18, 2018, http://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html.

[4] *From Fingerprints to Faces: Bank of America Explores Biometrics' Next Phase*, PYMNTS.com, Sept. 27, 2017, https://www.pymnts.com/news/security-and-risk/2017/bank-of-america-biometrics-facial-recogniton/.

[5] *Biometric Church Management*, Bayometric, http://www.bayometric.co.uk/biometric-church-management/.

[6] *See, e.g.*, *The Growth of Biometrics in Schools*, identiMetrics, 2017, https://www.identimetrics.net/images/Growth-of-Biometrics-in-Schools.pdf. While

some schools have started installing facial recognition systems to control entry into buildings.[7]

Major technology companies continue to invest heavily in turnkey systems that allow private and public entities to collect, analyze, and store biometric information at scale. Amazon, for example, markets a system called "Rekognition" that the company says "provides highly accurate facial analysis and facial recognition on images and video that . . . can detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases."[8] According to Amazon's promotional materials, Rekognition is not only able to store facial recognition images of large numbers of people, but it is also able to "perform real-time face searches against collections with tens of millions of faces" and "detect, analyze, and index up to 100 faces . . . in a single image," such as photographs captured at "crowded events . . . [and] department stores."[9] The system can purportedly be used to analyze minute facial details

---

collection of biometric information by private schools is regulated by BIPA, collection of the same data by public schools is regulated by a separate statute that provides similar and additional protections. *Compare* 740 Ill. Comp. Stat. 14/15 (regulating collection and use of biometric information by "private entit[ies]"), *with* 105 Ill. Comp. Stat. 5/34-18.34 (regulating collection and use of "student biometric information" by "school districts").

[7] Sidney Fussell, *Schools Are Spending Millions on High-Tech Surveillance of Kids*, Gizmodo, Mar. 16, 2018, https://gizmodo.com/schools-are-spending-millions-on-high-tech-surveillance-1823811050; Christian Byers, *St. Mary's High School Adds Facial Recognition Locks*, St. Louis Post-Dispatch, Mar. 9, 2015, https://www.stltoday.com/news/local/crime-and-courts/st-louis-parochial-high-school-adds-facial-recognition-locks/article_db488bb5-44f2-5301-b131-8a7ebe04bba9.html.

[8] Amazon Rekognition, AWS, https://aws.amazon.com/rekognition/. Microsoft offers a similar service called "Face API," https://azure.microsoft.com/en-us/services/cognitive-services/face/.

[9] Ranju Das, *Amazon Rekognition Announces Real-Time Face Recognition, Support for Recognition of Text in Image, and Improved Face Detection*, AWS Machine Learning Blog (Nov. 21, 2017), https://aws.amazon.com/blogs/machine-learning/amazon-rekognition-announces-real-time-face-recognition-support-for-recognition-of-text-in-image-and-improved-face-detection/.

to identify an individual's estimated age range, determine whether a person has his or her eyes or mouth open or closed, and even his or her emotional state.[10] As these technological capabilities have scaled up, their cost has come down: Amazon charges just one cent ($0.01) per month for storage of 1,000 face scans and only $0.10 to $0.12 per minute to perform facial recognition analysis on video feeds.[11]

While Amazon and others sell powerful systems to store and analyze biometric data, other companies are developing increasingly sophisticated and accurate tools for capturing biometric data. Over time, "ongoing advancements and higher quality camera resolutions [have] result[ed] in better accuracy, improved capture and enhanced picture[s]."[12] For example, a company called StoneLock uses near-infrared wavelengths (commonly used in night-vision goggles) "to overcome the inconsistencies of visible light to penetrate subdermally while . . . measure[ing] and map[ping] over 2,000 points on a user's face."[13] Researchers are also "incorporating artificial intelligence and deep learning into biometrics, which learns the evolving characteristics of the user and updates identification files automatically."[14] Other advances have enabled researchers to conduct iris scans at a distance of up to 12 meters, eliminating the need for people to place their

[10] Amazon Rekognition Developer Guide, https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf.
[11] Amazon Rekognition Pricing, AWS, https://aws.amazon.com/rekognition/pricing/.
[12] Deborah L. O'Mara, *Breaking Down Barriers: Biometric Advancements*, Electrical Contractor, June 2017, https://www.ecmag.com/section/systems/breaking-down-barriers-biometric-advancements.
[13] *Id*.
[14] *Id*.

eye directly in front of an eye-scanning camera or even to be aware that the scanning is taking place.[15]

In sum, since BIPA was enacted ten years ago, private entities have deployed vastly improved and more numerous tools for capturing biometric information, and they have access to an array of increasingly powerful platforms to analyze that information for any number of reasons. Without the enforceable guarantees of notice and informed consent found in BIPA, the collection, retention, and use of biometric information poses serious privacy concerns to all Illinoisans. First, the rapidly improving capability to scan individuals' faces and eyes from a distance enables surreptitious collection. Absent statutory notice requirements, people will often have no way to know if their biometric information is being collected, much less why or how it is being used and retained. In a recent survey conducted by the ACLU, for example, 18 of the top 20 American retail companies refused to say whether they collect facial recognition scans of their customers.[16] People can avoid pervasive invasions of privacy through surreptitious surveillance technologies only with a legal requirement that entities provide notice and obtain informed consent before collecting unique biometric information, and only if that requirement is readily enforceable.

---

[15] Robinson Meyer, *Long-Range Iris Scanning Is Here*, The Atlantic, May 13, 2015, https://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/; *see also* Kien Nguyen, et al., *Long Range Iris Recognition: A Survey*, 72 Pattern Recognition 123 (2017), *available at* https://www.cse.msu.edu/~rossarun/pubs/NguyenLongRangeIris_PR2017.pdf.

[16] Jenna Bitar & Jay Stanley, *Are Stores You Shop at Secretly Using Face Recognition on You?*, Free Future, ACLU (Mar. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face.

Second, without the legal protections afforded by BIPA, people cannot control the dissemination of their biometric information and cannot know if information collected for one purpose is sold, traded, or used for another. This is frightening enough when commercial entities collect biometric information, but it is all the more so when law enforcement agencies access that information because law enforcement's ability to purchase or informally request biometric data collected by private entities can evade critical protections under the Fourth Amendment. *See Carpenter v. United States*, __ S. Ct. __, 2018 WL 3073916 (U.S. June 22, 2018) (requiring search warrant for law enforcement access to certain sensitive records held by third-party companies). Easy law enforcement access to sensitive biometric data can also facilitate abusive practices, including enabling rogue police officers to more easily stalk and harass current or former intimate partners and others.[17] Individuals cannot have a meaningful opportunity to decide whether they wish their biometric identifiers to be collected unless they have an enforceable right to notice of the "specific purpose . . . for which . . . [the data] is being collected, stored, and used," 740 ILCS 14/15(b)(2), and to deny consent for its "disclos[ure or] redisclos[ure]," 740 ILCS 14/15(d)(1). Automated license plate reader (ALPR) technology provides a cautionary tale, serving as a model case of just how

[17] *Cf.* Jim Avila, Alison Lynn, & Lauren Pearle, *Police Sergeant Had Secret Life as Serial Rapist*, ABC News, Aug. 30, 2010, https://abcnews.go.com/Primetime/illinois-police-sergeant-jeffrey-pelo-doubled-serial-rapist/story?id=11497530 (Bloomington, IL police officer used "police computer . . . to run license plate searches on three of the victims" he targeted for stalking and rape); Lauren Kirchner, *When Your Stalker Is a Cop*, Pacific Standard, Nov. 6, 2014, https://psmag.com/news/stalker-cop-police-protection-danger-crime-harassment-93995.

prevalent this is, the technology both having expanded rapidly and deployed on a large scale without meaningful notice or informed consent.[18]

Unlike license plate numbers, passwords, ID cards, and social security numbers, biometric identifiers cannot be changed in the wake of unauthorized disclosure or misuse. In many cases, this information cannot be protected and concealed against unauthorized acquisition in the first instance because our faces, eyes, and voices are routinely and unavoidably exposed to public view. *See* 740 ILCS 14/5(c). Only strong and enforceable legal protections can safeguard against abuses of this highly sensitive data. As biometric technologies continue to advance and become increasingly ubiquitous in everyday life, the modest safeguards contemplated by the Illinois legislature more than a decade ago in BIPA become even more essential to protect personal privacy.

II. FAILURE TO REQUIRE NOTICE AND INFORMED CONSENT FOR A COMPANY'S BIOMETRIC DATA PRACTICES HARMS INDIVIDUALS' PRIVACY INTERESTS AND IS A VIOLATION OF THE LAW.

The issue before this Court is whether failure to comply with the substantive provisions of BIPA is sufficient to show that the plaintiff is "aggrieved" by the defendants' violations of the statute. *Amici* support the plaintiff's position that

[18] ALPRs are high-speed cameras that automatically photograph passing license plates, recording the date, time, and GPS coordinates of each plate, and constructing detailed profiles of large number of vehicles and, correspondingly, their drivers. *See* You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements, ACLU (July 2013). Police are able to circumvent limitations on their data collection by contracting with private companies that maintain their own ALPR networks. Vigilant Solutions ("Vigilant"), for example, offers police departments paid access to its database of more than five billion plate reads, which are collected at a rate of 150 million per month for "commercial applications such as access control, tolling, asset recovery and more." PlateSearch, Vigilant Solutions, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/. The same dynamic can be expected for tracking data generated by private entities' collection of biometric information and concerns precisely the sort of protection that Illinois set out to ensure in its passage of BIPA.

fingerprinting an individual without disclosing how that information will be stored, used, or destroyed and without properly obtaining written consent creates an actionable privacy harm. The Illinois Court of Appeals has undervalued the essential importance of notice and informed consent to empower individuals to protect their privacy and, in doing so, acts contrary to privacy laws in the United States, generally, and the intentions of the drafters of BIPA, specifically.

Notice is the "most fundamental principle" of privacy protection. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998). "There is a sense in which notice underpins law's basic legitimacy." M. R. Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1028 (2013). The function of notice is to provide the necessary transparency to enable meaningful consent. This meaningful consent is a prerequisite for individuals to maintain agency and autonomy.

Indeed, the Federal Trade Commission has acknowledged: "Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information." FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998). The primacy of meaningful notice originates from the earliest deliberations about privacy protection within the federal government. In a 1973 report, an advisory committee within the U.S. Department of Health, Education, and Welfare initially proposed a set of Fair Information Practice Principles (FIPPs) to protect the privacy of personal data in record-keeping systems. Crucially, the committee stated that "[t]here must be no personal-data record-keeping systems whose very existence is secret" and that "[t]here must be a way for an individual to find out what information about him is in a

record and how it is used."[19] As the federal government has observed, the FIPPs have informed both federal statutes and the laws of many states and are a basic practice of many organizations around the world.[20]

Federal privacy laws protect categories of sensitive information precisely by requiring entities to provide notice to consumers about their data practices. Such notice enables individuals to make informed decisions and, therefore, exercise their agency and autonomy. For example, the Gramm-Leach-Bliley Act requires financial institutions to provide customers and consumers notice of privacy practices, and financial regulators engaged in a lengthy rulemaking process to provide "more useful privacy notices." 72 Fed. Reg. 14939, 14943 (Mar. 29, 2007). Model notices permit customers to compare how different financial institutions share and disclose categories of individual financial information. Transparency about the data practices of health care providers can be even more consequential to individuals. The Health Insurance Portability & Accountability Act requires covered entities to provide notice "that provides a clear, user friendly explanation of individuals[']rights with respect to their personal health information and the privacy practices of health plans and health care providers."[21] The U.S. Department of Health and Human Services has explained that "[t]rust in electronic exchange of

[19] SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS XX-XXI (1973).
[20] FEDERAL OFFICE OF MANAGEMENT AND BUDGET, CIRCULAR NO. A-130, MANAGEMENT OF FEDERAL INFORMATION RESOURCES (Dec. 25, 1985, Revised 2016).
[21] Dep't of Health & Human Servs., Model Notices of Privacy Practices, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html (last visited June 25, 2018).

individually identifiable health information can best be established in an open and transparent environment."[22] Failure to provide notice effectively undermines trust.

When legislators enact new notice requirements, they typically do so in response to identified concerns about data collection, use, or dissemination. For example, the Video Privacy Protection Act (VPPA) is similar to BIPA in both legislative history and effect. The VPPA was enacted after a Washington, D.C.-area video rental store provided the video rental records of Judge Robert Bork to a reporter upon request. Senator Paul Simon cautioned then that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." 134 Cong. Rec. S5401 (May 10, 1988). To address this concern, the VPPA restricts disclosure of personally identifiable information that is linked to requesting or obtaining specific video materials or services. 18 U.S.C. § 2710(a)(3). In order to disclose personally identifiable information beyond an enumerated list of exceptions, video tape service providers are required to obtain from individuals "informed, written consent" that is "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and that is obtain at the time of the disclosure or in advance. 18 U.S.C. § 2710(b)(2)(B).

Importantly, laws that provide details as to what precisely should be disclosed in a notice provide a minimum guidepost for businesses to follow. Recognizing the Orwellian potential of two-way cable television systems, Congress passed the Cable

[22] Office of the Nat'l Coordinator for Health Info. Tech., NATIONWIDE PRIVACY AND SECURITY FRAMEWORK FOR ELECTRONIC EXCHANGE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 7, Dep't of Health & Human Servs. (2008), *available at* https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

Communications Policy Act (CCPA), which creates a framework for protecting the privacy of cable subscribers. Michael I. Meyerson, *The Cable Communications Policy Act of 1984: A Balancing Act on the Coaxial Wires*, 19 GA. L. REV. 543, 612 (1985). The CCPA's framework is built on guaranteeing subscribers' rights to know what information is being maintained about them. Specifically, it requires cable operators provide a "separate, written statement" that "clearly and conspicuously informs" subscribers of:

> (A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;
>
> (B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;
>
> (C) the period during which such information will be maintained by the cable operator;
>
> (D) the times and place at which the subscriber may have access to such information . . . ; and
>
> (E) the limitations provided by this section with respect to the collection and disclosure of information.

47 U.S.C. § 551(a)(1). Also, the CCPA requires cable companies to obtain the customer's opt-in consent before collecting or disclosing personally identifiable information about them. 47 U.S.C. § 551(b)(1), (c)(1). These provisions detail the precise data practices with which Congress was concerned and, like the VPPA, the statute provides a private right of action for any individual aggrieved by a cable operator's failure to comply with the CCPA. 47 U.S.C. § 551(f).

The privacy legal landscape has demonstrated profound respect for the role transparency plays in protecting individuals' privacy. This framework recognizes the

importance that notice plays in empowering individuals to understand how emerging technologies will impact their autonomy and agency, which is also supported across privacy law and policy.[23]

III. NOTICE IS A SUBSTANTIVE RIGHT UNDER BIPA.

The Illinois legislature intended the requirement that a company provide adequate notice to be essential for compliance with BIPA. The legislature enacted BIPA in response to concerns over the risks posed by biometric data collection. Legislators were especially concerned with fingerprint scanners used in stores and other functionally nonvoluntary environments. 740 ILCS 14/5. After Pay By Touch, a vendor used in Illinois grocery stores, filed for bankruptcy and, in despair, attempted to sell the bank of biometric data that it had collected over the years to a third-party, Representative Joseph Lyons suggested that BIPA was necessary because individuals who used Pay By Touch were left "without any information as to how their biometric and financial data will be used."[24] Legislative findings specifically noted that consumers were unaware of the connection between biometric data and other personal information. 740 ILCS 14/5(d) (noting that the "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").

---

[23] Even industry practice reflects this understanding. Industry-crafted rules frequently emphasize the importance of notice, and this is especially true with respect to biometrics. For example, The International Biometrics + Identity Association has called on the private sector to develop policies to "clearly set forth how identification data will be collected, stored, accessed, and used, and that preserve the rights of individuals to limit the distribution of the data beyond the stated purposes." INT. BIOMETRICS IDENTITY ASS'N PRIVACY PRINCIPLES, https://www.ibia.org/privacy-principles (last visited June 25, 2018).

[24] Justin O. Kay, *The Illinois Biometric Information Privacy Act*, ASS'N OF CORP. COUNS. (2017), http://www.acc.com/chapters/chic/upload/Drinker-Biddle-2017-1-BIPA-Article.pdf.

Accordingly, the legislature recognized that "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." 740 ILCS 14/5(g).

A key facet of BIPA's regulation of biometric data retention, collection, disclosure, and destruction is the requirement of notice and informed consent. BIPA explicitly requires that a company obtain "a *written release* executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." 740 ILCS 14/15(b)(3) (emphasis added). A "written release" is defined in the statute as "informed written consent." 740 ILCS 14/10. Black's Law Dictionary defines "informed consent" as "[a] person's agreement to allow something to happen, made with full knowledge of the risks involved and the alternatives." BLACK'S LAW DICTIONARY 368 (10th ed. 2014). Thus, in order for a business to comply with BIPA, it must ensure that its customers do in fact have full knowledge of the risks involved with the biometric data collection. The only way to have full knowledge of the risks involved with the collection of some data is to be provided adequate notice surrounding the collection of that data.

In the case of the defendants' BIPA violations, in the absence of any notice, there is no way that the plaintiff could be said to have had "full knowledge of the risks involved" with the collection of his biometric data. Therefore, along with the repeated injunctions that notice must be "*in writing,*" the language of informed consent in BIPA demonstrates that its drafters intended to combat the exact type of violation that the defendants are alleged to have committed in this case.

A court interpreting BIPA also has highlighted that notice plays a fundamental role in enabling an individual's control of his or her data. In *Patel v. Facebook, Inc.*, suit was brought against Facebook alleging the unlawful collection and storage of biometric data without prior consent through the use of its "Tag Suggestions" feature. *Patel v. Facebook, Inc.*, No. 15-cv-4265 (N.D. Ill. filed May 14, 2015) (subsequently transferred to the U.S. District Court for the Northern District of California and currently on appeal to the U.S. Court of Appeals for the Ninth Circuit). "Tag Suggestions" functions by allowing Facebook to scan incoming photographs uploaded to the site using "state-of-the-art facial recognition technology." Facebook's technology extracts biometric identifiers from the photographs in order to predict the users' identity and offer "tag" suggestions. In evaluating the existence of a concrete injury, the court explained that when companies simply disregard BIPA's notice and consent requirements that "the right of the individual to maintain her biometric privacy vanishes into thin air. *The precise harm the Illinois legislature sought to prevent is then realized*." *Patel v. Facebook, Inc.*, 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (order denying renewed motion to dismiss for lack of subject matter jurisdiction) (emphasis added). In the case at bar, the defendants failed to provide the notice needed in order for the plaintiff to provide informed, meaningful consent. As such, the plaintiff could not effectuate his privacy rights under BIPA and, as a result, was deprived of agency and autonomy. This is exactly the injury that BIPA was intended to foreclose, and it enacts a substantial harm on the person denied the right to receive notice and provide consent.

IV. THE STATUTORY RIGHT TO NOTICE AND INFORMED CONSENT CAN ONLY BE PROTECTED THROUGH ROBUST PRIVATE ENFORCEMENT.

A. The Illinois legislature intended strong enforcement of BIPA's protections through private litigation.

Section 20 of BIPA creates an express private right of action for "[a]ny person aggrieved by a violation of this Act." 740 ILCS 14/20. To incentivize private individuals to bring lawsuits to remedy violations of the rights that BIPA protects, the statute includes "liquidated damages" provisions guaranteeing that an individual will receive at least $1,000 in compensation for each negligent violation of the act (if their actual damages are greater than or equal to $0 and less than or equal to $999) and at least $5,000 in compensation for each intentional or reckless violation of the act (if their actual damages are greater than or equal to $0 and less than or equal to $4,999). 740 ILCS 14/20(1), (2). The inclusion of these statutory liquidated damages provisions are evidence of the Illinois legislature's intent to allow a private cause of action where there is no injury beyond loss of the statutory rights to notice and informed consent and where any additional injury is small or difficult to prove. BIPA further incentivizes private enforcement by authorizing the recovery of "reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses." 740 ILCS 14/20(3). Notably, there is no provision authorizing the Illinois Attorney General to enforce BIPA. Taken together, these provisions clearly evince the Illinois legislature's intent to create a robust enforcement regime that relies on private litigants to ensure compliance with BIPA's requirements of notice and informed consent.

B. Private litigation is a critical enforcement mechanism in the American legal system.

The American legal system relies upon ex post private enforcement as an important complement to ex ante public regulation. *See generally* J. Maria Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, 53 WM. & MARY L. REV. 1137, 1149 (2012) (tracing the "historical origins of the United States' diffuse system of regulation and the role that private-party litigants play as regulators in that system" and exploring "the American regulatory system's functional dependence on private regulation and the mechanisms that enable it"). This reliance has historical roots in our "inherited regulatory design, which relied largely on private suits brought pursuant to common law doctrines." *Id*. at 1147.

The role of private litigation in many areas of substantive law was enhanced throughout the second half of the twentieth century when Congress passed numerous statutes containing express private-right-of-action provisions. *Id*. at 1148. Congress' decision to "vest in private parties a great deal of responsibility for enforcement by extending the statutory mechanisms provided to private parties in order to facilitate and incentivize private suits" while, simultaneously, to "decrease the enforcement mechanisms available to relevant public regulatory bodies, which have suffered budget cuts and have decreased their enforcement efforts," occurred across a "wide range of substantive areas, ranging from consumer lending to civil rights abuses to antitrust." *Id*. at 1151. The result is that many federal statutes, particularly consumer protection statutes, provide for an express private right of action.[25]

[25] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C.A. § 1681n; Cable Communications Policy Act, 47 U.S.C. § 551(f); Drivers' Privacy Protection Act, 18 U.S.C. § 2724;

A similar trend was seen at the state level. *See, e.g.*, Dee Pridgen, *Wrecking Ball Disguised as Law Reform: ALEC's Model Act on Private Enforcement of Consumer Protection Statutes*, 39 N.Y.U. REV. L. & SOC. CHANGE 279, 283 (2015) ("While it first seemed that state laws would rely on the enforcement powers of the state governments alone, the need to also utilize private litigants eventually became clear to both state legislatures and their allies in the state and federal governments. The incorporation of private rights of action to the state UDAP [unfair or deceptive acts or practices] laws took place gradually, mostly occurring during the period of 1970-1980."). Like their federal counterparts, many state consumer protection laws include express private-right-of-action provisions.[26] In a 1979 speech, the former director of the Federal Trade Commission's Bureau of Consumer Protection summarized the argument for private enforcement of state UDAP laws as follows: "If states, because they are closer to the people, can be more responsive and tailor remedies to individual areas better than the federal government can, individual consumers are even better at that. Also, obviously, there is an even greater deterrent effect on wayward businesses." *Id*.

To ensure that private-right-of-action provisions are utilized, statutes often include "other enforcement incentives, such as damage multipliers, statutory damages, punitive damages, and fee-shifting." Glover, *The Structural Role of Private Enforcement*

Employee Polygraph Protection Act, 29 U.S.C. § 2005(c); Privacy Act, 5 U.S.C. § 552a(g)(1); Privacy Protection Act, 42 U.S.C. § 2000aa-6(a).

[26] *See, e.g.*, California's Invasion of Privacy Act, Cal. Penal Code § 637.2 (2018); Ohio's Telephone Solicitation Sales Act, Ohio Rev. Code Ann. § 4719.12 (2018); Tennessee's Video Consumer Privacy Act, Tenn. Code Ann. § 47-18-2201 (2018); Connecticut's Communications Consumer Privacy Act, Conn. Gen. Stat. Ann. § 53-422 (2018); Michigan's Preservation of Personal Privacy Act, Mich. Comp. Laws Ann. § 445.1715 (2018).

Mechanisms in Public Law, at 1151 (collecting examples); *see also* Pridgen, *Wrecking Ball Disguised as Law Reform*, at 284 (noting that the provisions under the Clayton Act that provide for treble damages and attorney fees have been "so successful that ninety-five percent of all antitrust cases are brought by private plaintiffs"). Statutory liquidated damages provisions (also referred to as statutory minimum damages provisions), like those contained in BIPA, are an important feature of private enforcement regimes, especially in the context of consumer protection and consumer rights. *See, e.g.*, Pridgen, *Wrecking Ball Disguised as Law Reform*, at 289 ("Statutory minimum . . . damages are . . . a common feature of state UDAP statutes.").

Such provisions are important because they guarantee that the plaintiff receives a minimum amount of compensation, and violators are held to account for their statutory violations, even when the plaintiff has suffered no actual money damages, a small amount of damages, or damages that are difficult to quantify. For example, this Court has explicitly recognized that statutory liquidated damages act as "an incentive for private parties to enforce" the law because "actual losses associated with individual violations" may be small. *Standard Mut. Ins. Co. v. Lay*, 989 N.E.2d 591, 600 (Ill. 2013) (discussing the statutory damages provision of the federal Telephone Consumer Protection Act). Other state supreme courts have explicitly recognized the need for statutory damages when the consumer has suffered no actual money damages, *see, e.g.*, *Zanakis-Pico v. Cutter Dodge, Inc.*, 98 Haw. 309, 316, 47 P.3d 1222, 1229 (2002) (holding that plaintiffs may recover statutorily prescribed damages from a company that engaged in deceptive practices even though the plaintiffs had not actually purchased the products fraudulently advertised by the company and observing that it would be "most strange if the legislature

had sought to protect such persons but failed to provide them with any remedy"). The incentivizing function of statutory damages provisions is especially important in the context of individual privacy rights because, in many instances, both the harm and resulting damages might be difficult to quantify. As the Illinois legislature recognized when it enacted BIPA, "[t]he full ramifications of biometric technology are not fully known." 740 ILCS 14/5(f).

C. A conclusion in this case that the plaintiff is not "aggrieved" would severely undercut the private enforcement mechanism that the Illinois legislature created in BIPA.

If this Court ultimately concludes that the plaintiff in this case is not an "aggrieved person" under BIPA, not only would this plaintiff be unable to hold these defendants accountable for their clear violations of BIPA's notice and informed consent requirements, but future potential plaintiffs would be similarly hamstrung in their efforts to hold wrongdoers accountable. Judicial restrictions on legislatively-created private enforcement mechanisms can "lead to undesirable consequences for the vindication of substantive rights or the deterrence of socially undesirable conduct." Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, at 1142 (collecting sources). For example, in the context of federal civil rights law, scholars have noted the "insidious" practice of some federal courts of "leav[ing] the formal right in place, but . . . constrict[ing] the remedial machinery." Pamela S. Karlan, *Disarming the Private Attorney General*, 2003 U. ILL. L. REV. 183, 185 (2003). "At best, this will dilute the value of the right, since some violations will go unremedied. At worst, it may signal [to] potential wrongdoers that they can infringe the right with impunity." *Id*. at 185. Thus, "the availability of meaningful ex post private enforcement is a significant determinant of

the rule of law's operation within the United States." Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, at 1153.

CONCLUSION

As discussed above, strong enforcement of BIPA's notice and informed consent requirements is especially important because of the particularly sensitive nature of an individual's biometric information. In enacting BIPA, the Illinois legislature created a remedial scheme to allow consumers to sue and demand pecuniary relief without proving that any actual damages occurred. This was done in recognition that, without notice, the collection of biometric information is surreptitious and that the privacy harms are difficult for the consumer to understand at the outset and discover after the fact. Adopting the defendants' reading of BIPA would effectively gut the statute's primary purpose and leave Illinoisans without meaningful recourse in a world of rapidly advancing technology and proliferating uses of biometric information. Thus, *amici* respectfully urge this Court to reverse the decision below.

Dated: July 5, 2018

Respectfully submitted,

/s/ Rebecca K. Glenberg
Rebecca K. Glenberg
ARDC No. 6322106
Roger Baldwin Foundation of ACLU, Inc.
150 North Michigan Ave., Suite 600
Chicago, IL 60601
(312) 201-9740
rglenberg@aclu-il.org

Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad St., 18th Fl.
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Joseph Jerome
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, DC 2005
(202) 407-8812
jjerome@cdt.org

Megan Rosenfeld
Chicago Alliance Against Sexual Exploitation
307 N. Michigan Ave., Ste. 1818
Chicago, IL 60601

Adam Schwartz
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
adam@eff.org

Michael C. Landis
Illinois PIRG Education Fund, Inc.
328 S. Jefferson St., Ste. 620
Chicago, IL 60661
(312) 544-4433
mlandis@pirg.org

RULE 341(c) CERTIFICATE OF COMPLIANCE

I, Rebecca K. Glenberg, certify that this brief conforms to the requirements of Supreme Court Rules 341(a) and (b). The length of this brief, excluding pages containing the Rule 341(d) cover, the Rule 341(h)(1) 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 7,056 words.

/s/ Rebecca K. Glenberg
Rebecca K. Glenberg
Attorney for *amici curiae*

NOTICE OF FILING AND PROOF OF SERVICE

The undersigned, an attorney, certifies that on July 5, 2018, she caused the foregoing Motion for Leave to File Brief of *Amici Curiae* American Civil Liberties Union *et al*. in Support of Plaintiff-Appellant and Brief of *Amici Curiae* American Civil Liberties Union *et al*. in Support of Plaintiff-Appellant to be filed with the Supreme Court of Illinois using the Court's electronic filing system and that the same was emailed to the following counsel of record:

David M. Oppenheim
Phillip A. Bock
Robert Hatch
BOCK, HATCH, LEWIS & OPPENHEIM LLC
134 N LaSalle St Ste 1000
Chicago, IL 60602-1086
(312) 658-5500
david@classlawyers.com
phil@classlawyers.com
robert@classlawyers.com

Debra R. Bernard
Kathleen O'Sullivan
PERKINS COIE LLP
131 S Dearborn St Ste 1700
Chicago, IL 60603
(312) 324-8400
dbernard@perkinscoie.com
KOSullivan@perkinscoie.com

Attorney for defendants-appellees

Mark Bulgarelli
Ilan Chorowsky
PROGRESSIVE LAW GROUP, LLC
1570 Oak Ave Ste 103
Evanston, IL 60201
(312) 787-2717
markb@progressivelaw.com
ilan@progressivelaw.com

Attorneys for plaintiff-appellant

Within five days of acceptance by the Court, the undersigned also states that she will cause thirteen copies of the Brief of *Amici Curiae* to be mailed with postage prepaid addressed to:

Clerk's Office - Springfield

Supreme Court Building
200 E. Capitol Ave
Springfield, IL 62701

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

/s/ Rebecca K. Glenberg
Rebecca K. Glenberg

One of the Attorneys for Supporting Amici