No. 18-15982

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE FACEBOOK 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 *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA, CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, AND ILLINOIS PIRG EDUCATION FUND, INC., IN SUPPORT OF PLAINTIFFS–APPELLEES SEEKING AFFIRMANCE

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

Rebecca K. Glenberg
Roger Baldwin Foundation of ACLU, Inc.
150 North Michigan Ave., Suite 600
Chicago, IL 60601

Jacob A. Snow
American Civil Liberties Union Foundation of Northern California, Inc.
39 Drumm St.
San Francisco, CA 94111
Attorney for American Civil Liberties Union Foundation of Northern California and American Civil Liberties Union Foundation of Southern California

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

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

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

CORPORATE DISCLOSURE STATEMENT

Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Illinois, American Civil Liberties Union Foundation of Northern California, American Civil Liberties Union Foundation of Southern California, Center for Democracy & Technology, Electronic Frontier Foundation, and Illinois PIRG Education Fund, Inc. are non-profit entities that do not have parent corporations. No publicly held corporation owns 10 percent of more of any stake or stock in *amici curiae*.

/s/ Nathan Freed Wessler

Nathan Freed Wessler

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTERESTS OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization of more than 1.8 million members dedicated to defending the civil liberties and civil rights guaranteed by the Constitution. The ACLU of Illinois, ACLU Foundation of Northern California, and ACLU Foundation of Southern California are state affiliates of the national ACLU. Each of these entities has been at the forefront of numerous cases addressing the right to privacy. The ACLU and its Illinois affiliate drafted the Illinois Biometric Privacy Act 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

[1] Pursuant to Rule 29(a)(2), counsel for *amici curiae* certify that all parties have consented to the filing of this brief. Pursuant to Rule 29(a)(4)(E), counsel for *amici curiae* state that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

privacy is important to protecting consumers from irresponsible data collection and use.

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 *Carpenter v. United States*, 138 S. Ct. 2206 (2018), *Riley v. California*, 134 S. Ct. 2473 (2014), and *Maryland v. King*, 133 S. Ct. 1958 (2013).

Illinois Public Interest Research Group 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.

SUMMARY OF ARGUMENT

In 2008, the Illinois legislature enacted the Biometric Information Privacy Act ("BIPA") to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 Ill. Comp. Stat. 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." *Id.* 14/5(c). In addition, the legislature found that the "use of biometrics is growing in the business and security screening sectors." *Id.* 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 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.

In this class-certification appeal, Defendant-Appellant Facebook calls into question the purpose, meaning, and import of BIPA. *Amici* write to explain the importance of honoring BIPA's purpose of providing an enforceable remedy for violations of its notice and consent provisions. 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. In order for individuals to protect such highly sensitive information, the statute creates substantive rights in receiving notice and making an informed choice about ceding their biometric data. Specifically, the statute requires private entities 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 Ill. Comp. Stat. 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," *id.* 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 legally authorized representative," *id.* 14/15(b)(3). BIPA protects these substantive rights by requiring private enforcement when they are violated.

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,"[2] and at least some companies are reportedly using such technology to track shoppers in their stores.[3] Employers collect biometrics for time tracking and attendance management, as well as to manage access to company phones, laptops, and cloud storage accounts.[4] Banks have invested in collecting customers' biometric data, including face scans, fingerprints, iris scans, and voiceprints, to

---

[2] Lowe's US Privacy Statement, Nov. 20, 2017, https://web.archive.org/web/20171121112556/https://www.lowes.com/l/privacy-and-security-statement.html.

[3] 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.

[4] Kronos Touch ID Plus (2017), https://www.kronos.com/resource/download/20106; Selena Larson, *Beyond Passwords: Companies Use Fingerprints and Digital Behavior to ID Employees*, CNN Business, Mar. 18, 2018, http://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html.

authenticate those customers' identities.[5] Churches have adopted facial recognition and fingerprint collection technology "to accurately track attendance for various events like Bible studies, worship services and Sunday school."[6] Many schools now collect fingerprints to manage attendance, cafeteria purchases, library services, and security,[7] and some schools have started installing facial recognition systems to control entry into buildings.[8]

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

---

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

[6] Bayometric, http://www.bayometric.co.uk/biometric-church-management/; *see also* Sarah Pulliam Bailey, *Skipping Church? Facial Recognition Software Could Be Tracking You*, Wash. Post, July 24, 2015, https://www.washingtonpost.com/news/acts-of-faith/wp/2015/07/24/skipping-church-facial-recognition-software-could-be-tracking-you/.

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

[8] 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.

cases."[9] 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."[10] The system can purportedly be used to analyze minute facial details 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.[11] 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.[12]

While Amazon and others sell powerful systems to store and analyze biometric data, other companies are developing increasingly sophisticated and

[9] 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/.

[10] 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/.

[11] Amazon Rekognition Developer Guide, https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf.

[12] Amazon Rekognition Pricing, AWS, https://aws.amazon.com/rekognition/pricing/.

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]."[13] 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."[14] Researchers are also "incorporating artificial intelligence [AI] and deep learning into biometrics, which learns the evolving characteristics of the user and updates identification files automatically."[15] 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 eye directly in front of an eye-scanning camera or even to be aware that the scanning is taking place.[16] Facial recognition algorithms are increasingly able to identify partial or indirect images of faces.[17]

---

[13] Deborah L. O'Mara, *Breaking Down Barriers: Biometric Advancements*, Electrical Contractor, June 2017, https://www.ecmag.com/section/systems/breaking-down-barriers-biometric-advancements.

[14] *Id*.

[15] *Id*.

[16] 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/.

[17] *See, e.g.*, *Partial Face Recognition*, Face Forensics, http://www.faceforensics.com/PartialFaceRecog.aspx.

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. Without enforceable guarantees of notice and informed consent like those in BIPA, the collection, retention, and use of biometric information poses serious privacy concerns. First, the rapidly improving capability to identify individuals' faces and eyes from a distance or from less-than-perfect images enables surreptitious collection. Statutory notice requirements are often the only way for people to learn if their biometric information has been collected and how it is being used. 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.[18] 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 those requirements must be readily enforceable.

[18] 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*, 138 S. Ct. 2206 (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 conduct, including enabling rogue police officers to more easily stalk and harass current or former intimate partners and others.[19] Individuals cannot meaningfully decide whether to permit 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 Ill. Comp. Stat. 14/15(b)(2), and to deny consent for its "disclosure or redisclosure," *id.* 14/15(d)(1). Automated license plate reader (ALPR) technology

[19] *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).

provides a cautionary tale, showing how technology can expand rapidly and be deployed on a large scale without meaningful notice or informed consent.[20]

Finally, a critical reason to vigorously protect the right to opt-in consent before a company collects a person's biometrics is the inherent risk that the company will fail to adequately secure those biometrics from data thieves. Just last week, Facebook disclosed that a software bug may have allowed some 1,500 third-party apps to wrongly access the photos of some 6.8 million users, including images that people began to upload but did not post.[21] Unlike license plate numbers, passwords, ID cards, and social security numbers, biometric identifiers

[20] 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), https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked. 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. *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. *See FaceSearch*, Vigilant Solutions, https://www.vigilantsolutions.com/products/facial-recognition/.

[21] 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, https://www.washingtonpost.com/technology/2018/12/14/facebook-says-new-bug-allowed-apps-access-private-photos-up-million-users.

cannot be changed in the wake of unauthorized disclosure or misuse. Often this information cannot be protected against unauthorized acquisition in the first place, because our faces, eyes, and voices are routinely and unavoidably exposed to public view. *See* 740 Ill. Comp. Stat. 14/5(c). Only strong and enforceable legal protections can safeguard against abuses of this highly sensitive data. As biometric technologies become increasingly prevalent in everyday life, the modest safeguards contemplated by the Illinois legislature more than a decade ago are even more essential to protect personal privacy.

II. BIPA APPLIES TO FACE SURVEILLANCE TECHNOLOGIES.

The text, structure, and legislative goals of BIPA show that its opt-in consent and other privacy safeguards fully apply to technologies, like those at issue here, that identify and track people based on their faces—one of our most exposed and sensitive sources of biometrics.

BIPA expressly defines "biometric identifier" to include a "scan" of "face geometry." 740 Ill. Comp. Stat. 14/10. This language contains no qualifications or limitations. It is tailor-made for face recognition technology. Further, BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* Thus, "biometric information" includes any information

"based on" a scan of face geometry. Thus, contrary to Facebook's suggestion, *see* Appellant's Br. 19, BIPA applies to face recognition technology and all information derived from it.

BIPA's legislative findings buttress this conclusion. The law identifies two key attributes of biometrics that make them extraordinarily hazardous to privacy: first, they are "biologically unique to the individual"; and second, "once compromised, the individual has no recourse." 740 Ill. Comp. Stat. 14/5(c). Our faces exemplify both of these attributes: each is unique, and cannot be altered. BIPA's findings also emphasize that "the full ramifications of biometric technology are not fully known." *Id.* 14/5(f). This shows a need to interpret BIPA flexibly to cover emerging biometric technologies, including face recognition. Further, BIPA's findings specify that "major national corporations" operate biometric technologies in Illinois. *Id.* 14/5(b). Facebook is one of the largest corporations conducting face recognition in Illinois, and indeed, the entire world.

BIPA's exclusion of "photographs" from the definition of "biometric identifier" is not to the contrary. *Id.* 14/10. BIPA is most coherently read to provide that while a photograph itself is not a "biometric identifier," a scan of face geometry from an image in a photograph *is* a biometric identifier. In other words, it would not implicate BIPA for a company to create or obtain a set of digital images of people's faces, because those images are merely photographs. But BIPA *is*

implicated by processing those images to create a "scan of . . . face geometry"—sometimes called a faceprint—which is data wholly distinct from the photographic image itself.[22] Any conclusion to the contrary would allow for easy circumvention of the statute's core protections even in situations where a company is collecting face scans of people who are physically present with the scanner, by allowing the company's equipment to create a digital image (a "photograph") of the person's face, and then instantaneously conduct a facial geometry scan using the image rather than the physical face itself.[23]

This Court should reject any suggestion that the key statutory term "scan" is limited to situations where a scanned person is physically present. *See In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d at 1171–72 (rejecting this

[22] "A faceprint or facial template is essentially a digital code that a facial recognition algorithm creates from an image." U.S. Gov't Accountability Off., GAO-15-621, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law* 3 n.5 (2015), https://www.gao.gov/assets/680/671764.pdf.

[23] Alternately, this Court can follow the court below in interpreting the term "photographs" to mean paper photographs. *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016). Like other items in the same statutory list of excluded items (including written signatures, height, weight, hair color, and eye color), paper photographs are a lesser threat to biometric privacy. Moreover, this interpretation gives full and coherent meaning to all of BIPA's statutory terms, including "scan of face geometry." *See generally S. Illinoisan v. Ill. Dep't of Pub. Health*, 844 N.E.2d 1, 14 (Ill. 2006) ("words and phrases should not be construed in isolation, but must be interpreted in light of other relevant provisions of the statute").

argument advanced by Facebook in this litigation). There is no textual support for this limitation, and courts should not "depart from the plain statutory language by reading into [a] statute exceptions, limitations, or conditions that the legislature did not express." *People v. Lewis*, 860 N.E.2d 299, 305 (Ill. 2006). Moreover, such a limitation would contradict BIPA's substantive rule that a private entity may not "collect, capture, purchase, receive through trade, *or otherwise obtain*" a person's biometrics without their consent. 740 Ill. Comp. Stat. 14/15(b) (emphasis added). Scanning the image of an absent person is clearly a means to "otherwise obtain" their biometrics. Nor does anything in the history or purpose of BIPA require such a crabbed interpretation, which would strip BIPA protections from anyone whose biometrics are scanned from an image of their face (as well as from an image of their retina, iris, or hand, or even a fingerprint inked onto a card and only later electronically scanned). Indeed, as the Government Accountability Office explains, "There are generally four basic components to a facial recognition technology system: a camera to *capture an image*, an algorithm to create a faceprint (sometimes called a facial template), a database of stored images, and an algorithm to compare the captured image to the database of images . . . ." GAO, Facial Recognition Technology, at 3 (emphasis added). Interpreting BIPA to apply only to in-person scanning would remove from the Act's coverage the typical way in

which facial biometric scanning is conducted—by first capturing an image (i.e., a digital photograph) of a person's face.

For the reasons above, courts have consistently held that BIPA applies to face recognition technology. *See Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, **2–5 (N.D. Ill. 2017); *Rivera v. Google Inc.*, 238 F. Supp. 3d. 1088, 1092–1100 (N.D. Ill. 2017); *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1105–06 (N.D. Ill. 2015). *See also In re Facebook Biometric Information Privacy Litig.*, 185 F. Supp. 3d at 1170–72 (decision below on this point).

III. 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.

Among the issues Facebook has raised to this Court is whether Facebook's failure to comply with the substantive provisions of BIPA is sufficient to show that the plaintiffs are "aggrieved." Appellant's Br. 46–48. *Amici* support the plaintiffs' position that performing a scan of an individual's face without disclosing how that information will be stored, used, or destroyed, and without properly obtaining written consent, creates an actionable privacy harm. Notice and informed consent empower individuals to protect their privacy and are central to privacy laws in the United States, generally, and to 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. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1028 (2012). 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*, at 7. 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."[24] As the federal

[24] 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).

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.[25]

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

[25] Fed. Off. of Mgmt. & Budget, Circular No. A-130, *Management of Federal Information Resources* (Dec. 25, 1985, Revised 2016).

information and the privacy practices of health plans and health care providers."[26] The U.S. Department of Health and Human Services has explained that "[t]rust in electronic exchange of individually identifiable health information can best be established in an open and transparent environment."[27] Failure to provide effective notice 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

[26] 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.

[27] Off. 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), https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

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 obtained at the time of the disclosure or in advance. 18 U.S.C. § 2710(b)(2)(B).

Importantly, notice requirements offer businesses minimum standards to follow. Recognizing the Orwellian potential of two-way cable television systems, Congress passed the Cable 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 to provide a "separate, written statement" that "clearly and conspicuously informs" subscribers of the nature of the information collected, the nature and purpose of any disclosure of that information, and the period the information will be retained, among other facts. 47 U.S.C. § 551(a)(1). The CCPA also requires cable companies to obtain the customer's opt-in consent before collecting or disclosing personally identifiable information about them. *Id.* § 551(b)(1), (c)(1). These provisions specify 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. *Id.* § 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.

IV. NOTICE IS A SUBSTANTIVE RIGHT UNDER BIPA.

The requirement that a company provide adequate notice is essential to BIPA's statutory purpose. The legislature enacted BIPA in response to concerns about the risks posed by biometric data collection. Legislators were especially concerned with biometric data collected in stores and other functionally nonvoluntary environments. 740 Ill. Comp. Stat. 14/5. At the time of enactment, Pay By Touch, a vendor that supplied fingerprint scan technology to Illinois grocery stores, had recently 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."[28] Legislative findings specifically noted that consumers were unaware of the connection between biometric data and other personal information. 740 Ill. Comp. Stat. 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"). 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." *Id.* 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." *Id.* 14/15(b)(3) (emphasis added). A "written release" is defined in the statute as "informed written consent." *Id.* 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

[28] 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.

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.

Accordingly, an Illinois appellate court recently confirmed that BIPA's plain language creates a "legal right" to notice before a private entity collects a person's biometric data. *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175, ¶ 52. Failure to give such notice is not merely a "technical" violation of the Act but an invasion of individual rights. The court rejected the defendant's argument that a person is not injured under the statute until her biometric data "has actually been compromised," noting that "the whole purpose of the Act is to prevent any harm from occurring in the first place, thereby reassuring the public, who will then be willing to participate in this new technology." *Id.* at ¶ 59. The Act does not merely protect consumers against the improper use or disclosure of their data; it protects their right to make an informed decision about whether to entrust a particular private entity with their information.

In the present case, the district court properly understood that notice plays a fundamental role in enabling an individual's control of his or her data. In evaluating the existence of a concrete injury, the court explained that when companies simply disregard BIPA's notice and consent requirements "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). Violation of BIPA's requirements enacts a substantial harm on individuals denied the right to receive notice and provide consent.

V. 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.

The Illinois legislature understood that strong, private enforcement mechanisms were essential to fulfilling BIPA's purpose. The defendant's cramped understanding of BIPA's enforcement provisions finds no support in the language of the statute. "The plain language of the Act states that any person 'aggrieved by a violation of this Act' may sue. . . . It does *not* state that a person aggrieved by a violation of this Act—*plus* some additional harm—may sue." *Sekura,* 2018 IL App (1st) 180175, at ¶ 50.

"[T]he overall structure of the Act also supports plaintiff's right to sue." *Id.* at ¶ 51. For example, the statute includes "liquidated damages" provisions guaranteeing that an individual will receive the greater of actual damages or $1,000

for each negligent violation of the act and $5,000 for each intentional or reckless violation of the act. 740 Ill. Comp. Stat. 14/20(1), (2). These statutory liquidated damages provisions "establish[] that actual damages are not required to obtain relief under the Act," *Sekura*, 2018 IL App (1st) 180175, at ¶ 51, and are further evidence that the Illinois legislature intended to provide a private cause of action based solely on injury to the statutory rights to notice and informed consent.

Moreover, as the *Sekura* court explained, BIPA's enforcement mechanisms are strikingly similar to those of the Illinois AIDS Confidentiality Act, a statute meant to address patients' "fear that test results . . . will be disclosed without their intent," in a situation where "disclosure can create irreparable harm." 2018 IL App (1st) 180175, at ¶ 70 (*quoting* 410 Ill. Comp. Stat. 305/2). Like BIPA, the AIDS Confidentiality Act provides a right of action to "[a]ny person aggrieved by a violation of this Act." 410 Ill. Comp. Stat. 305/1. Both statutes allow liquidated or actual damages, as well as other remedies such as an injunction. Both allow recovery of reasonable attorneys' fees.[29] Given this statutory scheme, an Illinois appellate panel "unanimously agreed that a person could recover liquidated damages without proof of actual damages." *Sekura*, 2018 IL App (1st) 180175, at ¶ 71 (citing *Doe v. Chand*, 781 N.E.2d 340 (Ill. App. 2002)). This interpretation "of

[29] BIPA also permits recovery of "costs, including expert witness fees and other litigation expenses," further demonstrating that the legislature intended to make it feasible for individuals to enforce the statute. 740 Ill. Comp. Stat. 14/20(3).

a statute that is similar in purpose and wording to [BIPA] further supports our finding that plaintiff may sue for a violation of the Act without proving additional harm." *Id.* at ¶ 72.

Finally, unlike many other statutes that protect individual rights against incursions by private entities, BIPA gives no enforcement authority to the Illinois Attorney General. *See, e.g.*, Illinois Human Rights Act, 775 Ill. Comp. Stat. 5/10-101, 102 (Individuals may sue to vindicate their own rights, and attorney general may sue when there is a pattern or practice of discrimination). Private actions are the only mechanism for enforcing all of BIPA's requirements—including the notice and informed consent requirements—and the legislature took pains to encourage such actions.

Taken together, BIPA's plain language, purpose, and structure show that the Illinois legislature intended 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, 1143 (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.[30]

[30] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C.A. § 1681n; Cable Commc'ns Pol'y 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.[31] 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

---

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

[31] *See*, *e.g.*, California's Invasion of Privacy Act, Cal. Penal Code § 637.2; Ohio's Tel. Solicitation Sales Act, Ohio Rev. Code Ann. § 4719.12; Tennessee's Video Consumer Privacy Act, Tenn. Code Ann. § 47-18-2201; Connecticut's Commc'ns Consumer Privacy Act, Conn. Gen. Stat. Ann. § 53-422; Michigan's Pres. of Pers. Privacy Act, Mich. Comp. Laws Ann. § 445.1715.

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, 53 Wm. & Mary L. Rev. at 1151 (collecting examples); *see also* Pridgen, *Wrecking Ball Disguised as Law Reform*, 39 N.Y.U. Rev. L. & Soc. Change 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 in BIPA, are an important feature of private enforcement regimes, especially in the context of consumer protection and consumer rights. *See*, *e.g.*, Pridgen, 39 N.Y.U. Rev. L. & Soc. Change 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. For example, the Illinois Supreme 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.*, 47 P.3d 1222, 1229 (Haw. 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"). This compliance-encouraging 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 Ill. Comp. Stat. 14/5(f).

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

If this Court ultimately concludes that the plaintiffs in this case are not "aggrieved persons" under BIPA without additional showings of harm, not only would these plaintiffs be unable to hold this defendant accountable for its violation

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, 53 Wm. & Mary L. Rev. 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, 53 Wm. & Mary L. Rev. 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 defendant's reading of BIPA would effectively gut the statute's primary purpose and leave people without meaningful recourse in a world of rapidly advancing technology and proliferating uses of biometric information.

//

//

//

//

//

//

//

//

//

//

//

//

//

Dated: December 17, 2018

Respectfully submitted,

s/ Nathan Freed Wessler

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

Rebecca K. Glenberg
Roger Baldwin Foundation of ACLU, Inc.
150 North Michigan Ave., Suite 600
Chicago, IL 60601
(312) 201-9740
rglenberg@aclu-il.org

Jacob A. Snow (CA Bar No. 270988)
American Civil Liberties Union Foundation of Northern California, Inc.
39 Drumm St.
San Francisco, CA 94111
(415) 621-2493
jsnow@aclunc.org

Attorney for American Civil Liberties Union Foundation of Northern California and American Civil Liberties Union Foundation of Southern California

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

Jennifer Lynch
Adam Schwartz
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org
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

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 6,993 **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/ Nathan Freed Wessler **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