No. 22-16925

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CLAYTON P. ZELLMER, on behalf of himself and all others similarly situated,

Plaintiff-Appellant,

v.

META PLATFORMS, INC.,

Defendant-Appellee.

On Appeal from the United States District Court
for the Northern District of California, Case No. 3:18-cv-01880-JD
Honorable James Donato

BRIEF OF *AMICUS CURIAE* SECURITY INDUSTRY ASSOCIATION IN SUPPORT OF DEFENDANT-APPELLEE META PLATFORMS, INC., AND AFFIRMANCE OF THE DISTRICT COURT

Roman Martinez
Jeremy L. Brown
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-2200

Gary Feinerman
LATHAM & WATKINS LLP
330 N Wabash Ave
Suite 2800
Chicago, IL 60611
(312) 876-7700

Counsel for Amicus Curiae Security Industry Association

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29, the undersigned counsel of record certifies that Security Industry Association, a non-profit business association, has no parent corporation and that no publicly held corporation holds 10% or more of its stock.

s/ Roman Martinez
Gary Feinerman
LATHAM & WATKINS LLP
330 N Wabash Ave
Suite 2800
Chicago, IL 60611
(312) 876-7700

Roman Martinez
Jeremy L. Brown
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-2200

Counsel for Amicus Curiae Security Industry Association

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

TREATISES

OTHER AUTHORITIES

INTERESTS OF *AMICUS CURIAE*[1]

The Security Industry Association is a non-profit trade association representing thousands of security professionals and more than 1,400 safety and security providers. The Association's members include manufacturers, developers, and users of security applications that rely on biometric technologies, such as facial recognition and fingerprint scanning, and that are used by individuals, schools, hospitals, and businesses across the country. Plaintiff Clayton Zellmer's claims rest on an incorrect reading of the Illinois Biometric Information Privacy Act, ("BIPA"), 740 ILCS 14/1 *et seq.*, that would frustrate—and in some cases make effectively impossible—the lawful use of those security applications in Illinois.

INTRODUCTION AND SUMMARY OF ARGUMENT

On its face, this case is about Tag Suggestions, a Facebook feature that uses facial-recognition technology to identify a user's Facebook friends in photographs uploaded to the site. But this case really is about much more. It implicates the fundamental processes underlying essential biometric security applications used across the country, and it threatens the continued use of those applications in Illinois.

---

[1] *Amicus curiae* has not been retained by any party to this action. This brief was not authored in whole or in part by counsel for any party. No party or person other than *amicus curiae* or its members and their counsel made a monetary contribution that was intended for preparation or submission of this brief.

Biometrics are a means to authenticate a person's identity based on biological characteristics. This makes biometrics a natural fit for security applications, where their use is becoming increasingly commonplace. Homeowners install biometric video doorbells, allowing them to grant access to family members and friends while also receiving alerts to the presence of strangers. Businesses deploy facial-recognition and fingerprint scanning to secure physical assets and voice recognition to protect customer data. And schools use facial-recognition systems at entrances to protect students and staff, while fingerprint scanners assist administrators with student recordkeeping.

Wherever they are used, biometric authentication systems follow the same basic processes. To fulfill its basic function, a biometric security system must enroll a set of authorized individuals, detect biometric features presented for authentication, and grant access to approved individuals while excluding others. For this to work, the system must retain the biometric data of enrolled individuals so that they can be authenticated in future encounters. The system need not retain the biometrics of unenrolled persons, but it inevitably will scan some such persons in the course of performing its functions. The reason is obvious: To determine whether to grant access to an individual encountering a biometric security system, the system must compare that individual's scan to those of approved and enrolled persons, and it is

impossible to determine in advance whether the scan will match that of an enrolled person.

Zellmer's claim depends upon an interpretation of BIPA that would in practice outlaw these basic processes. Zellmer does not use Facebook and never has. But when a Facebook user uploaded photographs in which Zellmer appeared, Facebook applied Tag Suggestions to try to identify him. Tag Suggestions did not identify Zellmer—it couldn't, lacking any data on him as a non-user—and it immediately deleted the scan after failing to match him to any of the uploader's Facebook friends. Nonetheless, Zellmer claims that Facebook violated BIPA because he did not consent in writing to the scan and because Facebook had not established and published a satisfactory data-retention schedule.

If accepted, Zellmer's extraordinarily expansive view of BIPA would have harmful ramifications extending far beyond the social media landscape. Like Tag Suggestions, biometric security applications will inevitably scan persons whom they cannot identify, to whom they could not possibly make BIPA disclosures, and from whom they could not possibly obtain a written release. That should not be illegal, especially when the scans are immediately deleted if no match is made. The Illinois General Assembly could not possibly have intended—and in fact did not intend—to prohibit these basic security functions.

This brief has two primary aims. *First*, it describes the widespread beneficial use of biometric security applications and explains how they work. As mentioned, these applications all employ the same basic processes to protect people and secure data: enroll known persons and store their biometrics, detect the biometrics of individuals attempting to gain access, and authenticate or reject those individuals based on whether their biometrics match any enrollee's biometrics. These processes resemble those underlying Tag Suggestions—and if Zellmer's interpretation of BIPA prevails, they would become unlawful, inflicting significant harm to the public.

Second, this brief demonstrates that BIPA does not prohibit the basic processes employed by biometric security systems. When enacting BIPA, the General Assembly expressed concern that "[a]n overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information." 140 ILCS 14/5(d). At the same time, the legislature was careful to recognize that "[t]he use of biometrics is growing in the … security screening sector[] and appears to promise streamlined … security screenings." *Id.* 14/5(a). BIPA's operative text and structure reflect the same positive view of biometric security applications: The statute does not regulate data that a biometric application cannot use to identify a particular individual, and it does not regulate ephemeral scans that are immediately deleted. Because unretained scans of data that a biometric application cannot use to identify a specific person do

not implicate the privacy concerns that prompted BIPA's enactment—and do not violate BIPA's prohibitions—this Court should affirm the dismissal of Zellmer's suit.

ARGUMENT

I. ZELLMER'S INTERPRETATION OF BIPA THREATENS THE USE OF BIOMETRIC SECURITY APPLICATIONS IN ILLINOIS

A key function of a security system is to confirm that you are who you say you are. One way to prove your identity is with an object you have—a key, a fob, or a security card. Another way to prove your identity is with something you know—a password, a PIN, or your mother's maiden name. A third way is biometrics. Unlike objects you hold, your facial geometry, fingerprint, or voice cannot be lost or stolen. And unlike something you know, they cannot be shared or forgotten.

Because of their convenience and enhanced security potential, biometric security systems are increasingly commonplace. Individuals use biometric video doorbells to monitor their homes, and private businesses employ biometric security systems to secure their facilities and safeguard customer data. Hospitals deploy biometric systems to solve complex security and access problems, while schools use them to protect students from bad actors and to facilitate student recordkeeping. While biometric security applications vary, they all detect biometrics presented to them to distinguish between enrolled and unenrolled individuals. This inevitably entails scanning unknown individuals whom a biometric security system has not

encountered, to whom the system's owner cannot feasibly provide notice, and from whom the owner cannot feasibly obtain written consent.

A. Biometric Security Applications Are Increasingly Used by Individuals, Schools, Hospitals, and Businesses

Biometrics have proven to be an effective tool to quickly and accurately identify individuals. This has been demonstrated most visibly, though not exclusively, in the law enforcement and public safety arenas.

Law enforcement agencies use facial-recognition tools to quickly and accurately solve crimes. To do so, officials compare the face of an unknown suspect in a video or image with a broader set of images of known persons. The NYPD, for example, compared images of a suspect who had placed rice cookers—hoax bombs, fortunately—in the New York City subway with images in its arrest database, allowing officers to identify the suspect in just one hour. *See* Jake Parker, *Facial Recognition Success Stories Showcase Positive Use Cases of the Technology,* Security Industry Association (July 16, 2020), https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology. Across the country, federal, state, and local agencies use similar tools to apprehend suspects who might otherwise go unidentified. *See id.*

The Department of Homeland Security uses facial-recognition at over 200 international airports and dozens of land entries and seaports to verify travelers. The

agency's system, Simplified Arrival, speeds up the entry process while also detecting fraudulent documents. *See* U.S. Customs and Border Protection, *Biometrics*, https://www.cbp.gov/travel/biometrics/airports (last visited August 28, 2023). And the nonprofit organization Thorn developed a facial-recognition tool to fight child sex trafficking. The tool, called Spotlight, scans online sex advertisements for images of missing children. In collaboration with law enforcement, Thorn has used Spotlight to rescue victims of human trafficking. Tom Simonite, *How Facial Recognition Is Fighting Child Sex Trafficking*, Wired (June 19, 2019), https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/.

Biometrics are not limited to law enforcement and public safety functions performed by federal, state, and local governments—entities that are exempt from BIPA's scope. *See* 740 ILCS 14/10, 14/15, 14/25(e). Pertinent here, the use of biometrics for security purposes is common among individuals, schools, hospitals, and businesses—which, with the exception of public schools, public hospitals, certain financial institutions, and certain healthcare uses, are not exempt from BIPA. *See*, *e.g.*, *id*. 14/10, 14/25(c).

Starting at home, biometrics have become regularly integrated into residential security systems. A homeowner can program video doorbells, security cameras, or fingerprint pads to recognize family members, friends, and other known persons.

See Amy Gamerman, *Home Is Where They Know Your Name (and Face, Hands and Fingerprints)*, Wall St. J. (June 20, 2019) ("Home is Where They Know Your Face"), https://www.wsj.com/articles/home-is-where-they-know-your-name-and-face-hands-and-fingerprints-11561047729. Once programmed, the system can unlock the door for approved individuals while sending an alert to the homeowner when an unknown person is present. *See Face Recognition Door Lock: How It Works*, Sure Lock & Key, https://surelockkey.com/blog/face-recognition-door-lock-how-it-works/ (last visited August 28, 2023).

Similar systems offer safety and convenience in apartment buildings. Installed at entrances, biometric-enabled cameras allow residents to give access to approved individuals, such as a babysitter or dogwalker, while denying entry to others. Such cameras can also detect unapproved individuals who attempt to "tailgate" into buildings. *See* Gamerman, Home is Where They Know Your Face; Kara Klein, *Emerging Uses of Facial Recognition Technology in the Private Sector*, Security Industry Association (Dec. 9, 2019), https://www.securityindustry.org/2019/12/09/emerging-uses-of-facial-recognition-technology-in-the-private-sector-highlights-from-itif-briefing/.

Biometric entry systems are especially helpful for populations who may be more likely to lose a key or forget a PIN. One study analyzed the effectiveness of facial-recognition locks at assisted-living homes. Prior to implementation, facility

staff expressed security concerns with the existing keycode systems—staff members often shared their codes with each other, residents sometimes figured out the staff codes, and the codes remained unchanged for years despite high staff turnover. H. L. Bradwell et al., *Facial Recognition Lock Technology for Social Care Settings: A Qualitative Evaluation of Implementation of Facial Recognition Locks at Two Residential Care Sites*, 5 Frontiers in Digit. Health, Mar. 2023, at 5. In implementing the facial-recognition system, staff, residents, and approved visitors were given the opportunity to voluntarily enroll by providing images of their faces. *Id.* at 3. Users reported enhanced security as a result of reduced PIN sharing and a more accurate accounting of persons in the building. *See id.* at 5-6, 10. As an additional benefit, the facial-recognition cameras protected residents by distinguishing those who could and could not safely leave on their own. *See id.* at 10.

Biometrics also significantly improve security at schools. Placed near an entrance or campus perimeter, facial-recognition cameras can alert school officials to potentially dangerous trespassers. Chris Schulz, *Four Counties To Implement Facial Recognition For School Safety*, W. Va. Public Broadcasting (May 11, 2023), https://wvpublic.org/four-counties-to-implement-facial-recognition-for-school-safety/. At a high school graduation in Texas, for example, facial-recognition technology alerted officials to the presence of a student in an alternative program who was forbidden from attending, allowing officials to escort him away without

incident. Kathryn Eastburn, *Texas City Schools Champion Use of Facial Recognition Technology*, Galveston Cnty. Daily News (Oct. 26, 2019), https://www.galvnews.com/news/texas-city-schools-champion-use-of-facial-recognition-technology/article_ce9c45ae-e309-5da6-b035-0796a8de86dd.html. The school's system works in the same manner to detect registered sex offenders or trespassers who have been previously banned from school grounds. *See id.*

School administrators also use biometric systems for efficient management and convenient recordkeeping. Students can enroll in biometric rosters by providing face scans, and administrators, using the same cameras that detect trespassers, use these rosters to simplify attendance-taking. Schools also deploy fingerprint scanning to allow access to school facilities, with students using their fingerprints to log onto computers, check out library books, or pay for lunch. *See* Emily Ann Brown, *Biometric Security Boosts School Safety and Efficiency*, District Administration (Mar. 19, 2019), https://districtadministration.com/biometric-security-boosts-school-safety-efficiency/.

Biometrics also find special uses in hospitals, which face especially complex security problems and heightened hygiene concerns. Hospital campuses often house many entities performing different functions, from inpatient and outpatient care, to research and teaching, to maintaining patient records and conducting clinical trials. Such campuses are visited by a corresponding diversity of visitors and staff, each

authorized to access just part of the campus. Using biometrics, administrators can enroll each individual in a facial-recognition system, providing simplified access to each enrollee's authorized locations while guarding against tailgating into restricted areas. The system implemented by the Dana Farber Cancer Institute, for example, allows easy travel around the campus by "quickly scan[ning] a person's face [in] less than one second to verify his or her access permission status." David Dunlap, *Securing Our Hospitals and Protecting Your Privacy*, Campus Security & Life Safety 10 (Mar./Apr. 2019), https://digital.1105media.com/SP/2019/CSS_1904/SI_APR19_SUP_CSLS_701922949.html#p=10.

These systems also reduce infection risk at hospitals by minimizing the need for keycards and PIN pads. A surgeon who has just scrubbed her hands, for example, can enter the operating room by scanning her face. Tori Whitacre Martonicz, *Facial Recognition Revolutionizes Health Care Facility Safety and Infection Control*, Infection Control Today (Nov. 7, 2022), https://www.infectioncontroltoday.com/view/facial-recognition-revolution-health-care-facility-safety-infection-control; Don Erickson, *Touchless Interface for Hygienic Access in Health Care and Travel*, Morning Consult (Apr. 24, 2020), https://morningconsult.com/opinions/touchless-interface-for-hygienic-access-in-health-care-and-travel/.

Businesses use biometric-entry systems to secure their facilities and protect their employees. *Face Facts: Dispelling Common Myths Associated with Facial Recognition Technologies*, Security Industry Association 2 (2019) ("Facial Recognition Technology"), https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf. Beyond physical security, businesses use biometrics to protect customer data, such as when a fingerprint or "faceprint" is used to access a smartphone or when banks use voice recognition to eliminate fraud. One British bank, for example, found that implementing voice recognition cut attempted telephone fraud in half, saving its customers nearly $350 million in a single year. Daphne Leprince-Ringuet, *The Latest Defence Against Banking Scams: Your Voice*, ZDNet (May 7, 2021), https://www.zdnet.com/article/the-latest-defence-against-banking-scams-your-voice/.

These examples illustrate just some of the many ways in which biometrics protect people, property, and data, offer convenience, and promote peace of mind.

B. Biometric Security Applications Cannot Lawfully Function Under Zellmer's Flawed Reading of BIPA

As noted, biometric authentication systems do three things: (1) enroll a set of authorized persons and store their biometrics; (2) detect the biometrics of persons presented for verification; and (3) identify and authenticate enrolled persons while rejecting unenrolled persons. *See Biometric Technologies*, Fingerprints White Paper

6, 17 (2020) ("Biometric Technologies"), https://www.securityindustry.org/wp-content/uploads/2021/04/Biometric-Technologies-Fingerprints-White-Paper-SIA-Center-of-Excellence.pdf; Simon Liu & Mark Silverman, *A Practical Guide to Biometric Security Technology*, IT Pro 28 (Jan./Feb. 2001) ("Guide to Biometrics").

At the enrollment stage, a biometric security system defines the set of authorized persons whom the system will authenticate in future scans. To enroll, a person provides a sample of his biometric identifier, such as a fingerprint scan or a headshot. *See* Facial Recognition Technology at 2; Biometric Technologies at 9. The system operator can make appropriate disclosures and obtain written consent at this stage, including the disclosures and consent required by BIPA. *See* 740 ILCS 14/15(b).

Using the enrollee's sample, the system analyzes the biometric identifier's essential features. For example, a facial recognition scanner will take detailed measurements of a face's dimensions and convert those measurements into a mathematical value—usually called a biometric "template"—that is retained for comparison with future authentication attempts. *See* Biometric Technologies at 12; Liu & Silverman, Guide to Biometrics at 29; Facial Recognition Technology at 2. After creating the template, the system has no need to keep the sample originally provided by the enrollee, and the template itself cannot be reverse engineered to create the original fingerprint or photograph. *See* Facial Recognition Technology at

7. As a result, biometric templates are typically strings of numbers that are entirely meaningless outside the security system in which they are used. *See id.* at 2, 7.

After enrollment of authorized persons, the system is ready to detect and authenticate. Detection occurs when an individual seeking entry or access presents his biometric feature(s) for scanning—for example, by placing a thumb on a fingerprint scanner or approaching a facial-recognition camera. The system calculates a mathematical value or template for the detected biometric feature, and then compares that template with the stored enrollee templates using an algorithm—and, if the values are close enough, it finds a match. *See* Facial Recognition Technology at 2; Liu & Silverman, Guide to Biometrics at 28. Unlike enrollee templates—which are necessarily retained for future authentication attempts—templates associated with attempted authentications can be immediately deleted. *See* Stelvi Cimato, Roberto Sassi, and Fabio Scotti, *Biometrics and Privacy*, 1 Recent Pats. on Comput. Sci. 98, 102 (2008). The entire detection and authentication process can take less than a second. *See* Facial Recognition Technology at 9; Biometric Technologies at 26.

These enrollment, detection, and authentication steps apply generally across biometric security and authentication systems. *See* Biometric Technologies at 6. Important here, they resemble the same general processes used by Tag Suggestions. To implement Tag Suggestions, Facebook creates face templates for Facebook users,

SER-91, the functional equivalent of an employee providing her headshot or fingerprint to enroll in an office security system. Next, Facebook detects faces appearing in images uploaded by users—regardless of whether those appearing in the image are Facebook users (and thus enrolled) or non-users (and thus unenrolled). SER-90. For each detected face, Facebook calculates a "face signature" to compare with the face templates of the uploading user's Facebook friends. SER-90. But Facebook can make a match and suggest a tag only for Facebook users, whom it can identify—and not for non-users, whom it cannot identify. SER-96; *see also* ER-15 (district court's summary judgment opinion observing that "Zellmer and the putative class are by definition entirely unknown to Facebook"). And after attempting to make a match, all face signatures—of users and non-users alike—are immediately deleted. Facebook Br. at 50-51.

Zellmer's interpretation of BIPA would effectively prohibit these basic processes. In his view, Tag Suggestions violates BIPA merely by attempting to identify someone in a photograph without having first made disclosures to and obtaining a written consent from that individual. As Facebook observes, *id*. at 25, that would make it unlawful to use Tag Suggestions at all. To properly function, Tag Suggestions must determine whether an individual appearing in a photograph is a Facebook user. In making this determination, Tag Suggestions will inevitably scan images of people who are *not* Facebook users. Zellmer's argument that such

incidental scans of non-users violate BIPA—even when any biometric data created with the scan is immediately deleted—essentially outlaws *any* use of Tag Suggestions. Zellmer recognizes as much, arguing that Facebook can comply with BIPA by "shutting down its face-recognition system." Zellmer Br. at 25; *see also* SER-61 (arguing that Facebook can comply by "refrain[ing] from scanning photos uploaded from Illinois").

Zellmer's view would likewise effectively outlaw biometric security applications. A biometric security camera, for example, will scan facial images appearing in a defined field of view, such as near a door. This process will inevitably scan persons who have not enrolled—effectuating the system's basic, beneficial function—and thus who have not consented in writing to being scanned by the camera (and who also cannot be identified by the system). Indeed, Zellmer contends that such a scan is unlawful even if it is deleted within a fraction of a second. SER-69 (arguing that Facebook "[went] so far as to create and compare" Zellmer's face signature to the face templates of the uploading user's Facebook friends). That reading of BIPA is untenable and would frustrate, if not eliminate, the use of biometric security technologies in Illinois.

Fortunately—as explained by Facebook and further explained below—that interpretation is erroneous. BIPA does not make illegal the wide array of beneficial

biometric security systems in use across the country, and these systems are compliant even without "shutting [them] down" in Illinois. Zellmer Br. at 25.

II. BIPA'S TEXT, STRUCTURE, AND HISTORY CONFIRMS THAT BIOMETRIC SECURITY APPLICATIONS DO NOT VIOLATE BIPA

The Illinois General Assembly enacted BIPA fully aware of the valuable security applications enabled by biometric technology. As the statute's history shows, the General Assembly sought to encourage the development and use of biometric technologies while also protecting the privacy of Illinois residents, particularly as to biometric data connected to financial accounts. This statutory intent is reflected in BIPA's text and structure, which demonstrate that it covers only certain types and uses of biometric data. Specifically, BIPA does not apply to biometric scans that are not used to identify an individual, or to ephemeral scans of data that are immediately deleted.

A. BIPA Was Prompted by Specific Privacy Concerns for Biometric and Financial Data

The General Assembly enacted BIPA in the wake of the bankruptcy of Pay By Touch, a biometric payments company. The company had developed a retail payment system that allowed shoppers to pay for purchases with a fingerprint scan. Pay By Touch's customers provided their fingerprint scans to the company, which connected the scans to customer financial accounts in order to facilitate payments. *See* Michael Garry, *Biometric Payment Ends After Vendor Files Bankruptcy*,

Supermarket News (Mar. 31, 2008), https://www.supermarketnews.com/technology/biometric-payment-ends-after-vendor-files-bankruptcy. The bankruptcy left the fate of those databases uncertain. As BIPA's sponsor explained, "thousands of customers from Albertson's, Cub Foods, Farm Fresh, Jewel Osco, Shell, and Sunflower Market [were] wondering what will become of their biometric and financial data." 95th Ill. Gen. Assem., House Proceedings, May 30, 2008, at 249 (statement of Representative Ryg).

Crucially, the General Assembly did not condemn biometric technology across the board. BIPA's legislative findings begin by observing that "[t]he use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings." 740 ILCS 14/5(a); *see also* Zellmer Br. at 28 (acknowledging that the legislature expected biometrics "to be used as a means for streamlining identification verification with a fast, reliable technology"). The findings proceed to hone in on BIPA's core privacy concerns. Alluding to Pay By Touch, the General Assembly observed that technology companies had selected Illinois to pilot "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias," 740 ILCS 14/5(b), and it found that "members of the public are wary of the use of biometrics *when such information is tied to finances and other personal information*," *id.* 14/5(d) (emphasis added).

The legislative findings make clear that the General Assembly did not intend for BIPA to govern *all* biometric applications—even among entities and uses that the statute does not categorically exempt. To the contrary, the legislature recognized the value of biometric applications and sought to advance their use consistent with specific privacy concerns. As explained below, BIPA aims to accomplish that goal by imposing tailored regulations on certain uses of certain types of biometric data under certain circumstances. And as the Illinois Supreme Court has made clear, the legislature intended that "[c]ompliance" with these regulations "should not be difficult," let alone practically impossible. *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019).

B. Scans of Unidentifiable Persons Are Not "Biometric Identifiers" or "Biometric Information" Under BIPA

BIPA regulates private entities that collect or store biometric data, including by imposing an informed-consent regime for collecting such data and requiring the publication of a retention schedule. *See* 740 ILCS 14/15(a), (b). BIPA's regulatory regime, however, applies to only certain types and uses of biometric data. Specifically, BIPA governs only "biometric identifiers" and "biometric information," which are defined terms and, as shown below, limited to data that a biometric application can use to identify a particular individual. *See id*. 14/10, 15. When a biometric system scans data that the system cannot use to identify the person to

whom the data belongs—because that person is not enrolled in the system—that data is not a "biometric identifier" or "biometric information" under BIPA.

1. BIPA defines "biometric identifier" in relevant part as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id*. 14/10. In isolation, this definition might be read broadly to include scans that a biometric application cannot connect to a particular identity. But the definition should be read not in isolation, but instead in context and with common sense.

Settled interpretative principles hold that a statutory definition must "must [be] read . . . in light of the term to be defined." *United States v. Doe*, 960 F.2d 221, 225 (1st Cir. 1992) (Breyer, C.J.); *see also Cummins v. Country Mut. Ins. Co.*, 687 N.E.2d 1021, 1025 (Ill. 1997) (plurality opinion) (interpreting an ambiguous definition in the context of surrounding provisions). A statutory definition may accordingly "yield to context" when there are "obvious incongruities" between a term and the broadest possible reading of its definition. *United States v. Olson*, 856 F.3d 1216, 1223 (9th Cir. 2017) (internal quotation marks omitted); *see also, e.g.*, *Bond v. United States*, 572 U.S. 844, 861-62 (2014) (interpreting the defined term "chemical weapon" to exclude toxic chemicals placed on another's personal belongings); *In re Tyrell A.*, 112 A.3d 468, 485 (Md. 2015) (interpreting the defined term "victim" to exclude co-perpetrators). More generally, a court's interpretation of statutory terms should comport with "[c]ommon sense," *Quad Cities Open, Inc.*

v. City of Silvis, 804 N.E.2d 499, 506 (Ill. 2004), and avoid creating "absurd, inconvenient, or unjust results," *People v. Ringland*, 89 N.E.3d 735, 740 (Ill. 2017).

Applying these principles here, a "biometric identifier" must be able to do just that—"*identify* a person." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017) (emphasis added); *see* Merriam-Webster, https://www.merriam-webster.com/dictionary/identifier ("one that identifies"); *Identifies*, Merriam-Webster, https://www.merriam-webster.com/dictionary/identifies ("to ascertain the identity of (someone or something that is unfamiliar or unknown)"); *Identify*, Black's Law Dictionary (11th ed. 2019) ("[t]o prove the identity of (a person or thing)"). A biometric scan that the biometric application cannot associate with personal data stored by the application—such as an apartment building's security system—does not qualify.

This reading makes sense given the items that "biometric identifier" is defined to enumerate—"a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. As a matter of common sense, each item is a means to identify a particular person. *See Rivera*, 238 F. Supp. 3d at 1094 ("Each specific item on the list, not surprisingly, fits within the meaning of the term 'biometric identifier,' that is, a biology-based set of measurements ('biometric') that can be used to identify a person ('identifier')."); *see also, e.g.*, *Voiceprint*, Black's Law Dictionary (11th ed. 2019) ("A distinctive pattern of curved lines and whorls made

by a machine that measures human vocal sounds for the purpose of identifying an individual speaker."). Absent connection to a particular person, a biometric template has no independent significance; it is merely a disassociated numerical value in a security system that cannot properly be called an "identifier."

2. This understanding of the term "biometric identifier" is reinforced by the definition of its counterpart, "biometric information." BIPA defines "biometric information" in relevant part 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*." 740 ILCS 14/10 (emphasis added). Defining "biometric information" in this manner ensures that conversions of a person's biometric identifier—such as through the creation of a numerical template—are "still covered by [BIPA] *if that information can be used to identify the person*." *Rivera*, 238 F. Supp. 3d at 1095 (emphasis added).

The phrase "used to identify an individual" in the definition of "biometric information" makes clear that the term excludes data that a biometric application cannot use to identify a specific person. Indeed, in the district court, Zellmer did not dispute that "biometric information" is limited in precisely that way; instead, he argued that the term "biometric identifier" does not include the same limitation. SER at 35 n.2, 65.

Zellmer was and remains wrong, as the definition of "biometric information" confirms that the term "biometric identifier" is limited to biometric data that a biometric application uses to identify a particular person. The General Assembly added the phrase "used to identify an individual" to the definition of "biometric information" to ensure that BIPA applies only where "biometric identifiers" can "still" identify a specific person. *Rivera*, 238 F. Supp. 3d at 1095. It was unnecessary for the legislature to repeat the phrase "used to identify an individual" to the definition of "biometric identifier" given that term's ordinary meaning and in light of the biometric features enumerated in its definition. Moreover, because BIPA subjects "biometric identifiers" and "biometric information" to the same regulations, *see* 740 ILCS 14/15, the only sensible course is to read both, and not just "biometric information," to exclude biometric data that a biometric application does not use to identify a particular individual. *See Sulser v. Country Mut. Ins. Co.*, 591 N.E.2d 427, 430-31 (Ill. 1992) (interpreting a statute's underinsured motorist and uninsured motorist provisions to have the same effect despite differing language in each).

3. This understanding of BIPA's key terms are further confirmed when "reading the statute as a whole and considering all relevant parts." *Sylvester v. Indus. Comm'n*, 756 N.E.2d 822, 827 (Ill. 2001). Section 15(e) requires that biometric identifiers and biometric information be handled in accordance with the standard of care given to "other confidential and sensitive information." 740 ILCS 14/15(e)(2).

BIPA defines other "confidential and sensitive information" as "personal information that can be used to *uniquely identify* an individual or an individual's account or property." *Id.* 14/10 (emphasis added). BIPA thus can be read as a "harmonious whole" only if "biometric identifier" and "biometric information" are limited to data—like "other confidential and sensitive information"—that a biometric application can use to identify a specific individual. *Sulser*, 591 N.E.2d at 429.

BIPA's consent regime reinforces the point. Sections 15(b) requires a private entity collecting biometric data to inform the subject of the reason for the collection and to obtain the subject's written consent. *See* 740 ILCS 14/15(b). The General Assembly could not have contemplated applying this informed consent requirement to subjects whom a security system cannot identify—and thus from whom consent cannot be obtained.

Reading "biometric identifiers" and "biometric information" to exclude data that a biometric application cannot use to identify a particular person is also consistent with BIPA's underlying purpose of codifying a common law "right of privacy." *W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, 183 N.E.3d 47, 57-58 (Ill. 2021). For common law privacy torts, blackletter law holds that a disclosure is not a privacy invasion unless it is "identifiably about the plaintiff." *Schivarelli v. CBS, Inc.*, 776 N.E.2d 693, 701 (Ill. App. Ct. 2002); *see also Green v.*

Chicago Trib. Co., 675 N.E.2d 249, 254 (Ill. App. Ct. 1996) ("The . . . publication never mentions plaintiff and thus does not invade *her* privacy."); *Newcombe v. Adolf Coors Co.*, 157 F.3d 686, 692 (9th Cir. 1998) ("[I]n order to constitute Newcombe's likeness, the pitcher depicted in the advertisement must be readily identifiable as Newcombe."). It follows, for example, that a person has no claim for the revelation of "his hand, leg or foot, or his house, his automobile or his dog, with nothing to indicate whose they are." *Bayer v. Ralston Purina Co.*, 484 S.W.2d 473, 474 (Mo. 1972) (quoting Prosser, Law of Torts § 112). Nothing in BIPA deviates from that bedrock principle.

For this reason and the others explained above, this Court should hold that biometric scans that a biometric application cannot use to identify a particular individual are not "biometric information" or "biometric identifiers," and thus that BIPA does not regulate such scans.

C. BIPA Does Not Prohibit Ephemeral Scans Of Biometric Data

Nor does BIPA apply to the ephemeral scanning and deletion of material that qualifies under BIPA as a biometric identifier or biometric information. Rather, it applies only to biometric identifiers or information that a biometric application retains. This principle provides an independent ground for affirming the decision below.

Zellmer asserts two BIPA claims. First, he brings a claim under Section 15(a) for Facebook's alleged "possession" of biometric data without publishing a satisfactory "retention schedule." 740 ILCS 14/15(a). Second, he brings a claim under Section 15(b) for Facebook's alleged "collect[ion]" or "capture" of biometric data without properly obtaining consent. *Id.* 14/15(b). But ephemeral scans that are immediately deleted—like Tag Suggestions' scans of Facebook non-users, and like a biometric security camera's scan of an unknown passerby—do not implicate BIPA's core privacy concerns because they pose no risk of being sold or otherwise compromised. For that reason, and as BIPA's text and structure make clear, ephemeral scans do not count as the "possession," "collection," or "capture" of biometric data.

1. BIPA does not define what it means to be "in possession" of biometric data under Section 15(a). The term must accordingly be given its ordinary meaning. *See Holland v. City of Chicago*, 682 N.E.2d 323, 325 (Ill. 1997). According to the Illinois Supreme Court, the ordinary meaning of "possession" is "the act or condition of having in or taking into one's control or holding at one's disposal," *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (quoting Webster's Third New International Dictionary 1770 (1986)), or the "[t]he fact of having or holding property in one's power" or "exercise of dominion over property," *id.* (quoting Black's Law Dictionary 1201 (8th ed. 2004)). Citing *Ward*, the Illinois Appellate Court applied

the same definition of "possession" to the term as used in Section 15(a). *Barnett v. Apple Inc.*, 2022 IL App (1st) 220187, ¶¶ 41-42.

An ephemeral scan of biometric data that is immediately deleted does not rise to the level of "possession" under BIPA. A person cannot reasonably be said to "possess" a neighbor's mail by removing it from her own mailbox, noticing the mail carrier made a mistake, and inserting it in the neighbor's slot. A coffee shop customer does not "possess" a cappuccino handed to him by the barista when, after realizing it isn't the black coffee he ordered, he sets it back on the counter. And the Illinois Appellate Court has held that a suspect does not "possess" drugs if he momentarily inspects them before handing them back to an undercover officer. *See People v. Dumas*, 2011 IL App (2d) 100006-U, ¶¶ 7, 17, 27 (holding that a defendant did not have "dominion or control" over cocaine after holding it "for about 30 seconds" and returning it to an undercover officer); *see also United States v. Kitchen*, 57 F.3d 516, 521 (7th Cir. 1995) (rejecting the argument that possession is established by holding something for a "fleeting moment" of "2 or 3 seconds"). Fleeting handlings or inspections are simply not "possession" under any sensible meaning of the word.

The context provided by the rest of Section 15(a) confirms this conclusion. Section 15(a) requires a private entity "in possession" of biometric data to establish and comply with a "retention" schedule for destroying it. 740 ILCS 14/15(a). But

it makes little sense to require a "retention schedule" for data that is not retained. BIPA's other operative provisions regulate the ways in which entities "in possession" of biometric data may "sell" it, *id*. 14/15(c), "disclose" it, *id.* 14/15(d), or "store, transmit, and protect" it, *id.* 14/15(e). All of the regulated actions require non-ephemeral control over data that automated, instantaneous creation and deletion does not contemplate or allow.

2. BIPA likewise does not define what it means to "collect" or "capture" biometric data under Section 15(b). But Illinois courts have fixed the meaning of these terms as well. Under BIPA, to "collect" is to "to bring together into one body and place," "to gather or exact from a number of persons or sources," or "to gather an accumulation of." *Mosby v. Ingalls Mem'l Hosp.*, 207 N.E.3d 1157, 1168 (Ill. App. Ct. 2022), *appeal denied*, 201 N.E.3d 591 (Ill. 2023). To "capture" is to "record in a permanent file (as in a computer)." *Id.*; *see also Barnett*, 2022 IL App (1st) 220187, ¶¶ 48-49 (providing the same definitions for "collect" and "capture" in Section 15(b)). Consistent with these holdings, courts have recognized that "collect" and "capture" require "something beyond" the mere possession of biometric data. *Jones v. Microsoft Corp.*, __ F. Supp. 3d __, 2023 WL 130495, at *2-3 (N.D. Ill. Jan. 9, 2023) (collecting cases); *see also Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 966 (N.D. Ill. 2020) ("Section 15(b) requires something more than mere possession of biometric data.").

An ephemeral scan of biometric data that is immediately deleted does not "collect" or "capture" biometric data. As explained, ephemeral scans do not even rise to the level of possession, so it necessarily follows that they are not "something *beyond* possession." *Jones*, 2023 WL 130495, at *3 (emphasis added). Further, the meanings of both "collect" ("to gather an accumulation of") and "capture" ("record in a permanent file") connote a sustained—or, at the very least, a non-ephemeral—seizure of biometric data. A biometric security camera that detects an unknown's individual's face, scans it for a match with the biometric features of enrolled persons, does not find a match, and immediately deletes the individual's data—all in less than a second—do not satisfy this standard.[2]

This interpretation is confirmed when reading "collect" and "capture" in accordance with the statutory terms with which they are grouped. *See Dynak v. Bd. of Educ. of Wood Dale Sch. Dist. 7*, 164 N.E.3d 1226, 1232 (Ill. 2020) ("[W]ords grouped in a list should be given related meaning."). Section 15(b) regulates private entities that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. 740 ILCS 14/15(b). Read together, "collect," "capture," "purchase,"

[2] *Cothron v. White Castle System, Inc.*, 2023 IL 128004, is not to the contrary. In that case, the court held that a BIPA claim accrued each time an employee used her fingerprint to clock into work. *Id.* at ¶ 24. But nothing in *Cothron* suggests that the repeated scans were immediately deleted. Moreover, *Cothron* concerned an employee enrolled in a biometric system, not unknown persons who might be detected and scanned by a biometric security scanner. *Id.* at ¶ 4.

and "receive through trade" envision the procurement and *retention* of biometric data. The trailing catchall "otherwise obtain" does not change this conclusion, as it simply ensures that the statute encompasses all like actions. *See Pooh-Bah Enterprises, Inc. v. Cnty. of Cook*, 905 N.E.2d 781, 799 (Ill. 2009) ("[W]hen a statutory clause specifically describes several classes of persons or things and then includes 'other persons or things,' the word 'other' is interpreted to mean 'other such like.'").

Section 15(b) must also be understood in light of Section 15's other four operative provisions. Section 15(a) governs the retention of biometric data; Section 15(c) its sale; Section 15(d) its disclosure and dissemination; and Section 15(e) its storage, transmission, and protection. *See* 740 ILCS 14/15(a), (c), (d), (e). Those four provisions describe actions on biometric data that a biometric application in fact retains—not data that is immediately deleted. Section 15(b) fits into the picture by regulating the process by which retained data is initially obtained: It requires a "written release" from a subject whose biometric data "is being *collected or stored*." 740 ILCS 14/15(b)(1), (3) (emphasis added). This context shows that BIPA cannot sensibly or correctly be read to require a written release for ephemeral scans—scans that do not implicate the narrow privacy concerns prompting the statute's enactment. Unlike the databases of customer data held by Pay By Touch, data that is not retained poses no risk of being sold, disseminated, or stolen.

In sum, the Court should hold that ephemeral scans of biometric data do not violate BIPA.

* * *

BIPA should be interpreted sensibly and in light of its historical privacy purposes without impeding the ubiquitous and valuable use of biometric security systems. This means interpreting BIPA (1) to not regulate biometric data that a biometric application does not use to identify any particular individual and (2) to not regulate ephemeral scans that are immediately deleted. Such a reading is faithful to BIPA's text and structure, and it is the only reading that avoids the untenable result of making it unlawful for individuals, schools, hospitals, and businesses to use biometric security applications in Illinois.

CONCLUSION

For the foregoing reasons, the Court should affirm the district court's judgment.

Dated: August 29, 2023

Respectfully submitted,

s/ Roman Martinez
Roman Martinez
Jeremy L. Brown
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-2200

Gary Feinerman

LATHAM & WATKINS LLP
330 N Wabash Ave
Suite 2800
Chicago, IL 60611
(312) 876-7700

Counsel for Amicus Curiae Security Industry Association

CERTIFICATE OF COMPLIANCE

I hereby certify that pursuant to Federal Rule of Appellate Procedure 32(g)(1), and Ninth Circuit Rule 32-1(e), this brief complies with the type-face and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in a proportionately spaced typeface using Microsoft Word in 14-point Times New Roman; and it complies with the length requirement of Federal Rule of Appellate Procedure 29(a)(5) because it contains 6,788 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f).

August 29, 2023

s/ Roman Martinez
Roman Martinez