

In the
United States Court of Appeals
For the Seventh Circuit

No. 25-1120

G.T., by and through next friend LILIANA T. HANLON, *et al.*,
Plaintiffs-Appellants,

v.

SAMSUNG ELECTRONICS AMERICA, INCORPORATED and
SAMSUNG ELECTRONICS COMPANY, LIMITED,
Defendants-Appellees.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 1:21-cv-4976 — **Lindsay C. Jenkins**, *Judge.*

ARGUED OCTOBER 28, 2025 — DECIDED AUGUST 7, 2026

Before BRENNAN, *Chief Judge*, and JACKSON-AKIWUMI and
LEE, *Circuit Judges.*

LEE, *Circuit Judge.* The photo gallery application in Samsung's smartphones and tablets can group together different images of the same individual based on the person's unique facial geometry. Plaintiffs, who use these devices, brought this class action suit against the device manufacturer for violating the Illinois Biometric Privacy Information Act ("BIPA"). The

district court dismissed their second amended complaint for failure to state a claim. Because the complaint fails to plausibly allege that Samsung gained or exerted control over the data on their devices as required by BIPA, we affirm.

I. Background

A. BIPA

When enacting BIPA, the Illinois legislature sought to regulate data that are “biologically unique to the individual.” 740 Ill. Comp. Stat. 14/5(c). Such personalized data, commonly referred to as “biometric data” or simply “biometrics,” stand apart from other identifiers, such as social security numbers, because, as the legislature found, “once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” *Id.* Moreover, “[t]he full ramifications of biometric technology are not fully known.” 740 Ill. Comp. Stat. 14/5(f). As a result, the Illinois legislature determined that “[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” 740 Ill. Comp. Stat. 14/5(g).

To accomplish this goal, the legislature enacted § 15, which states, in relevant part:

- (a) A private entity *in possession of* biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or

No. 25-1120

3

within 3 years of the individual's last interaction with the private entity, whichever occurs first....

(b) No private entity may *collect, capture, purchase, receive through trade, or otherwise obtain* a person's or a customer's biometric identifier or biometric information, unless it first:

- (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
- (2) informs 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; and
- (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 Ill. Comp. Stat. 14/15(a) and (b) (emphases added).

When a company that possesses or obtains an individual's biometric identifiers or information fails to comply with BIPA's applicable mandates, the individual can sue the company for monetary damages, attorney's fees and costs, and other appropriate relief. *See* 740 Ill. Comp. Stat. 14/20.

B. The Claims

Plaintiffs bought and used smartphone and tablet devices manufactured by Samsung Electronics America, Inc. and

Samsung Electronics Co., Ltd. (“Samsung”).¹ Among other things, they used the devices to take pictures of themselves and other people. The devices then saved these pictures to the preinstalled Samsung Gallery application (“Gallery App” or “App”).

Once a picture is saved on the device, the Gallery App automatically scans it to determine whether the photograph has captured a face, and, if the App detects a face, the App makes a template of the person’s unique facial geometry to create a “face template.” The App then matches the face template to other photos on the device with the same face template and clusters the matching photos together in a stack.

According to Plaintiffs, to create the face template, the Gallery App uses a proprietary algorithm to scan the faces in a photograph and measures the unique geometric properties of each face, such as the length, width, depth, spacing, and location of various facial landmarks, including the mouth, chin, nose, ears, eyes, and eyebrows. In this way, each face template is “a distinct numerical representation of the unique shape and geometry of an individual’s face” that “can be used to identify them.”

“Each time a user takes or receives a photograph,” Plaintiffs allege, Samsung “capture[s]” the geometry of each face in the photograph, which the App uses to create a face template, which is then stored, accessed, and used when a new

¹ Although the named Plaintiffs all own or owned a Samsung device, they allege a broader class, one defined as “[a]ll individuals who, while residing in the State of Illinois, had their biometric identifiers or biometric information collected, captured, received or otherwise obtained and/or stored by Samsung.”

No. 25-1120

5

photo with a face is added to the device. According to Plaintiffs, the “stored scan[s] of face geometry” are stored “at least ephemerally,” and the face templates derived from the facial geometry scans are stored “in a database that Samsung keeps at least in the solid state memory of the user’s Samsung Device.”

Prior to September 2021, device users could backup their photos in the Gallery App by uploading them to the Samsung Cloud, a “cloud-server created, hosted, and controlled by Samsung.” While users own the phone or tablet, they merely license the operating software, including the Gallery App, from Samsung and cannot alter it. As a result, users have no way of disabling the facial recognition features of the App, so if they want to use the camera and Gallery App, they must agree to the creation and collection of face template data. Also, Plaintiffs point out, Samsung’s own privacy policy says that it “may collect” personal information such as biometrics.

Furthermore, Plaintiffs allege, “Samsung has complete and exclusive control over the Biometrics it captured, collected and stored on Samsung Devices.” For example, Samsung determines whether and what biometrics are collected and how the data are stored (*i.e.*, whether locally on devices, with encryption or other protection, and with what level of access).

Finally, according to Plaintiffs, Samsung does not have a written policy for the retention and destruction of biometric data, which violates BIPA § 15(a). Nor does it inform its device users in writing that such data is collected in violation of BIPA § 15(b)(1). Moreover, Plaintiffs assert, Samsung neither explains the collection and storage practices nor obtains a release from the users, thereby violating BIPA § 15(b)(2) and (3).

Plaintiffs commenced this putative class action in Illinois state court, and Samsung removed it to federal court under the Class Action Fairness Act, 28 U.S.C. §§ 1332(d)(2), 1453. After Plaintiffs amended the complaint as of right, Samsung filed the first motion to dismiss for failure to state a claim. Plaintiffs then amended the complaint a second time, and Samsung moved to dismiss yet again.

The district court granted the second motion but permitted Plaintiffs to file one last amended complaint, remarking, “While there is some doubt on these facts, it is not certain that any amendment would be futile.” *G.T. v. Samsung Elec. Am. Inc.*, 742 F. Supp. 3d 788, 801–02 (N.D. Ill. 2024) (citation omitted). After Plaintiffs filed their second amended complaint, Samsung filed a third motion to dismiss. This time, the district court granted the motion with prejudice and entered judgment for Samsung, which led to this appeal. *G.T. v. Samsung Elec. Am., Inc.*, 760 F. Supp. 3d 665 (N.D. Ill. 2024).

II. Discussion

We review the grant of a motion to dismiss for failure to state a claim *de novo*. *League of Women Voters v. City of Chicago*, 757 F.3d 722, 724 (7th Cir. 2014). To survive a Federal Rule of Civil Procedure Rule 12(b)(6) motion, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A facially plausible claim “allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.*

Plausibility is “a context-specific task that requires the reviewing court to draw on its judicial experience and common

No. 25-1120

7

sense.” *W. Bend Mut. Ins. Co. v. Schumacher*, 844 F.3d 670, 676 (7th Cir. 2016) (citation modified). It is only when “the well-pleaded allegations plausibly suggest—as opposed to possibly suggest—that the plaintiff[is] entitled to relief” that she proceeds with the case. *Alarm Detection Sys., Inc. v. Village of Schaumburg*, 930 F.3d 812, 821 (7th Cir. 2019).

Because the claims arise under state law, we apply Illinois law. See *Mississippi ex rel. Hood v. AU Optronics Corp.*, 571 U.S. 161, 165 (2014) (“CAFA expanded diversity jurisdiction[.]”); *Liberty Mut. Fire Ins. Co. v. Statewide Ins. Co.*, 352 F.3d 1098, 1100 (7th Cir. 2003) (“Because this is a diversity case, we apply the law of Illinois as we believe the Illinois Supreme Court would apply it.”). And “[w]hen no decision from the state supreme court squarely controls,” we try to “predict how the relevant state court would rule.” *Clay v. Union Pac. R.R. Co.*, 171 F.4th 975, 979 (7th Cir. 2026) (citation omitted).

The question before us is whether Plaintiffs have sufficiently alleged that, by preinstalling the Gallery App on its devices and allowing its use, Samsung (1) is “in possession of” Plaintiffs’ biometric data as that phrase appears in BIPA § 15(a) or (2) “collect[ed],” “capture[d],” “or otherwise obtain[ed]” Plaintiffs’ biometric data within the meaning of BIPA § 15(b). 740 Ill. Comp. Stat. 14/15(a), (b).²

Because this is a question of statutory construction that “involves the interpretation of an Illinois statute, we apply Illinois’s rules of statutory construction.” *Zahn v. N. Am. Power*

² For this appeal, we will assume without deciding that the facial geometry data and facial templates in question constitute “biometric identifiers” or “biometric information” regulated by BIPA. See 740 Ill. Comp. Stat. 14/10.

& Gas, LLC, 815 F.3d 1082, 1089 (7th Cir. 2016) (citing *Carter v. Tennant Co.*, 383 F.3d 673, 682 (7th Cir. 2004)).

Under Illinois law, the “primary rule of statutory construction is to ascertain and give effect to the intent of the legislature.” *Id.* (quoting *People v. Donoho*, 788 N.E.2d 707, 715 (Ill. 2003)). We start with the “clear language of the statute” and read the statute “as a whole.” *Id.* (quoting *People v. NL Indus.*, 604 N.E.2d 349, 355–56 (Ill. 1992)). “Where the language is clear and unambiguous, we must apply the statute without resort to further aids of statutory construction.” *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 923–24 (Ill. 2023), *as modified on denial of reh’g* (July 18, 2023) (citation omitted). “Only if the statutory language is ambiguous may we look to other sources to ascertain the legislature’s intent.” *Id.* (citation omitted).

Because BIPA does not expressly define “possession,” “collect,” “capture,” or “obtain,” we “assume the legislature intended for it to have its popularly understood meaning.” *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019). Turning first to “possession” as it appears in BIPA § 15(a), the Illinois Supreme Court, when examining a different statute, has held that “‘possession’ as ordinarily understood, occurs when a person *has or takes control* of the subject property or holds the property at his or her disposal.” *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (citing Webster’s Third New International Dictionary 1770 (1986) and Black’s Law Dictionary 1201 (8th ed. 2004)) (emphasis added). More recently, an Illinois appellate court has applied this definition to BIPA § 15(a). *Barnett v. Apple Inc.*, 225 N.E.3d 602, 609 (Ill. App. Ct. 2022) (citing *Ward*, 830 N.E.2d at 560) (applying the

No. 25-1120

9

“ordinary and popular meaning of “possession” in § 15(a) as “to have control”).

As for the words “collect,” “capture,” and “obtain” in BIPA § 15(b), the Illinois Supreme Court has defined “collect” to mean “to receive, gather, or exact from a number of persons or other sources,” *Cothron*, 216 N.E.3d at 924 (citing Webster’s Third New International Dictionary 444 (1993)); and “capture” to mean “to take, seize, or catch,” *id.* (citing Webster’s Third at 334 (1993)). While the *Cothron* court did not offer a definition for “obtain,” the same 1993 dictionary defines the word as “to gain or attain possession or disposal” or “hold, keep, possess, occupy.” Webster’s Third at 1559 (1993). And so, the Illinois Supreme Court determined that “[t]he active verbs used in section 15(b)—collect, capture, ... and obtain—all mean *to gain control*.” *Cothron*, 216 N.E.3d at 923 (emphasis added).

From these Illinois decisions, we too conclude that the words “possession,” “collect,” “capture,” and “obtain,” as they appear in BIPA § 15(a) and (b), all require the subject company to have or have obtained some degree of “control” over the biometric data in question.

Here, the district court found that Plaintiffs’ allegations fell short of plausibly alleging that Samsung in fact controlled the biometric data collected and generated by the Gallery App. We agree. Although Plaintiffs describe how Samsung provided users with the products (the phones and tablets) and software (the App) to record, create, and save facial biometric data on the individual devices, they allege nothing from which we can reasonably infer that Samsung itself controlled the data.

Plaintiffs resist this conclusion, pointing to several cases for the proposition that a manufacturer, like Samsung, “controls” biometric data on user devices (thereby, triggering BIPA) when it prohibits users from accessing, deleting, or modifying the data on their devices. Take, for example, *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643 (S.D. Ill. 2021). There, Apple device users sued the company over the alleged use of biometric information in its Photos app, which employed facial recognition technology to scan a user’s photographs and added frequently detected faces to a user’s “People” album. The plaintiffs alleged that (1) Apple stored the “faceprints” in on-device databases that users could not access; (2) users could not delete the collected information or disable the feature on their devices; (3) users had to accede to the collection of such data in order to use the devices; and (4) only Apple could access the biometric data or disable its collection. *Id.* at 653. The district court found this was sufficient to allege “complete and exclusive control over the data on Apple Devices” to state a claim under § 15(a). *Id.*

By contrast, consider *Bhavilai v. Microsoft Corp.*, 716 F. Supp. 3d 640 (N.D. Ill. 2024). There, the class action plaintiff alleged that Microsoft designed, licensed, sold, and/or updated the facial scanning software in the Windows 10 or 11 operating system, which captured users’ facial biometric data when installed on a compatible device. This, the plaintiff asserted, was enough to satisfy the prerequisites of “dominion and control” under BIPA because Microsoft “exercised control over the device users’ ability to access and use the facial scan software.” *Id.* at 641. “But control of the facial scan software,” the district court held, “is not the same as control of the facial scan data that is collected using the software.” *Id.* Furthermore, the court continued, “selling or licensing a tool

No. 25-1120

11

that can be used to collect a facial scan is not the same as actually doing the collecting.” *Id.* The district court wrapped up, concluding, “[Plaintiff’s] argument conflates two different activities—providing the tool versus using the tool.” *Id.*

An Illinois appellate court has relied on similar reasoning to dismiss BIPA § 15(a) and (b) claims. *See Barnett*, 225 N.E.2d at 610–12. In *Barnett*, the plaintiffs claimed that Apple’s installation of Touch ID and Face ID features and related software on their Apple devices violated BIPA because they collected the users’ fingerprints and facial images and saved the mathematical representations derived from them on the devices for future use. 225 N.E.3d at 604. Like Plaintiffs, they also alleged that Apple exclusively owned the software and prohibited users from accessing the biometric data saved on the devices. *Id.*

Affirming the trial court’s dismissal of the BIPA claims, the state appellate court concluded that the plaintiffs had not adequately alleged that Apple possessed or collected their biometric data in a manner that triggered BIPA § 15(a) and (b). The plaintiffs’ contention that Apple possessed and collected the data because the software collected and analyzed the information, the court held, incorrectly “equates the product with the company.” *Id.* at 609. “The device and software are the tools,” the court continued, “but it is the user herself who utilizes these tools to capture her own biometric information.” *Id.* at 610. Moreover, the user could disable the features and delete the data, and there were no allegations that Apple saved the information on its servers. *Id.* at 609–10.

We believe the latter line of cases more faithfully comports with the plain language of BIPA § 15(a) and (b). To highlight the type of control BIPA requires, consider the following scenario. A company makes and sells an optical drawing tool

that uses a prism to superimpose an image of a person or object onto a sheet of paper so that the user can accurately sketch or paint the subject (commonly referred to as a “camera lucida”). Assume too that the user employs the device to sketch realistic portraits of various individuals and then preserves the hand-drawn depictions in a portfolio. The camera lucida device when employed by the user in this way can be said to “collect,” “capture,” or “otherwise obtain” the unique facial information of the subject. But it is difficult to see how, in this scenario, one could plausibly allege that the *company* possesses or controls the use of the device or the facial geometry information the user collects in the portfolio. Indeed, the user might not aspire to be a portrait artist at all and elect to employ the device exclusively to sketch or paint still lifes of fruit or flowers.

Admittedly, this example may stretch BIPA beyond its limits, and perhaps such hand-drawn portraits might fall within the “photographs” exception of BIPA anyway. 740 Ill. Comp. Stat. 14/10. Moreover, today’s smartphone and tablet cameras are undeniably more technologically advanced than camera lucida devices of old. But nowhere in the complaint do Plaintiffs allege that the facial geometry data that they captured using their devices were saved on anything but the devices themselves. Nor do Plaintiffs allege that Samsung somehow forced them to take pictures with faces or that Samsung has the ability to access, modify, or use facial geometry data in any way. In this way, the camera lucida example aptly illustrates the primary deficiencies in the complaint.

For their part, Plaintiffs point out that the Gallery App gives users the ability to back up their photos to Samsung’s cloud servers. From this, they argue, one could reasonably

No. 25-1120

13

infer that the associated facial geometry data (like the photographs themselves) are also backed up to Samsung's cloud servers. But this is not necessarily so, and Plaintiffs do not provide any plausible support for this theory.

Plaintiffs also note that Samsung's own privacy policy mentions that the company "may collect" personal information such as biometrics. But the fact that the company may collect biometric data does not mean that the facial geometry data in question are actually gathered and saved by Samsung.

We recognize that technology companies such as Samsung have significantly more information about their proprietary systems and software than everyday consumers, who may not be able to ascertain their inner workings without the aid of discovery. But, as Plaintiffs here demonstrate, much information can be gleaned from publicly available patents and other public disclosures, and the burden rests on Plaintiffs to plausibly state a cause of action that can withstand judicial scrutiny. *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 570).

At bottom, BIPA's stated purpose is to regulate information that is immutable and "biologically unique to the individual" to reassure the public of the safety and security of biometric identification systems and ensure that companies will collect, use, safeguard, handle, and store their biometric data in a transparent manner. *See* 740 Ill. Comp. Stat. 14/5(c)–(g). Manufacturing a device (and installing related software) that allows a user to voluntarily take pictures of oneself, friends, family, and other passersby and, in the process, create face templates that remain parked within the confines of the user's own personal device not only falls short of triggering BIPA's statutory requirements but strays too far afield from the statute's heartland. *See, e.g., Cothron*, 216 N.E.3d at 920,

923–24 (fast-food restaurant required employee to scan fingerprints to access pay stubs and computer systems); *Rosenbach*, 129 N.E.3d at 1200, 1204–05 (amusement park collected season passholder’s fingerprint for entry); *Fox v. Dakota Integrated Sys., LLC*, 980 F.3d 1146, 1149 (7th Cir. 2020) (company collected hand scans from employee when she clocked in and out of work for timekeeping); *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 619 (7th Cir. 2020) (work cafeteria vending machine payment system collected fingerprint from employee when she made a user account and to pay).

* * *

For the foregoing reasons, the judgment is AFFIRMED.