**UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISION**

G.T., et al.

*Plaintiffs*,

v.

Samsung Electronics America Inc., et al.

*Defendants*.

No. 21 CV 4976

Judge Lindsay C. Jenkins

**MEMORANDUM OPINION AND ORDER**

Defendants Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. (collectively, "Samsung") have moved to dismiss the consolidated amended class complaint filed by several Plaintiffs[1] who allege facial recognition technology in Samsung's Gallery photo application violates Illinois's Biometric Information Privacy Act ("BIPA"). For the reasons stated herein, the motion is granted.

## I. Background

The Court takes Plaintiffs' well-pleaded factual allegations as true for purposes of ruling on the motion to dismiss. *See Smith v. First Hosp. Lab'ys, Inc.*, 77 F.4th 603, 607 (7th Cir. 2023). Samsung manufactures various smartphones and tablets ("Devices"), and Plaintiffs are all Illinois residents who used Samsung Devices. All Devices come pre-installed with the Gallery application (the "App"), which Samsung designs and owns. [Dkt. 50 ¶¶ 2-3, 12; *see also id.* at 17-35.][2]

[1] Plaintiffs are G.T., by and through next friend Liliana T. Hanlon, Shimera Jones, Leroy Jacobs, Richard Maday, Mark Heil, Balarie Cosby-Steele, Sherie Harris, John DeMatteo, and Allison Thurman. The Court will refer to them collectively as "Plaintiffs."

[2] Citations to docket filings generally refer to the electronic pagination provided by CM/ECF, which may not be consistent with page numbers in the underlying documents.

The App allows users to "save, organize, edit, share and store" their videos and photographs, and everything captured by the Device's camera is saved on the App. [*Id.* ¶ 3.] But that is not all. Plaintiffs allege that the App automatically takes a series of actions when an image is created. First, Samsung's "proprietary facial recognition technology" scans images to search for faces. If the App detects a face, it analyzes the face's "unique facial geometry."[3] Based on this analysis, the App creates a unique digital representation of the face, called a "face template." [*Id.* ¶¶ 4-6; 52-54.]

Once a face template is created, the App organizes photographs based on images with similar face templates. The App does this through "face clustering", a process by which the App extracts key facial features from the face template and converts that information into numerical "vectors" based on the facial feature. The App compares the vectors in a new image to the previous images on the Device and will group together images that are sufficiently analogous. The result is pictures with a certain individual's face are "stacked" together on the App. [*Id.* ¶¶ 55-56.]

Plaintiffs allege this repository of digital face templates and corresponding vectors (collectively, the "Data") exists "at least" on the Samsung device itself. [*Id.* ¶ 54.] Plaintiffs do not affirmatively allege the Data is sent to any centralized Samsung repository or database, or that Samsung can access the Data on individual Devices.

Plaintiffs contend that through the process of generating the Data, Samsung is collecting the biometrics of all individuals whose faces appear in pictures on its Devices in violation of BIPA. Plaintiffs also allege that they are powerless to protect

[3] Facial geometry includes various measurements such as the length between the eyes, as well as the shape, width and depth of the mouth, chin, nose, ears, eyebrows, etc.

their biometric information because Samsung does not inform its users of these functions, nor does Samsung permit its users to disable them. According to Plaintiffs, it is an intractable part of the App. And because Samsung designs and installs the App, it has full control over what data is collected, as well as all components of the Data itself, including where and how it is stored. [*Id.* ¶¶ 57-63.] Accordingly, Plaintiffs sued Samsung alleging it has failed to abide by two BIPA provisions related to steps private entities must follow when they possess biometric data. [Dkt. 50]; 740 ILCS 14/15(a)(b). Samsung now moves to dismiss.

## II. Legal Standard

At the motion to dismiss stage, the Court takes well-pleaded factual allegations as true and draws reasonable inferences in favor of the plaintiff. *Choice v. Kohn L. Firm, S.C.*, 77 F.4th 636, 638 (7th Cir. 2023); *Reardon v. Danley*, 74 F.4th 825, 826-27 (7th Cir. 2023). "To survive a motion to dismiss under Rule 12(b)(6), plaintiff's complaint must allege facts which, when taken as true, plausibly suggest that the plaintiff has a right to relief, raising that possibility above a speculative level." *Cochran v. Ill. State Toll Highway Auth.*, 828 F.3d 597, 599 (7th Cir. 2016) (cleaned up). This occurs when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Garrard v. Rust-Oleum Corp.*, 575 F. Supp. 3d 995, 999 (N.D. Ill. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citations omitted)).

## III. Analysis

BIPA governs the collection, use, safeguarding, retention, disclosure, and disclosure of biometric data by private entities. The Illinois legislature enacted BIPA

to ease public concern regarding "the use of biometrics when such information is tied to finances and other personal information" because biometrics "are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c)-(d).

BIPA defines biometrics in two ways: "biometric identifier" and "biometric information."[4] Biometric identifier "means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry", but excludes items like writing samples and photographs. Biometric information "means 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.

Under BIPA, private entities that are "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." 740 ILCS 14/15(a). In addition, before a private entity "collect[s], capture[s], purchase[s] … or otherwise obtain[s] a person's" Biometrics, they must inform the person in writing (i) that they are collecting or storing the Biometrics; (ii) why and for how long they are storing the Biometrics; and (iii) receive a written release from the person authorizing the collection. 740 ILCS 14/15(b).

[4] The Court will refer to these terms collectively as "Biometrics."

Plaintiffs contend Samsung is in violation of these provisions through the App's use of face geometry scanning, and its creation and storage of Data. Samsung points to two main reasons why Plaintiffs' allegations are insufficient. First, Plaintiffs do not adequately allege that Samsung "possesses", "collects", or "otherwise obtains" Biometrics because Plaintiffs do not allege the Data ever leaves users' Devices. Consequently, Samsung does not and cannot access the Data, so Samsung does not possess or control it as those terms are understood in BIPA. Second, Samsung contends its facial scanning and resulting Data are not Biometrics because it cannot identify an individual. The Court reviews each argument in turn.

### A. Whether Samsung Possessed Biometric Information under Section 15(a)

Section 15(a) only applies to private entities that are "in possession of" Biometrics. BIPA does not define "possession", so courts use its "popularly understood meaning." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186 ¶ 29. "[P]ossession, as originally understood, occurs when a person has or takes control of the subject property or holds the property at his or her disposal." *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (quoting *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005)). In the context of BIPA, "possession occurs when someone exercises any form of control over the [biometric] data or held the data at his disposal." *Jacobs v. Hanwha Techwin America, Inc.*, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021) (quoting *Heard*, 440 F. Supp. 3d 960, at 968) (cleaned up).

The parties' central disagreement is whether a private entity is in possession of Biometrics when it creates and controls technology that purportedly generates

Biometrics, even if the entity does not receive or access the data.[5] [*Compare* Dkt. 55 at 11-12 ("Plaintiffs' conclusory allegations of Samsung's control over design decisions about [the App] do not mean that Samsung 'possessed' data that is later generated and stored locally on Plaintiffs' devices while the devices are in Plaintiffs' possession"); *with* Dkt. 62 at 13 (Samsung is in possession of Plaintiffs' Biometrics because "Samsung has complete and total control over the biometric data surreptitiously captured using proprietary software that Samsung owned and alone controlled, preventing users from turning it off or disabling it").] There is caselaw that supports both parties' positions.

Plaintiffs liken their allegations to those in *Hazlitt*. *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643 (S.D. Ill. 2021); [Dkt. 62 at 7.] Like here, *Hazlitt* involved a pre-installed, unmodifiable picture app that scanned and collected data from face geometries with the resulting data kept "locally in a facial recognition database in the solid-state memory on the device."[6] *Id.* at 646-47. Apple argued it did not possess Biometrics because "Plaintiffs have the choice to erase any or all data stored on their devices, only the plaintiffs know the identities of anyone in their photos, and there is

---

[5] Plaintiffs make two arguments that Samsung received the Data. Both are unavailing. Plaintiffs allege the App had "a feature that allow[ed] users to backup their photographs to a [centralized] cloud server" until September 2021, but photographs are explicitly excluded from the definition of biometric identifiers, and Plaintiffs do not allege the underlying Data was uploaded to the cloud. [*See* Dkt. 62 at 10-11; Dkt. 50 ¶ 66.] Second, Plaintiffs allege in several places that the Data is "at least" stored on the local Device (keeping open the possibility that Samsung received the Data elsewhere) but that is impermissibly speculative; Plaintiffs must allege facts. *Cochran*, 828 F.3d 597, at 599.

[6] The *Hazlitt* court noted Apple "does not store or transfer all user biometric identifiers or biometric information on its servers", which suggests at least some Biometrics were sent to Apple. *Id.* at 647.

no suggestion in the Complaint that Apple reserves the right to access a user's photos after selling the device." *Id.* at 652. The court sided with plaintiffs, holding they adequately alleged Apple possesses the data "because it has complete and exclusive control over the data on Apple Devices, including what biometric identifiers are collected, what biometric data is saved, whether biometric identifiers are used to identify users (creating biometric information), and how long biometric data is stored." *Id.* at 653.

Samsung's chief authority is *Barnett v. Apple Inc.*, 2022 IL App (1st) 220187, a case involving Apple's "Touch ID" and "Face ID" features. Also like this case, Apple developed and owned these technologies, and the resulting data was stored on the local user's device through mathematical representations. *Id.* ¶¶ 12, 14-15. Unlike this case, however, use of these features was voluntary, and users had the ability to delete the biometric information from their device. *Id.* ¶ 44. The *Barnett* court rejected plaintiff's argument that "Apple 'possess' their [biometric] information because Apple software collects and analyzes their information." *Id.* ¶ 43. The court reasoned this wrongfully "equates the product with the company" and that there is a salient difference between the data collected from a product created by the company, and the data the company itself possesses. *Id.; see also id.* ¶ 44 ("the device and the software are the tools, but it is the user herself who utilizes those tools to capture her own biometric information.")

In so ruling, *Barnett* distinguished *Hazlitt* thus: "the plaintiffs in *Hazlitt* alleged that Apple stored the facial information in Apple's own databases and that

users had no power to delete the collected information or disable the feature on their devices." *Id.* ¶ 45. Plaintiffs argue *Barnett*'s reference to "Apple's own databases" is the same database referred to in *Hazlitt*—the local database on the user's Device—so the sole difference between *Barnett* and *Hazlett* is that the consumer in *Barnett* had the option to use and/or remove her biometrics. [Dkt. 62 at 15-16.] Samsung posits *Barnett*'s holding is not about the amount of control a defendant (or plaintiff) has over the technology, but the defendant's level of access to the biometric data, which Apple had (at least to some degree) in *Hazlitt*.[7] [Dkt. 64 at 9.] And because Plaintiffs here have not alleged that Samsung has accessed or can access the Data (as opposed to the technology the App employs), Samsung is not in possession. [*Id.*]

The court in *Bhavilai* agreed with Samsung's logic. *Bhavilai v. Microsoft Corp.*, —F. Supp. 3d.—, 2024 WL 992928, at *1 (N.D. Ill. Feb. 8, 2024). In that case, the plaintiff alleged Microsoft was in possession of her biometric data, even though she admitted the data was not "physically stored on Microsoft's hardware", because a photo application Microsoft "owned and controlled" possessed her facial scan. *Id.* Plaintiff argued Microsoft was in possession of her biometric data "because it designed, licensed, and updated the facial scan software on users' devices" so Microsoft "exercised control over the device users' ability to access and use the facial scan software." *Id.* The Court rejected this argument and dismissed the plaintiff's Section 15(a) claim because the plaintiff failed to allege "Microsoft used or exercised

[7] After discovery was taken in *Hazlitt*, plaintiffs filed an amended complaint alleging the biometric information was sent to Apple's centralized servers. *Doe v. Apple Inc.*, 2022 WL 17538446, at *1 (N.D. Ill. Aug. 1, 2022).

any control over her facial scan data in any way." The Court added "the fact that Microsoft has the ability to give users the ability to collect facial scan data does not mean that Microsoft possesses the facial scan data." *Id.*

Other courts in this district have likewise found that control over the offending technology is insufficient; the defendant must have accessed or have access to the Biometrics. *Jacobs*, 2021 WL 3172967 (dismissing BIPA action against camera manufacturer with facial-recognition technology where manufacturer did not have access to camera footage or data used by third-party employer); *Heard*, 440 F. Supp. 3d 960, at 968 (plaintiff's allegations regarding possession inadequate where complaint "does not say whether BD could freely access the [biometric] data or even how BD allegedly received it.") Conversely, when the plaintiff alleges defendants possess the Biometrics, the Section 15(a) claim proceeds. *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 284 (N.D. Ill. 2019) ("Namuwonge's allegation that Brookdale disclosed their employees' fingerprint data to Kronos sufficiently alleges that Kronos possessed the fingerprint data collected by Brookdale.")

The Court concludes Plaintiffs have not adequately alleged Samsung was "in possession" of their Biometrics. Samsung controls the App and its technology, but it does not follow that this control gives Samsung dominion over the Biometrics generated from the App, and plaintiffs have not alleged Samsung receives (or can receive) such data. Multiple courts have held these allegations are insufficient where the defendant does not also receive the underlying data:

> Bhavilai alleges that Microsoft exercised control over the device users' ability to access and use the facial scan software. But control of the facial

> scan software is not the same as control of the facial scan data that is collected using the software. Bhavilai has not alleged that Microsoft used or exercised any control over her facial scan data in any way. The fact that Microsoft has the ability to give users the ability to collect facial scan data does not mean that Microsoft possesses the facial scan data.

*Bhavilai*, 2024 WL 992928, at *1; *Barnett*, 2022 IL App (1st) 220187 ¶ 43 (the argument that a defendant possesses information because the software it owns "collects and analyzes their information … equates the product with the company"); *see also Heard*, 440 F.Supp.3d 960, at 968 (no possession where plaintiff failed to allege defendant could access or receive the data).

The Court also disagrees that "possession" should turn on whether the technology is optional. Under BIPA, "possession does not contemplate [i.e., require] exclusive control", *Heard*, 440 F.Supp.3d 960, at 968, so Samsung would not lose possession because Plaintiffs also have it. Put differently, possession must be viewed from the eyes of the possessor, Samsung, which does not change if Plaintiffs have the option to alter settings in the App. Ultimately, the Court concludes the salient inquiry for determining possession under Section 15(a) is whether the entity exercised control over the Biometrics, not whether it exercised control over the technology generating the Biometrics. Plaintiffs have no allegations to that effect, so Samsung's motion to dismiss on this basis is granted.

### B. Whether Samsung Collects, Captures, or Otherwise Obtains Biometrics under Section 15(b)

To state a Section 15(b) claim, a plaintiff must allege the defendant entity "collects", "captures", "or otherwise obtains" a person's Biometrics. 740 ILCS 14/15(b). As with "possession", BIPA does not provide definitions for these terms, so courts

supply their "popularly understood meaning." *Rosenbach*, 2019 IL 123186 ¶ 29. "Collect" means "to receive, gather, or exact from a number of persons or other sources", whereas "capture" means "to take, seize, or catch." *Cothron v. White Castle System, Inc.*, 2023 IL 128004 ¶ 23. Courts have understood "otherwise obtain" to mean procure through effort. *Heard*, 440 F. Supp. 3d 960, at 966; *Jones v. Microsoft Corp.*, 649 F. Supp. 3d 679, 683-84 (N.D. Ill. 2023). Collectively, all these verbs "mean to gain control" of Biometrics. *Cothron*, 2023 IL 128004 ¶ 16. This requires the defendant to make an affirmative effort—to take an "active step"—towards receiving the Biometrics. *Jones*, 649 F. Supp. 3d 679, at 683-84; *Heard*, 440 F. Supp. 3d 960, at 966; *Jacobs*, 2021 WL 3172967, at *2.

Plaintiffs contend Samsung has obtained their Biometrics through the App's collection of the Data. [Dkt. 62 at 19.] According to Plaintiffs, Samsung necessarily "obtained" the Data because otherwise the technology could not function—the App would have no ability to compare facial images. [*Id.* at 19-20.] Plaintiffs further argue Samsung took an "active step" by developing the App in a way that "automatically harvests biometric data from every photo stored on the Device and not only conceals this from users, but prevents them from disabling the process or destroying that information." [*Id.* at 20.] In essence, Plaintiffs' position is that the same conduct that caused Samsung to violate Section 15(a) makes it in violation of Section 15(b).

The Court disagrees. Plaintiffs' argument again conflates technology with Biometrics. But Section 15(b) is concerned with private entities collecting, capturing, or obtaining Biometrics, not creating technology. Plaintiffs do not allege Samsung

receives the Data the App accumulates, or that Samsung even has access to it. Indeed, Plaintiffs do not allege that Samsung takes any action towards the Data whatsoever after it is generated.

This allegation is crucial to stating a Section 15(b) claim. In *Cothron*, for example, plaintiffs alleged White Castle affirmatively stored fingerprints on its own databases and used those fingerprints to give plaintiffs access to White Castle computers. These allegations satisfied Section 15(b) because this system could not function unless White Castle collected or captured the fingerprints. *Cothron*, 2023 IL 128004 at ¶ 23. Consistently, in *Heard*, the Court dismissed a Section 15(b) claim where the plaintiff failed to "allege how the data made its way to BD's systems." 440 F.Supp.3d 960, at 967. After an opportunity to amend, however, the Court permitted the Section 15(b) claim to proceed because plaintiffs now alleged BD "stores users' biometric information both on the device *and* in BD's servers." *Heard*, 524 F. Supp. 3d at 841 (emphasis in original). The Court further explained it was not BD's mere possession of Biometrics that satisfied 15(b)'s requirements, but that the allegations "suggest that BD itself plays an active role in collecting or otherwise obtaining users' biometric information." *Id.*

Here, Plaintiffs do not argue that Samsung possesses the Data or took any active steps to collect it. Rather, the active step according to Plaintiffs is the creation of the technology. This argument was flatly rejected in *Bhavilai*:

> Bhavilai argues that Microsoft 'collected' her facial scan data when it 'enabled the facial biometric scanning within its Photos application.' Bhavilai argues that because Microsoft retained the ability to control whether and how a user could use the facial scan software demonstrates

> that Microsoft was in fact the collector. But selling or licensing a tool that can be used to collect a facial scan is not the same as actually doing the collecting. This argument conflates two different activities—providing the tool versus using the tool. Bhavilai has simply failed to allege that Microsoft did anything beyond providing a tool.

*Bhavilai*, 2024 WL 992928, at *1. As with Section 15(a), there is a salient difference between providing a technology and then using that technology to collect, capture, or obtain Biometrics. Here, Plaintiffs have failed to allege Samsung took an "active step" in gaining control over their Biometrics, which dooms their Section 15(b) claim.

### C. Whether BIPA Regulates the App and its Data

Samsung raises an additional argument as to why Plaintiffs' claims fail: the App does not generate "biometric identifiers" or "biometric information" subject to BIPA's regulation. [Dkt. 55 at 16.] The Court agrees, which provides another basis for the dismissal of Plaintiffs' claims.

Plaintiffs argue the App's functions implicate BIPA in two ways. First, the App scans facial geometry, which is an explicitly enumerated biometric identifier. Second, the App's storage of Data (mathematical representations of face templates) constitutes biometric information. [Dkt. 62 at 25.] Samsung's posits that neither process can identify individuals; rather, they are only capable of recognizing faces, so BIPA does not apply. [Dkt. 55 at 17-18.]

As stated above, a "biometric identifier" "means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. Courts are divided on whether a plaintiff must allege a biometric identifier can identify a particular individual, or if it is sufficient to allege the defendant merely scanned, for example, the plaintiff's face or retina. *Compare e.g., Brown v. AS Beauty Group LLC*,

2024 WL 2319715 (N.D. Ill. May 22, 2024) (rejecting argument that biometric identifiers must be capable of identifying particular individuals); *Konow v. Brink's Inc.*, 2024 WL 942553, at *4 (N.D. Ill. Mar. 5, 2024) (requirement that biometric identifiers identify a unique person is not "supported by BIPA's plain language"); *Colombo v. Youtube, LLC*, 679 F. Supp. 3d 940 (N.D. Cal. 2023) (same); *with Martell v. X Corp.*, 2024 WL 3011353, at *3 (N.D. Ill. June 13, 2024) ("if the Court were to read BIPA as applying to any retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry without those items actually identifying an individual, it would contravene the very purpose of BIPA"); *Clarke v. Aveda Corp.*, 2023 WL 9119927, at *2 (N.D. Ill. Dec. 1, 2023) (dismissing BIPA complaint that "contains no plausible allegations that Aveda's collection of their biometric data made Aveda capable of determining their identities") (cleaned up); *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117, 1123 (9th Cir. 2024) ("scans of face geometry … are not covered by BIPA if they cannot identify a person.")

Central to this disagreement is what meaning, if any, should be given to the word "identifier" in "biometric identifier." *Compare Hazlitt v. Apple Inc.*, 500 F. Supp. 3d 738, 749 (S.D. Ill. 2020) ("Apple reads the word 'identifier' to exclude data that does not identify an actual person. This Court finds that interpretation too narrow"); *with Zellmer*, 104 F. 4th 1117, at 1123 ("Zellmer would write the term 'identifier' out of BIPA. Under his reading, every 'retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry' is a biometric identifier and therefore within BIPA's reach. But this reading conflates necessary and sufficient conditions.") The parties'

arguments fall along these exact lines; Plaintiffs urge the Court to conclude every scan is necessarily a biometric identifier, whereas Samsung argues the plain meaning of "identifier", combined with BIPA's purpose, demonstrates that only those scans that can identify an individual qualify. [Dkt. 55 at 17-18; Dkt. 62 at 25.] Samsung has the better argument.

Plaintiffs' position is grounded in a comparison of statutory definitions. Unlike the definitions of "biometric information" and "confidential and sensitive information", 740 ILCS 14/10, the term "biometric identifier" does not include language stating it must be capable of "identifying an individual." [Dkt. 62 at 24 ("[n]othing in the definition of "biometric identifier" requires any of those items to be used (or be capable of being used) to identify a person").]

While this distinction is accurate, that does not mean the word "identifier" should be ignored. *Mosby v. Ingalls Memorial Hospital*, 2023 IL 129081 ¶ 36 (when interpreting statutes in Illinois, "[e]ach word in a statute is to be 'given a reasonable meaning and not rendered superfluous'") (quoting *Sylvester v. Industrial Comm'n*, 756 N.E. 2d 822, 827 (Ill. 2001)). "An 'identifier' is 'one that identifies,' and 'identify' means 'to ascertain the identity of [something or someone].'" *Zellmer*, 104 F. 4th 1117, at 1123 n.1; *see also Martell*, 2024 WL 3011353, at *3 ("Merriam-Webster defines 'identifier' as 'one that identifies' and Black's Law Dictionary defines 'identify' as 'to prove the identity of (a person or thing).'"")

Based on these principles of statutory interpretation and the plain meaning of identifier, the Court concludes BIPA only covers those "retina or iris scan[s],

fingerprint[s], voiceprint[s], or scan[s] of hand or face geometry" that are capable of identifying an individual. Therefore, the fact that the App performs face scans is not dispositive.

This holding comports with the legislation's intent in enacting BIPA. *Sylvester*, 756 N.E. 2d 822, at 827 (in matters of statutory construction, the "primary goal, to which all other rules are subordinate, is to ascertain and give effect to the intention of the legislature.") BIPA recognizes that biometrics "are biologically unique to the individual [and] once compromised, the individual has no recourse." 740 ILCS 14/5(c). For biometrics to be compromised, however, there must be some ability to connect the biometrics to an individual; a facial scan is meaningless if there is no way to determine who it belongs to. That is why the terms "biometric information" and "confidential and sensitive information" make clear the information must be capable of identifying the individual. But as the Ninth Circuit reasoned, it was unnecessary to add this language to biometric identifier because it is baked into the term. *Zellmer*, 104 F.4th 1117, at 1124 ("the ability to identify did not need to be spelled out in that term—it was readily apparent from the use of 'identifier.'")

The Court now turns to whether any function within the App is capable of identifying an individual. Again, the parties disagree on what level of identification is required. Plaintiffs contend the App's creation of unique mathematical representations of a person's face is sufficient because the technology identifies and groups unique faces. [Dkt. 62 at 25-26 ("Samsung uses the Face Templates to

recognize the person among the sea of faces appearing on the hundreds (if not thousands) of photographs stored in the Gallery App").]

According to Plaintiffs, it does not matter that the App cannot—either through the creation of the face template or in combination with other information on the Device—ascertain an individual's identity, [*id.* at 26], which is Samsung's argument. [Dkt. 55 at 18 (the Data cannot "identify who the individuals in the photos are. To the contrary: users' own knowledge, not the technology, is what may identify people in their photographs").]

Although this is another issue with law on both sides, the Court follows the line of cases that require biometric information to be capable of recognizing an individual's identity, not simply an individual's feature. *Zellmer*, 104 F. 4th 1117, at 1125 (holding that technology that cannot identify individuals does not fall within BIPA); *Castelaz v. Estee Lauder Companies, Inc.*, 2024 WL 136872, at *6-7 (N.D. Ill. Jan. 10, 2024) (dismissing BIPA claim where plaintiffs failed to provide "any specific factual allegations that [defendant] is capable of determining Plaintiffs and members of the Illinois class members' identities by using the collected facial scans, whether alone or in conjunction with other methods or sources of information available to" defendant); *Clarke*, 2023 WL 9119927 (same).

The *Daichendt* cases provide a helpful example. In ruling on a motion to dismiss the initial complaint, the district court held that for a BIPA claim to survive, "plaintiffs must allege that defendant's collection of their biometric data made defendant *capable of* determining their identities." *Daichendt v. CVS Pharmacy, Inc.*,

2022 WL 17404488, at *5 (N.D. Ill. Dec. 2, 2022) (emphasis in original). The court held plaintiffs failed to meet this burden because they did not allege CVS had any way, "such as their names or physical or email addresses, that could connect the voluntary scans of face geometry with their identities." *Id.* Accordingly, plaintiffs "failed to plead the most foundational aspect of a BIPA claim"—the ability to identify an individual—and their claim was dismissed. *Id.* In the amended complaint, however, plaintiffs alleged they included "their names, email addresses, and phone numbers into a computer terminal inside defendant's stores prior to scanning their biometric identifiers", which was sufficient to survive the motion to dismiss. *Daichendt v. CVS Pharmacy, Inc.*, 2023 WL 3559669, at *1 (N.D. Ill. May 4, 2023).

In arguing that individual identification is not a statutory requirement, Plaintiffs cite to several cases. But all these cases included allegations regarding a combination of factors that allowed individual identification. *Rosenbach*, 2019 IL 123186 (thumbprint scan in combination with personal identifying information); *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 517 (N.D. Ill. 2022) (AI technology that could "actually identify unique individuals"); *Hazlitt*, 500 F. Supp. 3d 738, at 749 (photography app that "applies an algorithm to identify the device user"); *Rivera v. Google*, 238 F.Supp.3d 1088, 1095 (N.D. Ill. 2017) (photography app that is capable of identifying a specific person).

Here, Plaintiffs do not allege the App's technology is capable of identifying a person's identity. Rather, Plaintiffs allege only that the App groups unidentified faces together, and it is the Device user who (has the option to) add names to the faces. The

Court concludes these allegations are insufficient to show that the Data constitutes either a biometric identifier or biometric information.

## IV. Conclusion

For these reasons, Samsung's motion to dismiss is granted. The dismissal will be without prejudice. Although Plaintiff G.T. has already had an opportunity to amend the complaint once, [Dkts. 1, 14], the operative pleading came before the motion to dismiss was filed. The Court's normal practice, in accordance with Seventh Circuit guidance, is to give one chance to amend after a motion to dismiss is briefed, even if a plaintiff has amended previously. *Zimmerman v. Bornick*, 25 F.4th 491, 494 (7th Cir. 2022). And Seventh Circuit precedent is clear that the Court should err on the side of allowing an amendment; "a court should deny leave to amend only if it is certain that amendment would be futile or otherwise unwarranted." *Runnion ex rel. Runnion v. Girl Scouts of Greater Chi. & Nw. Ind.*, 786 F.3d 510, 520 (7th Cir. 2015). While there is some doubt on these facts, it is not certain that "any amendment would be futile." *Id.*

Enter: 21 CV 4976
Date: July 24, 2024

Lindsay C. Jenkins
United States District Judge