IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

JANE DOE, *et al.*,	
Plaintiffs,	
v.	**Case No. 3:20-CV-421-NJR**
APPLE INC.,	
Defendant.	

MEMORANDUM AND ORDER

ROSENSTENGEL, District Judge:

Humans have used biometrics for identification for hundreds, if not thousands, of years.[1] Some of the earliest examples include fingerprints recorded in clay to memorialize business transactions and measurements of body dimensions to track criminal offenders.[2] Modern fingerprint classification systems were developed in the late 19th century, and by the 1960s, facial and speech recognition models were advancing.[3] By 2008, biometrics were commonly used for security screenings and financial transactions.

That same year, Illinois had the foresight to protect its citizens against the unknown and unwanted collection of their biometric identifiers and information by enacting the Biometric Information Privacy Act ("BIPA"). 740 ILL. COMP. STAT. 14/1 *et seq.* In passing BIPA, the Illinois General Assembly recognized that biometrics are different

[1] Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE (Feb. 1, 2018), https://www.biometricupdate.com/201802/history-of-biometrics-2.
[2] *Id.*
[3] *Id.*

from identifiers like social security numbers because they are "biologically unique to the individual" and cannot be changed, and that "once compromised, the individual has no recourse." *Id.* § 5(a), (c). Importantly, the legislature observed that "the full ramifications of biometric technology are not fully known." *Id.* § 5(f).

Time has borne out that insight. In 2008, when BIPA was enacted, facial recognition technologies had relied for decades on the measured distances and angles between facial landmarks like the eyes, nose, and mouth, and the spatial relationships between those landmarks. (Doc. 280-19, pp. 13-14). Now, facial recognition technology no longer requires measurements of the face. (Doc. 280-20, p. 7). Advances in machine learning and artificial neural networks in the 2010s "enabled a breakthrough in face recognition." (Doc. 280-19, p. 15). These deep neural networks, modeled off the human brain, derive information directly from the pixels in an image, allowing them to "capture complex, non-linear relationships between images of faces." (*Id.*). This new age of facial recognition, which does not solely rely on the spatial relationship between facial landmarks, offers "superior accuracy." (*Id.*).

This certified class action examines whether Apple violated BIPA when its facial recognition software created digital faceprints from photos saved in the Photos app without the written, informed consent of Illinois users and without establishing a retention schedule and destruction guidelines as required by BIPA. Apple has moved for summary judgment, arguing that it neither collects nor possesses any biometric identifiers or biometric information. Plaintiffs also seek partial summary judgment on the issue of Apple's liability.

For the reasons set forth below, the Court grants Apple's motion only as it pertains to so-called face crops. The remainder of Apple's motion is denied. Plaintiffs' motion for partial summary judgment is also denied.

BACKGROUND

Unless otherwise noted, the following facts are drawn from the parties' statements of undisputed facts.

Apple preinstalls the Photos app on its iPhones, iPads, Macs, and Apple TVs, and it cannot be uninstalled by users. (PSOF ¶ 3). When a user takes photos on their device using Apple's Camera app, those photos are saved to the Photos app unless a user chooses to download a third-party camera app instead. (*Id.* ¶ 4). The Photos app contains software that uses on-device machine learning to organize and sort photos of people in the appropriately-named "People" album.[4] (*Id.* ¶ 7).

While the parties sharply contest the legal significance of various aspects of the People album technology, they broadly agree about how it works. First, Apple's software runs every photograph in a user's Photos app through a deep neural network (DNN), which is a machine learning algorithm structured with "layers" similar to the neurons in the human brain. (SOF ¶ 41; Doc. 177-4,¶ 35). Apple's DNN detects faces, positions of face landmarks, and upper torsos in images or video frames. (*Id.*; PSOF ¶ 44; Doc. 177-4, ¶¶ 69, 73). The algorithm then creates "bounding boxes" around faces and upper bodies.[5]

[4] If cats or dogs are detected in any photos, the album will recognize them as well. The album is then named "People & Pets." (Doc. 280-1, ¶ 7).

[5] The parties dispute the process by which the bounding boxes are created. Plaintiffs insist that the detection algorithm "relies on the shapes of key facial features" such as the eyes, nose, and mouth, and uses "landmark detection to estimate facial shape and pose," ultimately outputting confidence levels for

From these "bounding boxes," the algorithm creates two smaller photos, one of the face (referred to as a "face crop") and one of the upper body (referred to as a "torso crop").[6] (*Id.* ¶ 44).

Although the DNN detects faces and face landmarks, it does not map the coordinates of the face. (SOF ¶ 46). Instead, facial landmark information is only used to determine the coordinates and size of a bounding box, allowing the DNN to then select the best "crop" of the image. (Doc. 280-20, ¶ 42). Once the face is located, the crop is merely a smaller section of the original photograph. (*Id.*).

Face crops are then processed by a convolutional neural network ("CNN"). (*Id.* ¶¶ 48-49). Dr. Sheryl Brahnam, Plaintiffs' expert in machine learning, explains that a CNN is a type of deep neural network designed to process images and other forms of data represented as matrices. (Doc. 280-55, ¶ 32). It is composed of tens to hundreds of layers of "neurons," which extract features in an image. (*Id.* ¶ 37).

The earlier layers of a CNN, which are closest to the input image, learn to recognize simple patterns and features such as edges and lines in different orientations (horizontal, vertical, and diagonal), corners, and color variations. (*Id.* ¶ 34). Subsequent layers combine and recombine the features from the lower layers to detect increasingly complex patterns. (*Id.*). Plaintiffs assert that the "deeper" layers of the CNN "can

each detection, and information about the orientation and pose of the face. (PSOF ¶¶ 58-60). Apple acknowledges that the algorithm determines the coordinates and size of a bounding box but insists it provides no information about what is inside the box and does not pass any facial landmark information to subsequent steps in the process. (*Id.* ¶ 59).

[6] Plaintiffs do not allege that the torso crop contains or is derived from biometric data, so the Court limits its discussion to face crops.

recognize more sophisticated and abstract features like facial components (eyes, eyebrows, lips) until the combination of patterns within patterns within patterns encompasses entire objects . . . ." (Doc. 280-55, ¶ 34).

The layers of a CNN extract features by processing an image against a small matrix of weights, referred to as a "kernel" or "filter." (*Id.* ¶ 37). As a kernel crosses an image, it divides an image into small squares, which are then processed into a new image called a "feature map." (*Id.*). This process is referred to as a "convolution." (*Id.*). Kernels can be designed to search for particular properties in an image; for instance, a kernel targeted to detect vertical edges will produce a feature map where high values indicate the presence of a vertical edge. (*Id.* ¶ 41). Plaintiffs assert that facial attributes are "encoded" into the feature maps, so that the feature maps "capture the geometric characteristics of faces that uniquely describe the shapes of a particular person's facial features." (*Id.* ¶ 107; *see also id.* ¶ 97). Apple contends, however, that the CNN processes only local, two-dimensional patterns of color and intensity. (SOF ¶ 49).

CNNs typically incorporate "pooling layers" after every few layers to summarize the features of an image and decrease the complexity of the model. (*Id.* ¶¶ 43-45). The convolutional process is repeated numerous times, as a variety of kernels operate on the image. At the final processing stage, so-called "fully-connected layers" transform the convolutional layers into an output: a 128-dimensional vector, or "embedding vector," made up of 128 decimal-point numbers. (*Id.* ¶ 46; SOF ¶¶ 51-52). The vector is "not a random collection of numbers," but rather "encapsulates the significant features of the input . . . in a condensed form." (*Id.* ¶ 49). Some Apple employees, numerous internal

Apple documents, and Plaintiffs refer to the 128-dimensional vectors or embeddings as "faceprints." (PSOF ¶ 77; *see e.g.*, Doc. 280-29 p. 179).

It is undisputed that the numbers comprising a faceprint are not the measurements of distances between points on an individual's face. Nevertheless, they can be used to distinguish between faces. Dr. Brahnam explains that by using "a distance metric such as Euclidean distance or cosine similarity," one can determine the closeness or separation between the feature representations. (*Id.* ¶ 50). Thus, in a facial recognition program, the faceprints created from different photos of the same person would cluster closer in the "embedding space," while the faceprints of different people would cluster further away. (*Id.*). "By setting a threshold on the distance between vectors of the same person, the system can decide whether two images represent the same person." (*Id.*).

Apple does not dispute that its CNN, which was trained on a labeled dataset of thousands of cropped photos of faces from Flickr, stock photography, and Apple's own data, generates a faceprint for each photo. (Doc. 280-19, ¶¶ 22, 78-83; Doc. 280-28, pp. 195-97, 205). The software builds a model for each person appearing in the user's photo library against which the software can quickly compare faceprints from incoming photos. (Doc. 177-4, ¶ 102). The Photos app then runs a clustering algorithm on the faceprints, which scores the similarity and, if the scores are sufficiently close, groups or clusters the corresponding photos together in the People album. (SOF ¶¶ 58, 61-62).

Apple applies a unique numerical identifier to each cluster. (PSOF ¶ 136). Information about an individual depicted in a cluster of photos can become associated with the cluster in a variety of ways. A user can decide to label their People album

clusters, and Photos intelligently suggests names from the users' Contacts. (SOF ¶ 4; PSOF ¶ 140). The Photos app also generates a "knowledge graph" of people who are important to the user. (PSOF ¶ 144). The knowledge graph infers people who are important to the user based on the numbers of photos of a person, set relationships in Contacts, and the frequency of communications in the Messages app. (PSOF ¶ 145). To infer who is the user of the device, Photos considers information about the location where photos are taken and the overall frequency of certain individuals. (*Id.* ¶¶ 148-50). While Apple disputes that the Photos app or People album feature use "identity information" to infer the *identity* of the user, Apple's Senior Machine Learning Engineering Manager for Photos testified that the Photos app tries to understand the user of the device by looking to certain signals, including whether the photos are taken from the user's home, the number of selfies, and the number of photos with that person in them. (Doc. 280-10, pp. 149-152). Upon clustering photos of the inferred user, Photos will ask, "Is this a photo of you?" (PSOF ¶ 148).

For users who do not upload their photos to iCloud, faceprints remain on the device. Plaintiffs claim that faceprint data stored on-device is not encrypted, a fact that Apple disputes. (*Id.* ¶ 227). Apple admits, however, that the faceprint is not stored within the device's "Secure Enclave." (*Id.* ¶ 229).

For users who have enabled iCloud Photos, face crops and certain metadata, including user-supplied labels, are uploaded to Apple's servers in an end-to-end encrypted format. (*Id.* ¶ 203; SOF ¶ 83). Under the "Standard Data Protection" setting, Apple retains access to the encryption keys. (PSOF ¶ 219). If a user enables Advanced

Data Protection, the vast majority of their iCloud data is end-to-end encrypted, the encryption keys are stored only on the user's device, and the data is inaccessible to Apple. (SOF ¶ 94).

In July 2024, Apple released software updates that allow the transmission of users' faceprints to iCloud ("Sync Update"). (*Id.* ¶¶ 109-10). The Sync Update affects users who have iOS 17.6 or later versions, iCloud Photos enabled, an iCloud storage tier of at least 10 gigabytes, and more than 5,000 photos or videos on their device. (SOF ¶ 112). The Sync Update allows a user's other Apple devices signed into iCloud to download and decrypt the faceprint on that device, so that each device does not have to separately detect faces and regenerate the faceprint. (*Id.* ¶¶ 113-14). The clustering algorithm still runs locally on each device. (*Id.* ¶ 115). Apple claims the data is uploaded in an end-to-end encrypted format.[7] (*Id.* ¶ 119).

In the Fourth Amended Complaint (Doc. 251), Plaintiffs assert that the face crops and faceprints created and collected by Apple constitute biometric identifiers or biometric information. They further claim that, despite its collection of biometric data, Apple did not obtain users' informed, written consent or develop a written policy, made available to the public, establishing a retention schedule or guidelines for permanently destroying biometric data, in violation of BIPA sections 15(a) and 15(b).

On June 5, 2026, the Court certified the action as a class action comprised of the following three subclasses (Doc. 342):

[7] Plaintiffs dispute that the vector data is protected by end-to-end encryption, but they do not adequately support this claim with a citation to a relevant portion of the record.

Local Device Class

Every Illinois citizen whose Apple Device put a photograph of that citizen into a People album at any time between September 13, 2016, and the present.

iCloud Subclass

Every Illinois citizen who had an Apple Device with a People album tagged with that citizen's name or other identifier, and had an iCloud account enabled for photo storage, at any time between September 13, 2016, and the present.

iCloud Faceprint Subclass

Every Illinois citizen who had an Apple Device running iOS 17.6, MacOS Sonoma 14.6 or iPadOS 17.6 or later and: (1) had iCloud photo library enabled with at least 10 gigabytes of storage, and (2) their Apple Device put a photograph of that citizen into a People album, and (3) who had 5,000 or more assets (*i.e.*, photos and videos) in their iCloud photo library, at any time between March 25, 2025, and the present (inclusive).

LEGAL STANDARD

Summary judgment is appropriate where there is no genuine dispute of material fact and the movant is entitled to judgment as a matter of law. FED. R. CIV. P. 56(a). In determining whether a genuine issue of fact exists, the Court views the evidence and draws all reasonable inferences in favor of the non-moving party. *Ziccarelli v. Dart*, 35 F.4th 1079, 1083 (7th Cir. 2022). Once the moving party sets forth the basis for summary judgment, the burden shifts to the nonmoving party who must go beyond mere allegations and offer specific facts showing that there is a genuine issue of fact for trial. FED. R. CIV. P. 56(e); *see Celotex Corp. v. Catrett*, 477 U.S. 317, 323-24 (1986). A moving party is entitled to judgment as a matter of law where the non-moving party "has failed to make a sufficient showing on an essential element of her case with respect to which she has the

burden of proof." *Celotex*, 477 U.S. at 323.

DISCUSSION

I. Evidentiary Issues

The Court first addresses Apple's "Notice Regarding Plaintiffs' Failure to Dispute Its Additional Material Facts and Request to Deem Facts Admitted." (Doc. 325). Plaintiffs did not explicitly dispute Apple's Additional Material Facts in Opposition to Plaintiffs' Motion for Partial Summary Judgment (Doc. 306-2); therefore, Apple has asked the Court to deem those facts admitted pursuant to Local Rule 56.1(g).

In response, Plaintiffs argue that 96 of the 123 additional material facts are identical to facts that they already disputed or admitted, while the remaining 27 were previously addressed in substance by Plaintiffs. As a result, Apple's request would require the Court to consider identical and near-identical facts, both admitted and denied, for purposes of different summary judgment motions in the same litigation. Plaintiffs ask the Court to deny Apple's request or allow Plaintiffs leave to file their response to the additional facts.

The Seventh Circuit has "repeatedly held that a district court is entitled to expect strict compliance with Rule 56.1." *Ammons v. Aramark Unif. Servs., Inc.*, 368 F.3d 809, 817 (7th Cir. 2004) (citing *Bordelon v. Chicago School Reform Bd. of Trustees*, 233 F.3d 524, 527 (7th Cir. 2000) ("Given their importance, we have consistently and repeatedly upheld a district court's discretion to require strict compliance with its local rules governing summary judgment.")). Nevertheless, because the facts were addressed by Plaintiffs in response to Apple's motion for summary judgment, the Court denies Apple's request.

II. BIPA

Under section 15(a) of BIPA, a private entity in possession of biometric identifiers or information must develop, publish, and comply with a written policy that establishes a data retention schedule and guidelines for destroying biometric identifiers and information. 740 ILL. COMP. STAT. 14/15(a). Section 15(b) prohibits a private entity from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric identifier or biometric information unless they first provide notice and obtain the person's written consent. *Id.* § 15(b). The statute defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id.* § 10. "Biometric information" is information based on an individual's biometric identifier and used to identify an individual. *Id.*

There is no dispute that Apple did not develop, publish, and comply with a written data retention and destruction policy with respect to the Photos app's facial recognition technology. Nor did it provide notice and obtain written consent from any Illinois user. Thus, to prevail on summary judgment, Apple must point to evidence demonstrating, under section 15(a), that it is not in possession of biometric identifiers or information and, under section 15(b), that it has not collected, captured, or otherwise obtained a person's biometric identifier or biometric information. For Plaintiffs to be entitled to summary judgment, they must point to evidence proving the opposite.

III. Biometric Identifiers

Apple first argues that neither face crops nor faceprints are "biometric identifiers" or "biometric information" under BIPA. Because biometric information is derived from a

biometric identifier, the Court must first determine whether the data at issue is a biometric identifier.

BIPA explicitly defines a biometric identifier: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILL. COMP. STAT. 14/10. As this Court and others have observed, to constitute a biometric identifier, the data must be capable of identifying a person. *See Hazlitt v. Apple Inc.*, 500 F. Supp. 3d 738, 749 (S.D. Ill. 2020); *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117, 1123 (9th Cir. 2024) (explaining that an alternate reading of "biometric identifier" would "write the term 'identifier' out of BIPA."); *G.T. v. Samsung Elecs. Am. Inc.*, 742 F. Supp. 3d 788, 800 (N.D. Ill. 2024); *see also Javid v. M.A.C. Cosms., Inc.*, No. 25 CV 11693, 2026 WL 1601454, at *2 (N.D. Ill. June 4, 2026) (collecting cases). Thus, the questions before the Court are whether the face crops and faceprints created by Apple's technology are (1) scans of face geometry and (2) capable of identifying a person.

A. *Face Crops*

At the outset, the Court finds that the face crops created by Apple's face detection algorithm are not biometric information or biometric identifiers (*i.e.*, scans of face geometry that are capable of identification). Apple has presented evidence that in creating the face crops, the People album technology does not map the coordinates of a face, and that, even if some facial landmark information is used to create the face crop, that information is not provided to the faceprinting CNN. (SOF ¶¶ 46, 47). Instead, facial landmark information is only used to determine the coordinates and size of a bounding box to then select the best "crop" of the image for generating the faceprint. (Doc. 280-20,

¶ 42). Once that process occurs, the face crop is only that: a cropped image of a face.

Plaintiffs do not genuinely dispute these facts. They assert that the detection algorithm incorporates geometric information about the *location* of the face in the image and uses facial features such as eyes to adjust the face within the bounding box. But the location of a face within a photo says nothing about that face's geometry, and Plaintiffs have not identified any record evidence suggesting that this information would be sufficient to identify a person.

For these reasons, the Court finds that Apple is entitled to judgment as a matter of law that face crops are not biometric identifiers or biometric information. As a result, the iCloud Subclass, which claims only that face crops, user-inputted information, and other metadata was synced to iCloud, does not have a viable legal theory on which to proceed. The Court therefore decertifies the iCloud Subclass pursuant to Federal Rule of Civil Procedure 23(c)(1)(C). The class members, however, remain part of the Local Device Class.

The remainder of the Court's decision will discuss only faceprints.

B. *Faceprints*

i. Scans of Face Geometry

In arguing that faceprints are not scans of face geometry, Apple downplays the significance of its technology. It asserts that the People album software simply "generates data" from photographs to group together photos that are similar. Because the app is merely comparing photographs, not creating, collecting, or comparing face geometry, Apple argues, BIPA does not apply. *See Martell v. X Corp.*, No. 23 C 5449, 2024 WL

3011353, at *3 (N.D. Ill. June 13, 2024) ("If the scan merely compares the image to see if it is the same as other images, that does not imply the use of facial geometry."). Apple describes its process in three steps.

First, the People album's DNN "processes" a two-dimensional image to detect faces and upper torsos to create bounding boxes around them. (Doc. 281, p. 12). It then crops the photo into a face crop and a torso crop. (*Id.*). Second, the CNN analyzes the pixels within the face crop to generate the faceprint. (*Id.*, p. 13). Apple asserts the technology does not rely on the distances between parts of the face or the face's three-dimensional shape to do this. (*Id.*). Instead, two-dimensional patterns of color and intensity in the pixels are, again, "processed" to plot the photo into the vector. (*Id.*). The faceprint itself does not correspond to specific visible facial features or measurements, and it cannot be used to recreate a face. (*Id.*). Finally, Apple applies a clustering algorithm to the faceprint to group photos together "by calculating the vector distance between two samples in the high-dimensional feature space." (*Id.*). That is, it compares the faceprints to group similar faces. (*Id.*). The clustering algorithm does not, Apple contends, use geometric measurements.

In response, Plaintiffs claim that faceprints incorporate face geometry in the second step of Apple's process. They argue that the CNN mimics human vision by employing convolutional layers that detect and interpret geometric patterns in visual data, citing to Dr. Brahnam's testimony as an expert in machine learning and neural networks.

Few courts have meaningfully addressed what constitutes a "scan" of "face

geometry." One of the few to do so was the Northern District of California in *In re Facebook Biometric Information Privacy Litigation*. The technology at issue was Facebook's "Tag Suggestions" feature. *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. 535, 541 (N.D. Cal. 2018), *aff'd sub nom. Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019). Like Apple's technology here, Facebook's software detected faces, aligned their orientation, and computed a "face signature"—a string of numbers representing a particular image of a face. *Id.* The face signatures were then compared against a stored database of "face templates" to look for matches. *Id.* A "face template" was a string of numbers that represented a boundary between the face signatures of a given Facebook user and the face signatures of others. *Id.* If the face signature fell within the boundary of a user's face template, Facebook suggested tagging that user. *Id.* The face signatures were not stored by Facebook, but the face templates were. *Id.*

At the summary judgment stage, the plaintiffs claimed Facebook's technology collected scans of face geometry "because it use[d] human facial regions to process, characterize, and ultimately recognize face images." *In re Facebook Biometric Info. Priv. Litig.*, 2018 WL 2197546, at *2 (N.D. Cal. May 14, 2018). Facebook, like Apple, disagreed that its technology scanned facial geometry and instead claimed that it analyzed pixels, not any particular human facial features. *Id.* at *3. The technology then learned for itself what features of an image's pixel values are most useful for characterizing and distinguishing human faces. *Id.*

The Northern District of California rejected Facebook's suggestion that "scan of face geometry" must mean "an express measurement of human facial features," finding

that Facebook's argument begged the question of what the technology actually did—which was a question for a jury. *Id.* As relevant here, the court then stated:

> In addition, the word "scan" does not bear the definitional freight Facebook seeks to impose. BIPA does not specifically define it, and the ordinary meaning of "to scan" is to "examine" by "observation or checking," or "systematically . . . in order to obtain data especially for display or storage." Merriam-Webster's Collegiate Dictionary at 1107-08 (11th ed. 2003). "Geometry" is also understood in everyday use to mean simply a "configuration," which in turn denotes a "relative arrangement of parts or elements." *Id.* at 524, 261. None of these definitions demands actual or express measurements of spatial quantities like distance, depth, or angles. In addition, the Illinois legislature's decision to use the word "scan" rather than "record" does not indicate that express measurements are required, and limiting scans of face geometry to techniques that literally measure distances, depths, and angles cannot be squared with the legislature's clear intent to regulate emergent biometric data collection technology in whatever specific form it takes.

Id.

Here, Apple suggests that it merely "scans" photographs, not faces, and compares the photographs to sort them into albums. It also asserts that, under BIPA, "face geometry" means a "three-dimensional representation of the facial structure." Like Facebook, Apple has construed the terms "scan" and "face geometry" too narrowly.

"When the language of the statute is clear, it must be applied as written without resort to aids or tools of interpretation, even though the consequences may be harsh, unjust, absurd or unwise." *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117, 1122 (9th Cir. 2024) (cleaned up) (citing *DeLuna v. Burciaga*, 857 N.E.2d 229, 236 (Ill. 2006) and *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 928 (Ill. 2023)).

Here, the ordinary meanings of "scan" and "face geometry" are clear. Dictionaries define "scan" as "to examine by point-by-point observation or checking" or "to look at

searchingly, examine with the eyes."[8] And while geometry is defined as a branch of mathematics, it also can mean a "configuration" or the spatial arrangement of objects or constitutent parts"[9]—far broader than Apple's suggested definition.

And, there is evidence in the record from which a jury could conclude that Apple's faceprints constitute a scan of face geometry. In Dr. Brahnam's expert reports, she explains that the pixels in 2D photos "encode information" about 3D surfaces and shapes, including shading, perspective, and depth cues, as well as geometric properties including edges and corners. (Doc. 281-65, ¶ 5(c); Doc. 280-55, ¶ 92). When a photo of a face is inputted into a CNN, Dr. Brahnam explains, the early layers of the CNN learn to "recognize simple patterns and features such as edges and lines in different orientations (horizontal, vertical, and diagonal), corners, and color variations." (Doc. 280-55, ¶ 34). Subsequent layers then combine and recombine the features from the lower layers to detect increasingly complex patterns. (*Id.*). Finally, the deeper layers of a CNN recognize more sophisticated and abstract features like facial contours and the shapes of the mouth and eyes. (*Id.* ¶ 67). She also opines that deep learning models "can reconstruct high-fidelity 3D face representations from 2D images." (Doc. 281-65, ¶ 27).

Dr. Atif Hashmi, retained by Plaintiffs to review Apple's source code, opined that Apple's technology uses both the simple and complex facial features extracted by Apple's CNN to create a faceprint. (Doc. 280-15, ¶ 48). He further opined that a faceprint derived

[8] Merriam-Webster's Collegiate Dictionary at 1107-08 (11th ed. 2003); "Scan," Oxford English Dictionary https://www.oed.com/dictionary/scan_v?tab=meaning_and_use#24122676 (last visited Sept. 23, 2026).
[9] Merriam-Webster's Collegiate Dictionary at 524 (11th ed. 2003); "Geometry," Oxford English Dictionary, https://www.oed.com/dictionary/geometry_n?tab=meaning_and_use#3101995 (last visited Sept. 23, 2026).

from a CNN trained on human faces can be reverse-engineered through "model inversion" to reconstruct the original face to a certain degree of accuracy. (*Id.* ¶ 49). Model inversion is a type of machine learning process that involves using the output of a trained DNN in combination with the DNN parameters to reconstruct the corresponding training inputs. (Doc. 177-4, ¶ 44). Given that faceprints can be used to reconstruct the face, CNNs "inherently maintain and are able to determine spatial relationships among shapes present within a face." (Doc. 280-16, ¶ 49). Otherwise, a face reconstructed through model inversion may have an eye where the mouth should be, and so on. (*Id.*)

Even Apple's biometrics expert, Dr. Creed Jones, agreed that CNNs "operate directly" on the pixels on an image, "enabling them to capture complex, non-linear relationships between images of faces." (Doc. 280-19, p. 17). Moreover, Dr. Jones opines, "face recognition algorithms are designed to maximize the distinctions between human faces, to maximize the model's ability to distinguish between people even if they appear superficially similar." (*Id.* p. 18). To do this, the CNN "has as its input the entire face image, and each individual element in the embedding [faceprint] may be calculated from many different parts of the face image." (*Id.* p. 19). In other words, Dr. Jones does not dispute that CNNs "scan" the pixels of an image to create a faceprint that encapsulates the many different features of a face. Nor does he offer an alternative theory of how the CNN is able to distinguish between faces other than some reliance on geometry in its broadest sense.

From this evidence, along with the plethora of other exhibits including internal documents, patent applications, expert opinions, and testimony from Apple employees,

a reasonable jury could find that Apple's technology incorporates scans of face geometry, as those terms are ordinarily understood, to create faceprints. *See Fleury v. Union Pac. R.R. Co.*, No. 20 C 390, 2026 WL 2445189, at *16 (N.D. Ill. Aug. 20, 2026) (finding that the defendant's use of terminology such as biometrics, biometric scanner, fingerprint server, and biometric data when referring to its technology "shed light on [its] nature and purpose" and suggested the technology fell within the plain and ordinary meaning of those words as they are used in BIPA). Thus, Apple is not entitled to summary judgment on the issue of whether a faceprint is a scan of face geometry.

At the same time, there is enough competing evidence in the record to create a genuine issue of material fact and preclude summary judgment for Plaintiffs. For example, Dr. Jones opined that faceprints do not represent measurements of a person's face, are not based on facial landmarks, and do not measure or capture the geometric representation of a face. (Doc. 280-19, ¶ 75). He also explains in his rebuttal report that the "shapes recognized by CNNs are more accurately described as local intensity patterns in the pixels of a photograph than geometric shapes" and that the calculation performed by a convolutional layer is a "sum-of-products response to intensity patterns," not a geometric calculation (Doc. 280-20, ¶ 25). A jury crediting Dr. Jones's opinions over Dr. Brahnam's could conclude that Apple's CNN does not scan face geometry. Therefore, summary judgment for Plaintiffs is also not appropriate.

ii. Capable of Identification

The Court next considers whether faceprints are capable of identifying class members.

Apple argues that Plaintiffs lack any evidence that the Photos app identified them or that it *could* identify them. It reasons that the app merely groups similar faces together but does not "recognize" the identities of those individuals in any literal sense. Only users can identify the individuals in a particular photo by adding labels to the clusters. Even then, all user-inputs are encrypted and cannot be accessed by Apple. It further asserts that extending BIPA to any scan of any face, regardless of the ability to tie that scan back to an identifiable person, would depart from the General Assembly's intent in enacting BIPA.

In response, Plaintiffs contend that BIPA contains no requirement that they prove Apple actually used a biometric identifier to identify them, and, even if it did, Apple identifies its users in multiple ways. For instance, the Photos app "automatically identifies" the user and asks them to confirm their identity by asking them, "Is this you?" Plaintiffs also cite evidence that the app creates a "knowledge graph" of patterns in a user's life to infer the user's identity.

In its reply brief, Apple asserts that it is up to a user whether to label a grouping of photos in an album, and Apple has no way to verify whether a given label is accurate.

Courts evaluating the identification requirement, including this one, have generally agreed that it does not matter whether a defendant has actually used its technology to identify a person. Instead, the relevant question is whether the biometric data is *capable* of identifying a person. *See Eskridge v. HMD Trucking, Inc.*, No. 24 CV 12437, 2025 WL 1547435, at *2 (N.D. Ill. May 30, 2025) ("The statute does not require a defendant to have used biometric information or a biometric identifier to identify a person; only that

the identifier is capable of identifying an individual."); *Howe v. Speedway LLC*, No. 19-CV-01374, 2024 WL 4346631, at *8 (N.D. Ill. Sept. 29, 2024) (noting that whether a finger scan qualifies as a biometric identifier "depends on whether the scan is a sufficiently unique personal feature capable of being used to identify a specific person"); *Hartman v. Meta Platforms, Inc.*, No. 3:23-CV-02995, 2024 WL 4213302, at *10 (S.D. Ill. Sept. 17, 2024) (similar); *Castelaz v. Estee Lauder Companies., Inc.*, No. 22 CV 5713, 2024 WL 136872, at *7 (N.D. Ill. Jan. 10, 2024) (similar); *see also Zellmer*, 104 F.4th at 1125 ("[E]ven if a company *does not* use face scans to identify a person, BIPA applies if it *could*.").

The fact that a defendant collects other information about an individual in connection with the biometric data is a relevant factor in determining whether the technology is capable of identification. *See Javid*, 2026 WL 1601454, at *5-6 (finding the plaintiff had plausibly alleged an ability to identify where she claimed the defendant could pair her biometric data with information from her customer account, which included her name, date of birth, zip code, email address, and past purchases); *Castelaz*, 2024 WL 136872, at *7 (faulting a plaintiff for failing to allege that a defendant could use a facial scan either "alone or in conjunction with other methods or sources of information" to identify class members). While these district court cases were decided at the pleadings stage, the Court agrees that whether a defendant can connect users' biometric data with their account information is relevant to whether the data is capable of identifying.

Apple's argument that the People album—the technology itself—cannot identify users is misplaced. The relevant question is whether the output of the technology, *i.e.*, the faceprint, is capable of identifying a person. And here, there is evidence in the record

from which a reasonable jury could make that finding. Plaintiffs have pointed to testimony from Apple employees that a "faceprint can be used to uniquely identify a person," Apple's internal documents, and Apple's patent applications, which state among other things that "a faceprint is a feature vector defined in n-space that uniquely identifies a face image but does not associate a name with the face." (Doc. 280-60, p. 88; Doc. 287-29; Doc. 287-30 at p. 24; Doc. 287-31). Moreover, for users in the iCloud Faceprint Subclass, it is undisputed that the users' faceprints are synced to the cloud and, therefore, associated with their iCloud account, which includes significant identifying information. And for any user who adds personal identifying information to their People album, their faceprints are, without a doubt, connected to their identity.[10]

The Court also is not persuaded by Apple's argument that identification requires an enrollment process whereby known and confirmed identities are added to a database along with corresponding biometric templates. This "enrollment" step can be illustrated, for example, by the fact that a suspect in a criminal case can be identified by fingerprint, but only if that fingerprint is already part of a database of known individuals. Apple's position would require the Court to read into BIPA a requirement that does not exist in its text. BIPA was enacted, in part, to protect unique biometric identifiers. There is no condition that a person's biometric identifier is only protected if it has been affirmatively enrolled into a database. Moreover, Apple's expert, Dr. Jones, opined that enrollment can include "the capture of one or more samples to be used for later comparison." (Doc. 280-

[10] The Court notes, however, that none of the named Plaintiffs labeled their People albums with anything more than a first name.

19, ¶ 55). Dr. Hashmi explains that is exactly what happens when Apple's algorithm analyzes faceprints that correspond to individuals verified by the user or by Apple's knowledge graph. (Doc. 280-15, ¶ 53).

From a practical standpoint, this makes sense. If the faceprints of a specific person cluster together, thereby permitting every photo of that person to be grouped together in the People album, then those faceprints are inevitably connected to the images of that person (and name, if the user has verified the identity or Apple has intelligently suggested an identifier). And, because clustering is done on the device, a jury could reasonably infer that a user's clustered faceprints and associated metadata are connected with their unique Apple account information, particularly if they checked "yes," when asked, "Is this a photo of you?" And even if the statute incorporated an enrollment requirement in some sense, the evidence discussed above suggests the existence of a fact question regarding whether Apple associates its faceprints with personally identifying information in much the same way as an enrollment database would.

For these reasons, the Court finds that Apple is not entitled to summary judgment on the issue of identification.

On the other hand, there is also evidence from which a jury could find that faceprints are not capable of identifying an individual. It is undisputed that a faceprint is a 128-dimensional vector of decimal-point numbers, not an image of a face. Dr. Jones stated that if the faceprinting CNN were presented with an image *without* a human face in it, the CNN would still generate a vector of 128 floating-point numbers that would not look, to the human eye, any different than a faceprint. (Doc. 280-19, ¶ 79). He further

opined that reconstruction of a face from a faceprint is unrealistic, if not impossible, given that model inversion requires an intimate knowledge of the model, and Apple's model is not publicly available. (*Id.* ¶¶ 134-35). There is also testimony from key Apple engineers, including Apple's Senior Machine Learning Engineering Manager in Photos, that the algorithm does not identify a person in a photo. Rather, it is merely "a number of bits and bytes." (*See, e.g.*, Doc. 280-10, pp. 90, 97; Doc. 280-11, p. 120-22). From this evidence, a jury could find that the faceprints created by Apple's technology are not capable of identifying a person. Accordingly, Plaintiffs also are not entitled to summary judgment on the issue of identification.

IV. Collection or Possession of Biometric Data

Apple next argues that Plaintiffs have not established a BIPA violation because there is no evidence that it *collects* or *possesses* biometric data.

BIPA section 15(a) applies to a private entities that are in "possession" of biometric identifiers or biometric information, while section 15(b) applies to private entities that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric identifiers or biometric information. 740 ILL. COMP. STAT. 14/15(a), (b). Because BIPA does not define these terms, both Illinois state and federal courts within the Seventh Circuit have turned to their dictionary definitions. In so doing, they have concluded that whether an entity possesses, collects, captures, purchases, receives, or obtains biometric data comes down to the issue of control.

In *Cothron v. White Castle System, Inc.*, the Illinois Supreme Court noted the dictionary definition of "collect" is "to receive, gather, or exact from a number of persons

or other sources," while "capture" means "to take, seize, or catch." 216 N.E.3d 918, 924 (Ill. 2023). The *Cothron* court further observed that that "[t]he active verbs used in section 15(b)—collect, capture, purchase, receive, and obtain—all mean to gain control[.]" *Id.; cf. Salinas v. Arthur Schuman Midwest, LLC*, 283 N.E.3d 45, 52 (Ill. App. Ct. 2026) (holding that defendants' "ministerial implementation" of a biometric time clock system was insufficient to trigger section 15(b) liability when a different entity possessed the data and could access or control its use).

Courts interpreting the possession requirement of section 15(a) have also imposed a control requirement. *See Clark v. Microsoft Corp.*, 688 F. Supp. 3d 743, 749 (N.D. Ill. 2023) ("While data storage alone may be insufficient, storage of data together with the ability to control access to that data adequately pleads possession."); *Tapia-Rendon v. Workeasy Software, LLC*, No. 21 C 3400, 2025 WL 2299592, at *7 (N.D. Ill. Aug. 8, 2025) (concluding that a jury could find the defendant violated BIPA when it controlled its servers and, thus, possessed the data on those servers).

The Seventh Circuit recently signaled its approval of the control requirement in *G.T. by & through Hanlon v. Samsung Elecs. Am., Inc.*, 186 F.4th 470 (7th Cir. 2026). Although decided on a motion to dismiss, the facts of *G.T.* are closely analogous to those at issue here, and Apple argues it is dispositive of this case.

In *G.T.*, the plaintiffs, who were owners of Samsung smartphones, allegedly used their devices to take photos and then saved those photos on the preinstalled Samsung Gallery app. *Id.* at 473. Like here, the plaintiffs alleged that, once a picture is saved on the device, the Gallery app automatically scans the photo to determine whether it captured

a face. *Id.* If a face is detected, the app then makes a template of the person's unique facial geometry to create a "face template." *Id.* Plaintiffs further alleged that "Samsung has complete and exclusive control over the Biometrics it captured, collected and stored on Samsung Devices." *Id.*

On appeal from the dismissal of the case on the pleadings, the question before the Seventh Circuit was whether the plaintiffs adequately alleged Samsung possessed, collected, captured, or otherwise obtained the facial geometry scans or face templates generated by its software. Because BIPA does not define those terms, the court turned to Illinois state court decisions and the words' ordinary meanings. It determined that "possession" under section 15(a) "occurs when a person *has* or *takes control* of the subject property or holds the property at his or her disposal." *Id.* at 475 (quoting *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005)); *see also Barnett v. Apple Inc.*, 225 N.E.3d 602, 609 (Ill. App. Ct. 2022) (the meaning of "possession" within BIPA section 15(a) is "to have control").

Turning to section 15(b), the court relied on the Illinois Supreme Court's definitions of "collect" and "capture" in *Cothron*. Having no authority for the meaning of "obtain," the Seventh Circuit referred to Webster's Third New International Dictionary, which defines obtain as "to gain or attain possession or disposal" or "hold, keep, possess, occupy." *Id.*

Considering these definitions, the Seventh Circuit determined that BIPA sections 15(a) and (b) require an entity to "have or have obtained some degree of 'control' over the biometric data in question." *Id.* at 475-76. The court rejected the idea that a company "controls" biometric data by virtue of it solely providing the software that captures the

data. *Id.* at 476.

In coming to this conclusion, the Seventh Circuit relied in part on the Northern District of Illinois's decision in *Bhavilai v. Microsoft Corp*., which also was decided on a motion to dismiss. 716 F. Supp. 3d 640 (N.D. Ill. 2024). There, the plaintiff alleged Microsoft designed, licensed, and sold software in the Windows operating system that captured users' facial biometric data, and that Microsoft's "control over the device users' ability to access and use the facial scan software" was sufficient to satisfy BIPA's control requirement. *Id.* at 641. The Northern District court rejected this argument and held that "control of the facial scan software is not the same as control of the facial scan data that is collected using the software." *Id.* Because the plaintiff did not allege that Microsoft exercised control over the facial scan data "in any way," it found Microsoft did not possess the data. *Id.*

The Seventh Circuit also relied on the Illinois appellate court's decision in *Barnett*, where the plaintiffs claimed Apple's Touch ID and Face ID features and software 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." 25 N.E.2d at 604. The plaintiffs also alleged that Apple "exclusively owned the software and prohibited users from accessing the biometric data saved on the devices." *Id.* On appeal from the trial court's dismissal of plaintiffs' claims, the Illinois appellate court found that Apple's "device and software are the tools," but it is the user who "utilizes these tools to capture her own biometric information." *Id.* at 610. The user also could disable the features and delete the data, and the plaintiffs did not allege that Apple saved

the data on its servers. *Id.* Thus, the court found that the plaintiffs did not adequately allege possession. *Id.*

With those cases in mind, the Seventh Circuit concluded that the *G.T.* plaintiffs failed to adequately allege control because the facial geometry at issue was only stored on their devices, Plaintiffs did not allege that Samsung had the ability to access, modify, or use facial geometry data in any way, and the plaintiffs failed to plausibly support their theory that their facial geometry data was being backed up to the cloud along with their photos. *Id.* at 477.

While the court acknowledged that technology companies have more information about their proprietary systems than consumers, who "may not be able to ascertain their inner workings without the aid of discovery," it found that the plaintiffs could have relied on "publicly available patents and other public disclosures" to draft a complaint that would withstand judicial scrutiny. *Id.* In conclusion, the Seventh Circuit held 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." *Id.* at 478.

Apple argues that *G.T.* is dispositive as to the Local Device class because all on-device processed data remains on the users' devices, and Apple has no ability to access this data. Apple also contends that *G.T.* compels summary judgment as to the iCloud Faceprint Subclass because the faceprints are end-to-end encrypted, and it has no ability to decrypt or read the data. It directs the Court to criminal cases where courts have found

the Government did not posssess data where it could not break a device's encryption.

G.T. is not the silver bullet that Apple believes it to be. Unlike the plaintiffs in *G.T.*, it is undisputed that, with its July 2024 software update, Apple took faceprints from users' devices and began syncing them to its cloud-based servers. This evidence demonstrates not only that Apple likely has possession and control over the iCloud Faceprint Subclass's data, but that it *may* also have possession and control for purposes of BIPA over the on-device faceprints of the Local Device class. Indeed, Meera Shah, a former senior software engineer and head of product, program, and operations for Apple Cloud Services testified that Apple decides whether to make faceprints, what metadata is associated with the faceprints, where faceprints are stored on a user's device, the security measures on the device, whether the data is encrypted, the retention period for faceprints, whether any Application Programming Interface (API) can access the faceprints stored locally on devices, and whether to issue an update that would delete faceprints for all users. (Doc. 280-60, pp. 145-51). Shah noted, "it's software. You could write any software that is enabled on iOS and [it] could do what you are asking to be done." (*Id.*, p. 151). And unlike *G.T.*, where Samsung's devices were operating on Google's Android software, Apple has control over its software at all times. (Doc. 306-2, ¶ 213 (admitting that "the software installed on Apple devices is owned by Apple, and that Apple determines the contents of its source code.")).

The Court is also not persuaded by Apple's argument that because the data synced to the cloud is end-to-end encrypted, meaning it cannot *read* the data, it does not possess, collect, capture, or obtain the data.

First, BIPA contains no explicit defense or carveout for entities with encryption protocols to protect biometric data and, in fact, the statute contains a provision mandating that private entities in the possession of such data protect it "using the reasonable standard of care within the private entity's industry" and "in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILL. COMP. STAT. 14/15(e). Thus, the legislature clearly recognized the value of data security. Had the legislature wished to make such protection a complete defense to an action under section 15(a) or (b), it could have done so. Instead, the statute includes distinct and independent claims under each subsection, suggesting that the legislature intended to emphasize different issues with each provision. For section (a), that focus is the existence of a written records retention policy. For section (b), the focus is the user's informed consent to the entity's collection of biometric data. Apple might be required to encrypt data under section (e), but that encryption is not an affirmative defense to other provisions.

Second, for purposes of BIPA, "control" does not necessarily require an entity to understand the contents of the data. To illustrate, consider a collector of Ancient Egyptian artifacts covered in hieroglyphic scripts. For centuries, these hieroglyphics were considered indecipherable, and the stories they encoded were considered lost to history. But with the discovery of the Rosetta Stone—a slab bearing the text of a decree written in both Ancient Greek and Ancient Egyptian—scholars learned to decipher the

hieroglyphics and read many Egyptian texts.[11]

Before scholars made these advances, however, our collector had no way to know what the writing on his artifacts meant. He might have speculated that a particular piece heralded the deeds of the Pharaoh Ramesses the Great, but it could have just as easily been an agricultural log. Even after the discovery of the Rosetta Stone, he might have opted *not* to decode the artifact, preferring to leave the contents of its hieroglyphics a mystery.

Yet, as the possessor of the artifact, one would naturally view our collector as assuming a degree of control over its contents. The collector, for instance, indisputably could modify the text, perhaps by adding a few random hieroglyphic characters of his choosing. He might post the hieroglyphs in some public forum. He could even destroy the artifact altogether. The collector thus undoubtedly exercises "control" over the hieroglyphic text regardless of whether he (or anyone else) can understand it.

The situation is similar for the faceprint data here. Apple concedes that faceprints are "transmitted[] and stored" in the iCloud Photos library for users who meet a specific list of criteria. (SOF ¶¶ 110-12). But its insistence that it cannot unscramble and decipher the data is immaterial to its "control" of the data. By dint of its authority over its servers where the data is maintained and its software, it undoubtedly *could* (among other things) re-write, make available to the public, remove encryption from, or delete entirely, the faceprint data. Apple admitted as much at oral argument, when it conceded that it could

[11] *See* Meilan Solly, *Two Hundred Years Ago, the Rosetta Stone Unlocked the Secrets of Ancient Egypt*, Smithsonian Magazine (Sept. 27, 2022), https://www.smithsonianmag.com/history/rosetta-stone-hieroglyphs-champollion-decipherment-egypt-180980834/.

decide one day to no longer protect the data with end-to-end encryption. (Doc. 369, p. 22). And technological progress may make today's encryption flimsy. Apple is not entitled to judgment as a matter of law on the issue of control just because the faceprints are encrypted.

Finally, Apple argues that the decision whether to use the Camera app, to store photos and videos in the Photos app, and to sync any data to iCloud Photos is completely optional. Thus, the undisputed facts show that the control required by BIPA resides exclusively with Plaintiffs as the device owners, not Apple.

This argument, which originated in *Barnett* and was mentioned by the court in *G.T.*, does not carry the same weight here. In *Barnett*, users voluntarily elected to use Face ID or Touch ID (as opposed to a numerical passcode) and knew the device was capturing their biometric data when they enabled those features. They also knew Apple was saving the data on the device so that they could log in to their phone using their face or finger. Here, users do not consent to the collection of their faceprints, they do not know the faceprints are being collected, there is no ability for users to turn off the feature, and there is no user knowledge that faceprints are saved on the device or in the cloud.

Because Plaintiffs have presented evidence that the faceprints created by Apple's software are uploaded to Apple's servers, Apple is not entitled to judgment as a matter of law on the issue of collection or possession as to the iCloud Faceprint Subclass. The Court also declines to grant summary judgment for Plaintiffs as to the Local Device class because Plaintiffs have conceded that an issue of fact exists as to whether Apple can access faceprints stored on the device. Finally, the Court reserves ruling as to the iCloud

Faceprint Subclass until class notice can be issued to the remaining class and subclass, as amended by this Order.

V. Whether Plaintiffs Are Entitled to Damages

Finally, Apple argues that Plaintiffs cannot meet their burden to prove they were aggrieved when there is no evidence that it has ever accessed their faceprints, whether on device or in the cloud, for any purpose. Rather, it is Plaintiffs who decide whether to use the Photos app, when to delete photos, whether to label People albums, and whether to use iCloud Photos. Plaintiffs assert this argument has no basis in law; federal courts agree with Illinois state courts that a person is "aggrieved" by the mere violation of BIPA's statutory requirements, as unlawful collection or retention of biometric data is itself a cognizable privacy injury.

The Court agrees with Plaintiffs. There is no statutory requirement that Apple actually access a user's biometric for him or her to be aggrieved, only that it is possesses, or is in "control" of the data. *See Citizens Ins. Co. of Am. v. Wynndalco Enters., LLC*, 70 F.4th 987, 991 (7th Cir. 2023) ("A violation of the statute as to one's biometric information is sufficient in and of itself to render an individual an "aggrieved person" entitled to pursue relief; he or she need not suffer an actual injury as a result of the violation."); *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 627 (7th Cir. 2020) (holding that "a consumer's loss of the power and ability to make informed decisions about the collection, storage, and use of her biometric information" alone is a concrete and particularized injury).

Because Plaintiffs have presented evidence from which a jury could find that Apple collected and possessed their faceprints, they have met their burden of proving

they were aggrieved under BIPA sections 15(a) and 15(b).

CONCLUSION

For these reasons, the Court **GRANTS in part and DENIES in part** Defendant Apple Inc.'s Motion for Summary Judgment. (Doc. 281).

The Court finds that face crops do not constitute biometric identifiers or biometric information and therefore **DECERTIFIES** the iCloud Subclass. The members of the former iCloud Subclass remain members of the Local Device Class.

The Court **RESERVES RULING** on the issue of collection or possession of the data at issue as to the iCloud Faceprint Subclass. The remainder of Plaintiffs' Partial Motion for Summary Judgment (Doc. 280) is **DENIED**.

Plaintiffs' Motion for Approval of Class Notice (Doc. 353) is **DENIED as moot and without prejudice**. Plaintiffs are **ORDERED** to modify their proposed class notice to reflect the decertification of the iCloud Subclass and file an amended motion on or before **October 14, 2026**.

This Order shall remain provisionally sealed until **October 7, 2026**. Motions to redact any portion of the Order shall be filed by that date.

IT IS SO ORDERED.

DATED: September 30, 2026

Nancy J. Rosenstengel

NANCY J. ROSENSTENGEL
United States District Judge