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

ROSLYN HAZLITT, JANE DOE, by and through Next Friend JOHN DOE, RICHARD ROBINSON, and YOLANDA BROWN, on behalf of themselves and all other persons similarly situated,	
Plaintiffs,	
v.	**Case No. 3:20-CV-421-NJR**
APPLE INC.,	
Defendant.	

MEMORANDUM AND ORDER

ROSENSTENGEL, Chief Judge:

Pending before the Court is a Motion to Dismiss filed by Defendant Apple Inc. (Doc. 19). Defendant seeks dismissal of the Complaint for failure to state a claim under Rule 12(b)(6). Alternatively, Defendant moves to dismiss Count II for lack of subject matter jurisdiction under Rule 12(b)(1). For the reasons set forth below, the motion is granted in part and denied in part.

FACTUAL AND PROCEDURAL BACKGROUND

On March 2, 2020, Plaintiffs Roslyn Hazlitt, Jane Doe, a minor, by and through Next Friend John Doe, Richard Robinson, and Yolanda Brown ("Plaintiffs") filed a putative Class Action Complaint against Defendant Apple Inc. ("Apple"), in the Circuit Court for the Twentieth Judicial Circuit in St. Clair County, Illinois. Within the Complaint, Plaintiffs allege violations of Illinois' Biometric Information Privacy Act

(BIPA), 740 ILL. COMP. STAT. § 14/1 *et seq.* (Doc. 1-1). Specifically, Plaintiffs allege Apple violated sections 14/15(a)-(c) of BIPA by collecting, possessing, and profiting from their facial geometries, which qualify as biometric identifiers and biometric information (*Id.* at ¶¶ 1, 3).

A. The Illinois Biometric Information Privacy Act

In 2008, Illinois passed BIPA due to concerns with emerging technology and the increasing collection and use of biometrics in the business and security screening sectors. The Illinois legislature recognized that unlike other personal identifiers, like social security numbers, biometrics are biologically unique to each individual and cannot be altered or changed once compromised. If this data is compromised, due to the sensitive nature of biometrics, an individual is at heightened risk for identity theft and lacks recourse. *See* 740 ILL. COMP. STAT. §§ 14/5(a)-(c). The Illinois legislature observed an overwhelming majority of the public is wary of the use of biometrics when such information is tied to finances and other personal information. While the full ramifications of biometric technology are unknown, BIPA is intended to serve public welfare, security, and safety by regulating the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." *See* 740 ILL. COMP. STAT. §§ 14/5(d)-(g).

BIPA regulates private entities or "any individual, partnership, corporation, limited liability company, association, or other group, however organized." *See* 740 ILL. COMP. STAT. §§ 14/10-20. BIPA requires all private entities in possession of biometric identifiers or biometric information to "develop a written policy, made available to the

public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity." 740 ILL. COMP. STAT. § 14/15(a). Further, private entities are prohibited from collecting, capturing, purchasing, or receiving through trade, or otherwise obtaining a person's biometric identifier or biometric information unless it informs the subject in writing with the specific purpose and length of time disclosed, and receives a written release, *i.e.*, informed written consent. 740 ILL. COMP. STAT. §§ 14/10, 15(b). Moreover, BIPA prohibits private entities from selling, leasing, trading, or otherwise profiting from a person's or customer's biometric identifier or information in their possession. 740 ILL. COMP. STAT. § 14/15(b).

BIPA's definition of "biometric identifier" includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILL. COMP. STAT. § 14/10. BIPA excludes writing samples, written signatures, photographs, human biological samples for valid scientific testing or medical uses, demographic data, tattoo descriptions, and physical descriptions from the definition for "biometric identifier." *Id.* The Act defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* BIPA further narrows the definition by not including "information derived from items or procedures excluded under the definition of biometric identifiers." *Id.*

The Illinois legislature devised BIPA to protect consumers against the threat of

irreparable privacy violations, identity theft, and economic injuries stemming from the use biometric identifiers and biometric information by private entities. Notably, as a matter of state law, BIPA creates a private right of action for "[a]ny person aggrieved by a violation" of the outlined provisions. 740 ILL. COMP. STAT. § 14/20.

B. Plaintiffs' Complaint and Procedural Background

Plaintiffs allege Apple violated sections 14/15(a)-(c) of BIPA by collecting, possessing, and profiting from their facial geometries and associated data, which qualify as biometric identifiers and biometric information (Doc. 1-1 at ¶¶ 1, 3).

Facial recognition or "faceprinting" uses biological characteristics to verify an individual's identity by extracting an individual's face geometry data in order to confirm a subsequent match of the individual's face (*Id.* at ¶ 44). Geometric attributes of faces include distance between the eyes, width of the nose, and other features (*Id.* at ¶ 75). Face geometry is a physiological characteristic and qualifies as a "biometric identifier" under BIPA (*Id.* at ¶ 26).

Plaintiffs allege Apple's Photos app employs a proprietary software and facial recognition technology to scan individual face geometries from a user's photographs creating a unique "faceprint" for every person detected (*Id.* at ¶¶ 2, 27, 67, 77). Apple's devices use facial recognition technology to add frequently detected faces to the user's "People" album within the Photos app (*Id.* at ¶ 67). Further, Apple pre-installs the Photos app on all devices including phones, tablets, and computers, and the app cannot be removed or modified (*Id.* at ¶¶ 2, 64). This feature of the Photos app allegedly enables users to "recognize the people, scenes, and objects in [photographs]" and easily sort or

find images of their "favorite subjects—the people in [their lives]" (*Id.* at ¶¶ 80, 81, 83).

Plaintiffs also allege that the Photos app applies an algorithm to specifically identify the Apple device user, which creates biometric information as defined by BIPA (*Id.* at ¶ 101). Moreover, device users can "tag" and input names for each of the faces detected in the People album (*Id.* at ¶¶ 146, 147). Apple does not store or transfer all user biometric identifiers or biometric information on its servers, but rather, as Plaintiffs allege, on each Apple device locally in a facial recognition database in the solid-state memory on the device (*Id.* at ¶¶ 71, 105, 179).

Plaintiffs allege this conduct presents an imminent threat of serious harm to Plaintiffs and the proposed class, as Apple does not delete the biometric data it collects on the devices, even discarded Apple devices (*Id.* at ¶ 130). Moreover, Plaintiffs cannot prevent their devices from collecting their unique and sensitive biometric data (*Id.* at ¶ 132). And because this information is stored on individual devices, Plaintiffs and the class members face the imminent threat of disclosure of their biometric data as the result of a data breach on any Apple device on which their biometric data is stored (*Id.* at ¶ 133).

Each named Plaintiff is a resident of Illinois (*Id.* at ¶¶ 10-13). According to the Complaint, each named Plaintiff has used an Apple device to take or store photographs of themselves or others using the Photos app (*Id.* at ¶¶ 2, 143). Furthermore, each named Plaintiff had his or her facial geometry scanned from the photographs and their biometric data collected, stored, and used by Apple (*Id.* at ¶ 14). Apple is a California corporation conducting business throughout Illinois (*Id.* at ¶ 15).

Plaintiffs assert three counts of BIPA violations, 740 ILL. COMP. STAT. §§ 14/15(a)-

(c). In Count I, Plaintiffs claim Apple violated BIPA section 14/15(b) by collecting Plaintiffs' and Class Members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, without first notifying Plaintiffs in writing and obtaining informed consent (*Id.* at ¶¶ 162-164). In Count II, Plaintiffs assert Apple violated BIPA section 14/15(a) by possessing biometric identifiers and biometric information without creating and following a written, publicly available policy with retention schedules and destruction guidelines (*Id.* at ¶ 171). In Count III, Plaintiffs allege Apple violated BIPA section 14/15(c) by profiting from biometric identifiers and biometric information it possessed, through marketing and selling its devices based upon claims of photograph sorting technology (*Id.* at ¶¶ 179-181).

Plaintiffs seek to represent a class consisting of all Illinois citizens whose faces appeared in one or more photos taken or stored on their own, or someone else's, Apple device using the Photos app from March 4, 2015, until present (*Id.* at ¶ 153). On behalf of themselves and the putative class, Plaintiffs seek actual damages, statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILL. COMP. STAT. § 14/20(2), statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILL. COMP. STAT. § 14/20(1), an order enjoining Apple from further violating BIPA, attorneys' fees and costs, and pre- and post-judgment interest (*Id.* at ¶ 42).

In the motion before the Court, Apple argues that Plaintiffs have failed to state a claim under BIPA because: (1) the alleged scans of face geometry are derived from photos and not linked to identifiable individuals; (2) facial recognition takes place solely on the device; (3) Plaintiffs lack standing under Article III to pursue the section 15(a) claim in

Count II; (4) Plaintiffs fail to allege that Apple sold or profited from biometric identifiers or biometric information; and (5) Plaintiffs fail to allege any factual support for an intentional or reckless violation of BIPA as necessary to sustain the request for enhanced statutory damages. The Court considers each of these arguments in turn.

SUBJECT MATTER JURISDICTION UNDER CAFA

On May 6, 2020, Apple removed the action from the Twentieth Judicial Circuit in St. Clair County, Illinois, to this Court under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d)(2) (Doc. 1). CAFA authorizes federal jurisdiction over class actions where: (1) any member of the proposed class is a citizen of a state different from any defendant (minimal diversity requirement); (2) the proposed class consists of more than 100 members; and (3) the amount in controversy is $5,000,000 or more, aggregating all claims and exclusive of interest and costs. *See* 28 U.S.C. §§ 1332(d)(2), 1332(d)(5)(B), 1332(d)(6).

Here, minimal diversity of citizenship exists between the parties, as Plaintiffs are residents of Illinois, and Apple is a California corporation (Doc. 1-1 at ¶¶ 10-13, 15). Moreover, the proposed class involves more than the requisite 100 members, as Plaintiffs allege that the putative class includes "thousands of people" (*Id.* at ¶ 154). Finally, the amount in controversy requirement is satisfied. Plaintiffs seek statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILL. COMP. STAT. § 14/20(2) and damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILL. COMP. STAT. § 14/20(1). Plaintiffs allege at least three separate BIPA violations in Count I-III and have asserted there are thousands of Class Members. Even assuming a class size

of only 1,000, and without considering attorneys' fees, the Complaint alleges possible damages of $5,000,000. The amount in controversy meets the required threshold.

The Court will discuss subject matter jurisdiction specifically with regard to Article III standing in detail below.

ANALYSIS

The Court will first address Apple's Article III standing argument raised in opposition to Count II. Additionally, the Court will evaluate Article III standing for Plaintiffs' other two claims *sua sponte*. Finally, the Court will address Apple's remaining arguments for 12(b)(6) dismissal.

I. Article III Standing

Jurisdiction must be established as a threshold matter, due to the nature and limits of federal judicial power. *Steel Co. v. Citizens for a Better Environment*, 532 U.S. 83, 94-95, 118 S.Ct. 1003, 140 L.Ed.2d 210 (1998). Without Article III standing, federal courts have no authority to resolve a case for want of subject matter jurisdiction. *MAO-MSO Recovery II, LLC v. State Farm Mut. Auto. Ins. Co.*, 935 F.3d 573, 581 (7th Cir. 2019); *see also Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547, 194 L.Ed.2d 635 (2016). Article III standing requires: (1) plaintiffs to suffer an actual or imminent, concrete and particularized injury-in-fact; (2) a causal connection between the injury and the conduct complained of; and (3) a likelihood that the injury can be redressed by a favorable decision. *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 620-21 (7th Cir. 2020) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61, 112 S.Ct. 2130, 119 L.Ed.2d 352 (1992)). Bare procedural violations separated from any concrete harm do not satisfy the injury-in-fact requirement. *Spokeo*, 136 S.Ct. at 1549,

194 L.Ed.2d 635 (2016). The violation of a procedural right, conferred by a statute, may sufficiently constitute an injury-in-fact. *Id.* A statutory violation, however, must present "an 'appreciable risk of harm' to the underlying concrete interest [the legislature] sought to protect by enacting the statute." *Bryant,* 958 F.3d at 621 (quoting *Groshek v. Time Warner Cable, Inc.*, 865 F.3d 884, 887 (7th Cir. 2017)).

A. Standing Under Section 15(a) of BIPA

Apple claims that Plaintiffs fail to allege any particularized harm that resulted from Apple's supposed failure to comply with section 15(a) of BIPA. Section 15(a) requires private entities that possess biometric data to develop, publish, and follow a written policy containing a retention schedule and destruction guidelines. Without a particularized harm, Apple avers that the allegations do not satisfy Article III standing (Doc. 20, pp. 14-15).

Typically, the party that has removed a case to federal court, here Apple, has the burden to prove standing. Yet, after removing the case under CAFA, Apple now seeks to dismiss this claim for lack of standing. Despite this unusual positioning, the Court will review this argument, as a federal court must satisfy itself that it has jurisdiction over the claims that appear before it. *Ruhrgas AG v. Marathon Oil Co.,* 526 U.S. 574, 577, 119 S.Ct. 1563, 143 L.Ed.2d 760 (1999).

As cited by Apple, the Seventh Circuit's recent decision in *Bryant v. Compass Group USA, Inc.* informs the discussion on subject matter jurisdiction over Plaintiffs' claims under BIPA section 15(a) (Doc. 20, pp. 14-15). *Bryant,* 958 F.3d at 626. In *Bryant*, the Seventh Circuit resolved an important issue that divided several district courts

concerning which BIPA violations give rise to a particularized and concrete injury for purposes of standing under Article III. *Id.* The *Bryant* court examined standing under sections 15(a) and 15(b) of BIPA. *Id.* at 619-20.

The Seventh Circuit, applying the analysis from Justice Thomas' concurring opinion in *Spokeo*, distinguished between the violation of personal and public rights. *Id.* at 624; *see Spokeo,* 136 S.Ct. at 1550-54, 194 L.Ed.2d 635 (2016). In *Bryant*, the plaintiff used a vending machine, owned and operated by the defendant, that scanned fingerprints to create user accounts for payment purposes. 958 F.3d at 619. The plaintiff asserted claims that the defendant never published a data-retention policy or guidelines for destroying biometric information, violating section 15(a), and that the defendant never obtained written consent in the collection of her fingerprints, violating 15(b). *Id.*

In *Bryant*, the Seventh Circuit only evaluated a claim under the provision of section 15(a) requiring development of a publicly available written policy establishing a retention schedule and destruction guidelines. *Id.* at 626. Under this theory, the court held that the plaintiff did not sufficiently allege a concrete, particularized injury-in-fact resulting from the defendant's failure to develop such a written policy. *Id.* The *Bryant* court found the duties conferred in this provision of section 15(a) are owed to the public generally, not to private individuals. *Id*.

This is not to say that a plaintiff never has standing under section 15(a), just that a particularized harm stemming from a public duty must be sufficiently alleged. *Id.* at 622; *see Miller v. Southwest Airlines Co.,* 926 F.3d 898, 902-03 (7th Cir. 2019) (union airline workers sufficiently alleged a concrete injury-in-fact under section 15(a) when they faced

a potential material change in the terms and conditions of their employment with regards to clocking in with a fingerprint scanner). Because obligations imposed by section 15(a) are directed at the public as opposed to the individual, Article III standing under this provision "seems to hinge more on the relationship of the parties." *Stauffer v. Innovative Heights Fairview Heights, LLC*, ---F.Supp.3d at ---, 2020 WL 4815960 *6 (S.D. Ill. Aug. 19, 2020).

It appears the Seventh Circuit left open the possibility of Article III standing when a plaintiff does allege a particularized harm even when the duties imposed by a statute, as in section 15(a), are generally duties to the public. Importantly, the *Bryant* court only assessed a claim under the provision requiring development of a written policy with a retention schedule and destruction guidelines, not under the provision mandating compliance with the retention schedule and destruction guidelines. 958 F.3d at 626.

As in *Bryant,* Apple's purported failure to publicize a retention and destruction policy in violation of BIPA section 15(a) constitutes a public harm, not a harm particular to Plaintiffs. This violation, as *Bryant* illuminates, does not create the type of concrete, particularized injury necessary to satisfy Article III's requirements. Therefore, the Court finds Plaintiffs lack standing to bring this claim in federal court. As a result, Plaintiffs' claims under BIPA section 15(a) shall be remanded to the Circuit Court of St. Clair County. *See Bergquist v. Mann Bracken, LLP*, 592 F.3d 816, 819 (7th Cir. 2010) ("If some parts of a single suit are within federal jurisdiction, while others are not, then the federal court must resolve the elements within federal jurisdiction and remand the rest.").

Unlike *Bryant*, however, Plaintiffs also allege Apple's failure to *destroy* biometric

information, in violation of section 15(a), caused harm. Section 15(a) requires destruction of biometric data when "the initial purpose for collecting or obtaining such [data] has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILL. COMP. STAT. § 14/15(a).

After the Seventh Circuit decided *Bryant,* the Northern District of Illinois evaluated Article III standing in *Cothron v. White Castle.* In *Cothron,* the court hypothesized that the second part of section 15(a) requiring permanent destruction of biometric data, when the initial purpose has been satisfied or within three years of the individual's last interaction with the private entity, could potentially create an individualized right; however, the court did not ultimately address that possibility because the plaintiff still worked for the entity collecting her biometric data. *See Cothron v. White Castle,* ---F.Supp.3d ---, 2020 WL 32505706 at *3 (N.D. Ill. 2020).

In their Complaint, Plaintiffs allege Apple violated their right to have their personal data deleted, which makes Plaintiffs' personal data vulnerable to hacking or other means of extraction (Doc. 1-1 at ¶¶ 110, 130, 133-38, 171, 174). Similar to *Cothron*, however, Plaintiffs do not allege that they have ceased use of the application or device collecting the biometric data. Thus, the initial purpose for collecting the data has not been satisfied, nor have three years passed since Plaintiffs last interacted with Apple or its devices. As such, Plaintiffs fail to describe a violation of the destruction requirements in section 15(a).

B. Standing Under Section 15(b) of BIPA

Continuing the Article III standing analysis, the Court undertakes an analysis of

whether it has subject matter jurisdiction over Plaintiffs' claims under section 15(b).

In *Bryant*, unlike the claims asserted under section 15(a), the Seventh Circuit found that the plaintiff asserted a concrete, particularized injury, as required to satisfy Article III's requirements with respect to her claim under section 15(b). *Id.* at 626. The Seventh Circuit also found that the obligations conferred in section 15(b) are owed to private individuals. *Id.* at 624-26. The court reasoned that, by failing to obtain written consent, the defendant "inflicted the concrete injury BIPA intended to protect against, *i.e.* a consumer's loss of the power and ability to make informed decisions about the collection, storage, and use of her biometric information." *Id.* at 627. Moreover, the court noted that a failure to adhere to the informed consent provision caused a concrete injury because the associated information was "substantive and personal" and may change a person's actions with regard to how he or she uses the device. *Id.* at 626.

Bryant sets out the analysis for Plaintiffs' claims under section 15(b). Section 15(b) requires private entities to make specific disclosures and receive written informed consent from consumers before collecting or capturing their biometric information. 740 ILL. COMP. STAT. § 14/15(b). And Plaintiffs allege that Apple never requested or received informed consent before collecting face geometries from their photos within the Photos app. Apple's purported violation of section 15(b) would create a concrete, particularized injury to Plaintiffs, as their power to make informed decisions about the collection and storage of their biometric data has been eroded. Accordingly, Plaintiffs have Article III standing for their claims under section 15(b).

C. Standing Under Section 15(c) of BIPA

While the Seventh Circuit has not addressed Article III standing for BIPA claims arising under section 15(c), the analysis directly follows the *Bryant* court's approach to claims under section 15(a).

Article III standing requires allegations of a particularized and concrete harm. *Bryant,* 958 F.3d at 624. A concrete injury does not necessarily mean a tangible harm. *Id.* The *Spokeo* Court further clarified that for a plaintiff's injury to be particularized, the plaintiff must be affected in a personal and individual way. 136 S. Ct. at 1548. And, for a plaintiff's injury to be concrete, the injury must be "de facto" and actually exist. *Id.*

Section 15(c) prohibits entities in possession of a person's or customer's biometric identifiers or information from selling, leasing, trading, or otherwise profiting from that data. 740 ILL. COMP. STAT. § 14/15(c). Here, Plaintiffs allege that Apple violated section 15(c) by marketing and selling its devices based upon claims that its facial recognition technology could sort photographs, thus profiting from a person's or customer's biometric data (Doc. 1-1 at ¶ 181). Importantly, Plaintiffs do not allege that Apple sold or otherwise profited from their *individual* biometric data. Plaintiffs seem to generally allege that Apple profited from sales of its devices which include a facial recognition feature within the pre-installed Photos app.

Plaintiffs' allegations are devoid of any particularized or concrete injury. Plaintiffs do not, nor could they, claim to be personally or individually affected by Apple selling devices based on the facial recognition technology in its Photos app. Moreover, by its plain language, section 15(c) clearly prohibits profiting from "a person's or a customer's"

biometric identifier or biometric information, not the general sales of devices equipped with facial recognition technology. Notably, even if BIPA sought to prohibit marketing campaigns or sales based on facial recognition technology, that prohibition would protect a right generally conveyed to the public, not an individual right, much like the public retention and destruction policy required through section 15(a).

Under the Supreme Court's guidance in *Spokeo,* as used by the Seventh Circuit in *Bryant*, Plaintiffs' claim under section 15(c) does not satisfy the requirements of Article III standing. Plaintiffs have failed to demonstrate a concrete and particularized injury-in-fact resulting from Apple's purported violation of section 15(c) of BIPA. Thus, this claim also will be remanded to the Circuit Court of St. Clair County.

II. Motion to Dismiss under 12(b)(6)

Because the remaining claim under BIPA section 15(b) is within the Court's jurisdiction, the Court now turns to Apple's remaining arguments in its motion to dismiss.

The purpose of a motion to dismiss under Rule 12(b)(6) is to evaluate the adequacy of a complaint, not to determine the merits of the case or decide whether a plaintiff will ultimately prevail. *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). To survive a Rule 12(b)(6) motion, the plaintiff only needs to allege enough facts to state a claim for relief that is plausible on its face. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A plaintiff need not plead detailed factual allegations, but must provide "more than labels and conclusions, and a formulaic recitation of the elements." *Id.* In deciding a motion to dismiss under Rule 12(b)(6), the Court accepts as true all well-pleaded facts in

the complaint and draws all reasonable inferences in the plaintiff's favor. *Burke v. 401 N. Wabash Venture, LLC,* 714 F.3d 501, 504 (7th Cir. 2013). Taken together, the factual allegations contained within a complaint must "raise a right to relief above the speculative level, on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." *Twombly,* 550 U.S. at 555 (internal citations omitted).

A. Biometric Identifiers and Biometric Information

Apple argues that Plaintiffs fail to allege that Apple, the device, or the Photos app links the alleged scans of face geometry from photos to identifiable individuals (Doc. 20, p. 1). In Apple's view, the purported facial templates do not qualify as biometric identifiers as defined by BIPA because they are anonymous and do not actually identify any individual (*Id.* at 7). According to Apple, the Illinois legislature chose to attach the word "identifier" to the word biometric to intentionally exclude data that does not identify an actual person (*Id.*). Apple further reasons that device users have a choice to "tag" and assign names to the albums within the People folder by inputting a name themselves and that Apple does not receive this information, even if it is personally identifying (*Id.* at 1).[1]

BIPA exhaustively defines what is a biometric identifier, along with providing

[1] Apple distinguishes several BIPA cases relied on by Plaintiffs. Apple distinguishes *Rivera v. Google, Inc.* by emphasizing the fact that Google Photos created a set of biology-based measurements that were *used to identify a person*. (Doc. 20, p. 10). Further, Apple distinguishes *Monroy v. Shutterfly* because Shutterfly operates a database that stores individual names to suggest for people in users' photographs, and only if no match is found, the user is prompted to enter a name. Apple argues *Norberg v. Shutterfly, Inc.* is also not comparable, as Norberg alleged Shutterfly used his personal face pattern to recognize and identify him in photographs posted to the photo sharing website. Apple separates this case from *In re Facebook Biometric Info. Privacy Litig.*, because Facebook suggests an individual's name to automatically tag them, and the program puts names on the faces in the photos (*Id.*).

examples of what is not a biometric identifier, as follows:

> "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

740 ILL. COMP. STAT. § 14/10. Even though photographs are explicitly excluded from the definition of biometric identifier, several courts have determined that scans of photographs for facial geometry do qualify under the definition of biometric identifier. *See Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017); *In re Facebook Biometric Information Privacy Litigation*, 185 F.Supp.3d 1155 (N.D. Cal. 2016); *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846 (N.D. Ill. 2017).

Apple argues, however, that these facial scans cannot qualify as biometric identifiers because Apple does not use the scans to actually identify a person (Doc. 20, p. 10). First, the Court is not convinced of Apple's proposed reading of the statutory language regarding biometric identifiers. The definition of biometric identifier explicitly includes scans of face geometry, which Plaintiffs allege Apple collected without consent

(Doc. 1-1 at ¶ 27). Apple reads the word "identifier" to exclude data that does not identify an actual person (Doc. 20, p. 7). This Court finds that interpretation too narrow. Each specific item on the list fits within the meaning of the term "biometric identifier." The word "identifier" modifies the word "biometric" to signal that the types of data listed *could* be used to identify a person. *See Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017) (interpreting "biometric identifier" to mean a biology-based set of measurements that can be used to identify a person). This reading is supported by the legislative intent finding for BIPA, which reads "Biometrics are unlike other unique identifiers that are used to access . . . sensitive information. For example, social security numbers, when compromised, can be changed." *See* 740 ILL. COMP. STAT. § 14/5(c). This language suggests that "biometrics" are a type of "identifier" different from other identifiers like social security numbers. Second, even if Apple's proposed reading is correct, within the Complaint, Plaintiffs allege that the Photos app applies an algorithm to identify the device user (Doc. 1-1 at ¶ 101). Taken as true, at this stage, Plaintiffs sufficiently allege that the face scans qualify as biometric identifiers.

Further, Apple argues BIPA's definition of biometric information expressly excludes information derived from photographs. Apple cites to language in *Monroy v. Shutterfly, Inc.*, stating that "[i]t is clear that the data extracted from Monroy's photograph cannot constitute 'biometric information' within the meaning of the statute . . . " 2017 WL 4099846 * 3 (N.D. Ill. 2017); (Doc. 20, p. 7). Notably, only one district court has concluded that facial scans from photographs are emphatically excluded within the definition of biometric information. However, as BIPA section 15(b) covers the collection, capturing,

purchasing, receiving, or obtaining of "biometric identifiers *or* biometric information," it is unnecessary at this stage to decide whether the facial scans qualify as biometric information, as this Court has already found that the facial scans qualify as biometric identifiers. 740 ILL. COMP. STAT. § 14/10 (emphasis added). Plaintiffs need only sufficiently allege that Apple collected one or the other to state a plausible claim for relief under section 15(b), and they have done so.

B. Collection and Possession of Biometric Data

Apple next argues that Plaintiffs fail to allege that Apple—as the manufacturer of Plaintiffs' devices or licensor of software—ever actually collects, captures, possesses, or otherwise obtains any of the information at issue (Doc. 20, pp. 10-11). Apple considers Plaintiffs' allegation that Apple "possesses the Biometric Data" collected through the Photos app and stored locally on users' device to be speculative and conclusory (*Id.* at 11). Further, Apple argues only Plaintiffs own and control the devices and physical media that run the processes and generate the alleged scans of face geometry, and users choose to take and store photographs (*Id.* at 12). Apple also asserts the Complaint lacks allegations that Apple reserves the right to access a user's photos or associated information (*Id.*). Apple disputes Plaintiffs' theory that Apple is vicariously liable for the actions of the Photos app, as Apple's "software agent" (*Id.*).

Plaintiffs allege that Apple both "collected" and "possessed" their biometric data using proprietary software that Apple owned, exclusively controlled, and barred individual users from accessing, removing, or disabling (Doc. 1-1 at ¶¶ 75-79, 105-10). More specifically, Plaintiffs allege that Apple used its software to create, gather, and

harvest faceprints, which Apple stored in facial recognition databases that Apple provided users no knowledge of, or control over, and Apple alone could access the biometric data or disable its collection (*Id.* at ¶¶ 32, 65-104). Plaintiffs assert that Apple is subject to BIPA liability from its collection and possession of Plaintiffs' biometric data based on common law agency principles (*Id.* at ¶¶ 101-04). In furtherance of this theory, Plaintiffs allege that Apple's software cannot be used as intended without biometric data automatically being collected, that device users had no ability to disable the collection (or notice of collection), and Apple prevents users from accessing, disabling, or altering the software (*Id.* at ¶¶ 85-87, 89-91, 142-52).

Both parties correctly recognize that BIPA applies only to those entities "in possession" of or who "collect, capture, purchase, receive through trade, or otherwise obtain," biometric identifiers and biometric information (Doc. 20, p. 10); 740 ILL. COMP. STAT. § 14/15. Apple urges the Court to adopt the definition of "collect" as "to gain or regain control of" (Doc. 20, p. 11). Plaintiffs urge the Court to interpret the word "collect" to mean "bring[ing] together [biometric data] into one body or place," and the term "possess" to mean "taking [those data] into control." (Doc. 24, p. 11).

Under either definition, at this stage—taking all allegations as true and making all inferences in favor of Plaintiffs—the Court finds that Plaintiffs state a plausible cause of action to survive Apple's 12(b)(6) motion to dismiss. Apple argues that many BIPA claims against equipment manufacturers and vendors have been dismissed due to failure to allege the manufacturer collected or used the biometric data in violation of BIPA (Doc. 20, p. 14). *See Heard v. Becton, Dickinson & Co.*, 440 F.Supp.3d 960, 965-66 (N.D. Ill. 2020); *Kloss*

v. Acuant, Inc., 2020 WL 2571901, at *3 (N.D. Ill. May 21, 2020); *Namuwonge v. Kronos, Inc.*, 418 F.Supp.3d 279, 286 (N.D. Ill. 2019); *Bernal v. ADP, LLC*, 2019 WL 5028609, at *1-2 (Ill. Cir. Ct. Aug. 23, 2019). The cases Apple cites are distinguishable here. In those cases, the relationship between the plaintiff and the manufacturer was a third-party relationship—the manufacturers sold machines to employers or businesses who then had employees or customers use the devices, ultimately collecting their biometric data. In those cases, the intervening employer or business possessed and collected the biometric data, not the manufacturer of the device. Here, Apple's relationship with the Plaintiffs is more direct. Apple sells devices directly to customers and, if what Plaintiffs allege is true, collects the biometric data into a facial recognition database on the device that Apple alone can access.

Again, taking their allegations as true, Plaintiffs plausibly allege that Apple collected or possessed their data through the Photos app on their Apple devices, and that Apple alone can access the data stored within an internal database on their devices. Apple's further discussion disputing Plaintiffs' underlying theories of liability attempts to examine the merits of Plaintiffs' case, which is inappropriate at this stage absent further discovery. As the facts develop, it may be that Apple cannot access any data stored on the device via its software or otherwise. Other fact issues can inform the application of BIPA, but the Court does not reach those issues yet. The Court accepts as true Plaintiffs' allegations that Apple collected, possessed, and exercised exclusive control over the biometric data extracted from Plaintiffs' photos within the Photos app, and that Apple did not obtain Plaintiffs' consent in doing so.

C. Intentional or Reckless Violations of BIPA

Apple next argues that because Plaintiffs seek heightened statutory damages under BIPA, they must allege scienter supporting recovery for intentional and reckless conduct and have failed to do so (Doc. 20, p. 16). This argument has been raised in many BIPA cases. Section 20 of BIPA allows recovery for each violation:

> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) other relief, including an injunction, as the State or federal court may deem appropriate.

740 ILL. COMP. STAT. § 14/20. Several courts have held that mental states need not be alleged for the purpose of stating a plausible claim under BIPA to survive a motion to dismiss. *See Stauffer v. Innovative Heights Fairview Heights, LLC.*, ---F.Supp.3d at ---, 2020 WL 4815960 * 13-14 (S.D. Ill. 2020) (finding that mental state standards come into play when determining remedies, not at the pleading stage); *Cothron v. White Castle System, Inc.*, ---F.Supp.3d at ---, 2020 WL 3250706 * 5 (N.D. Ill. 2020) (finding that overcoming a Rule 12(b)(6) motion does not require the plaintiff to plead facts that will determine the amount of actual damages possible to recover); *Peatry v. Bimbo Bakeries USA, Inc.*, 2020 WL 919202 * 6 (N.D. Ill. 2020) (finding that Rule 8 does not require a plaintiff to plead damages with particularity but only requires a demand for relief sought); *Neals v. PAR Technology Corp.*, 419 F.Supp.3d 1088, 1092 (N.D. Ill. 2019) (finding that under Rule 9(b), states of mind may be alleged generally, and Rule 8 does not demand that a plaintiff plead facts he or she would have no way of knowing prior to discovery). These courts

have found that mental states go only to the damages recoverable for a given claim and can be proven later, but per the relevant pleading requirements plaintiffs may allege states of mind generally.

Further, allegations that a defendant has made no effort to comply with BIPA's requirements, even though BIPA has been in effect for over ten years, are enough, at the pleading stage, to make claims of negligence or recklessness plausible. *Rogers v. BNSF Railway Co.*, 2019 WL 5635180 * 5 (N.D. Ill. 2019). *But see Namuwonge v. Kronos, Inc.*, 418 F.Supp.3d 279, 286 (N.D. Ill. 2019) (dismissing the claim for damages based on intentional and reckless conduct because allegations were only sufficient to plausibly infer negligent conduct); *Rogers v. CSX Intermodal Terminals, Inc.*, 409 F.Supp.3d 612, 618-19 (N.D. Ill. 2019).

Plaintiffs allege that Apple continues to collect faceprints from Illinois residents in violation of BIPA more than eleven years after BIPA's enactment (Doc. 1-1 at ¶¶ 21, 104). These allegations are sufficient to create an inference that the conduct was either negligent or reckless. As other courts have established, the states of mind with regard to BIPA only relate to possible recovery for each violation, which is not yet before the Court. Accordingly, Plaintiffs have sufficiently pled facts to state a cause of action under BIPA section 15(b).

CONCLUSION

For these reasons, the Motion to Dismiss (Doc. 19) filed by Defendant Apple Inc. is **GRANTED in part and DENIED in part**. Plaintiffs' claims in Count II and III under BIPA sections 15(a) and (c) are **REMANDED** to the Twentieth Judicial Circuit, St. Clair

County, Illinois, for lack of subject matter jurisdiction. Defendant Apple Inc.'s motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) as to Count I is **DENIED.**

IT IS SO ORDERED.

DATED: November 12, 2020

NANCY J. ROSENSTENGEL
Chief U.S. District Judge