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, known and unknown, Plaintiffs, v. **APPLE INC.**, Defendant.	Case No. 3:20-cv-421

APPLE INC.'S NOTICE OF REMOVAL

PLEASE TAKE NOTICE that Apple Inc. ("Apple") hereby removes this action, originally filed as case number 20 L 206 in the Circuit Court for the Twentieth Judicial Circuit, St. Clair County, Illinois, to the United States District Court for the Southern District of Illinois under 28 U.S.C. §§ 1332, 1441, 1446, and 1453. In support of removal, Apple states:

I. PRELIMINARY STATEMENT

1. The plaintiffs filed this action in the St. Clair County court on March 12, 2020, seeking to assert claims on behalf of themselves and a putative class under the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*

2. Copies of all process, pleadings, and orders served upon Apple in this matter are attached as Exhibits 1 to 3. *See* 28 U.S.C. § 1446(a).

3. The plaintiffs served Apple with the summons and Complaint on April 7, 2020. *See* Ex. 2. Apple is timely filing this notice within 30 days of service. *See* 28 U.S.C. § 1446(b).

4. Removal to this Court is proper because it is the U.S. district court for the district and division embracing the Circuit Court in St. Clair County, Illinois. 28 U.S.C. § 93(c).

5. As set forth in greater detail below, the Court has diversity jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §§ 1332(d), 1453, and 1711-1715, because minimal diversity exists and the amount in controversy exceeds $5,000,000.[1]

II. BACKGROUND

6. Each plaintiff alleges that he or she is a resident of the State of Illinois. Ex. 1 ¶¶ 10-13. The plaintiffs acknowledge that Apple is a California corporation. *Id.* ¶ 15.

7. The Complaint alleges that Apple "violated BIPA by collecting, possessing, and profiting from the biometric identifiers and biometric information of Illinois citizens"—specifically, scans of face geometry—via the "Photos software application ('Photos App')" on "[Apple's] phones, tablets, and computers (the 'Apple Devices')." *Id.* ¶¶ 1-2. The devices allegedly "automatically collect[]" scans of face geometry from photographs "without the knowledge or informed written consent of" the user or others who may appear in the photographs. *Id.* ¶ 2. Although the Photos app uses on-device processing (and thus ***Apple*** does not collect or possess the putative biometric information as required to apply BIPA), *see, e.g.*, *id.* ¶ 105, the plaintiffs claim Apple is "directly and vicariously" liable because it provides the Photos app, *id.* ¶ 141.

8. The plaintiffs "seek to represent [classes] of individuals whose face geometries were collected, stored, and/or used by [Apple]," *id.* ¶ 6, defined as follows:

- All Illinois citizens whose faces appeared in one or more photographs taken or stored on their own Apple Devices running the Photos App from March 4, 2015 until present.

[1] By filing this notice, Apple does not concede any allegation, assertion, claim, or demand for relief in the Complaint, or that any damages exist. Apple expressly denies that it has violated BIPA, intends to defend this matter vigorously on the merits and as to class certification, and reserves all defenses and objections to the plaintiffs' allegations, assertions, claims, demands for relief, and supposed damages.

- All Illinois citizens whose faces appeared in one or more photographs taken or stored on an Apple Device other than their own running the Photos App from March 4, 2015 until present.

Id. ¶ 153. The classes allegedly include "thousands of people." *Id.* ¶ 154.

9. In the Prayer for Relief, the Complaint requests: (1) injunctive relief, (2) "actual damages," (3) "statutory damages of $5,000 for each intentional and reckless violation of BIPA," (4) statutory damages "of $1,000 for each negligent violation" of BIPA, and (5) "attorneys' fees, costs, and other litigation expenses." *Id.* at 42.

III. REMOVAL IS PROPER UNDER CAFA

10. As amended by CAFA, 28 U.S.C. § 1332(d) grants U.S. district courts original jurisdiction over "any civil action" in which: (a) the aggregate number of members in the proposed class is 100 or more; (b) the "matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs"; and (c) "any member of a class of plaintiffs is a citizen of a State different from any defendant." 28 U.S.C. § 1332(d)(2), (d)(5)(B).

11. **This is a "class action" under CAFA**. Because the plaintiffs invoke procedures "authorizing an action to be brought by 1 or more representative persons as a class action," this matter qualifies as a "class action" for purposes of CAFA. 28 U.S.C. § 1332(d)(1)(B).

12. **The putative class contains at least 100 members**. Under controlling precedent, Apple "may rely on the estimate of the class number set forth in the complaint." *Sabrina Roppo v. Travelers Commercial Ins. Co.*, 869 F.3d 568, 581 (7th Cir. 2017). Here, the plaintiffs allege that the putative class numbers in the "thousands." Ex. 1 ¶ 154.

13. **The amount placed in controversy exceeds $5,000,000**. The amount in controversy under CAFA is determined by aggregating "the claims of the individual class members." 28 U.S.C. § 1332(d)(6). The burden for removing under CAFA is low and requires only "a reasonable probability that the ***stakes*** exceed the minimum." *Brill v. Countrywide Home*

Loans, Inc., 427 F.3d 446, 448 (7th Cir. 2005) (emphasis added); *see also Blomberg v. Serv. Corp. Int'l*, 639 F.3d 761, 763 (7th Cir. 2011) (plausible, good-faith estimate). Apple need not "confess liability" or offer "proof" of damages, since it may rely on "***what the plaintiff is claiming***." *Spivey v. Vertrue, Inc.*, 528 F.3d 982, 986 (7th Cir. 2008) (emphasis added). Here, Apple denies that actual damages to the plaintiffs, if any, are quantifiable; that statutory damages may be awarded; and that certification of a class is appropriate. However, solely for the purposes of removal, the amount in controversy is determined by what the plaintiffs are claiming is at stake, that is: up to $5,000 in statutory damages per supposed violation of BIPA for allegedly "thousands" of putative class members. Ex. 1 at 42 and ¶ 154. Accordingly, the plaintiffs have put an amount in excess of $5,000,000 in controversy.

14. **Diversity is undisputed**. The plaintiffs, all of whom allegedly reside in Illinois, and Apple, a California corporation, satisfy the minimal diversity requirements under 28 U.S.C. § 1332(d)(2)(A). *See e.g.*, *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965–66 (7th Cir. 2016) (holding that diversity existed where Illinois class representatives sued a Delaware corporation with its principal place of business in Arizona).

15. Attached as Exhibit 4 hereto is a copy of the notice required under 28 U.S.C. § 1446(d), which Apple promptly will provide to the plaintiffs and file with the Clerk of the Circuit Court for the Twentieth Judicial Circuit, St. Clair County, Illinois.

IV. CONCLUSION

Apple therefore removes this action from the Circuit Court for the Twentieth Judicial Circuit, St. Clair County, Illinois, and respectfully requests that the action proceed in this Court as a matter properly removed.

Dated: May 6, 2020

Respectfully Submitted,

Apple Inc.

By: /s/ *Raj Shah*
One of its attorneys

Raj N. Shah (ARDC # 06244821)
Eric M. Roberts (ARDC # 6306839)
DLA Piper LLP (US)
444 West Lake Street, Suite 900
Chicago, Illinois 60606
312.368.4000
raj.shah@dlapiper.com
eric.roberts@dlapiper.com

Isabelle L. Ord*
DLA Piper LLP (US)
555 Mission Street, Suite 2400
San Francisco, California 94105
isabelle.ord@dlapiper.com

Amanda Fitzsimmons*
DLA Piper LLP (US)
401 B. Street, Suite 1700
San Diego, California 92101
amanda.fitzsimmons@dlapiper.com

* motion to appear *pro hac vice* forthcoming

Certificate of Service

I hereby certify that on May 6, 2020, I electronically filed the foregoing **Notice of Filing of Notice of Removal** with the Clerk of the Court using the CM/ECF system. I further certify that I caused a true and correct copy of the foregoing by electronic mail and U.S. Postal Mail delivery upon the following counsel of record:

Jerome J. Schlichter (jschlichter@uselaws.com)
Andrew D. Schlichter (aschlichter@uselaws.com)
Alexander L. Braitberg (abraitberg@uselaws.com)
Brett C. Rismiller (brismiller@uselaws.com)
Schlichter, Bogard & Denton LLP
100 South Fourth Street, Suite 1200
St. Louis, Missouri 63102

Christian G. Montroy (cmontroy@montroylaw.com)
2416 North Center
P.O. Box 369
Maryville, Illinois 62062

Attorneys for the plaintiffs

/s/ *Raj Shah*

Raj N. Shah (ARDC # 06244821)
DLA Piper LLP (US)
444 West Lake Street, Suite 900
Chicago, Illinois 60606
312.368.4000
raj.shah@dlapiper.com

Exhibit 1

IN THE CIRCUIT COURT
TWENTIETH JUDICIAL CIRCUIT
ST. CLAIR COUNTY, 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, known and unknown, Plaintiffs, v. APPLE INC., Defendant.	Case No.: 20L0206 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Roslyn Hazlitt, Jane Doe, a minor, by and through next friend John Doe, Richard Robinson, and Yolanda Brown ("Plaintiffs"), individually and on behalf of all other persons similarly situated, bring this class action lawsuit for violations of the Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA"), against Defendant Apple Inc. ("Defendant"). Plaintiffs allege the following facts based upon personal knowledge, investigation by retained counsel, and on information and belief.

1. Plaintiffs allege that Defendant violated BIPA by collecting, possessing, and profiting from the biometric identifiers and biometric information (collectively, "Biometric Data") of Illinois citizens via Defendant's Photos software application ("Photos App"). For the reasons discussed in greater detail below, Defendant's violations of BIPA pose a serious threat of permanent harm to Illinois citizens.

2. Defendant's Photos App comes pre-installed on Defendant's phones, tablets, and computers ("Apple Devices"). The Photos App, which cannot be removed or modified, automatically collects face Biometric Data from Apple Device users' photographs. Defendant's Photos App collects Biometric Data without the knowledge or informed written consent of the Apple Device users or Apple Device nonusers—including minors—who appear in photographs on Apple Devices. Users of Apple Devices are not told by Defendant that it is collecting face Biometric Data, and cannot disable Defendant's collection of face Biometric Data.

3. Defendant's conduct violates BIPA in three ways:

First, Defendant violates Section 15(b) by collecting the Biometric Data of Plaintiffs and other Illinois citizens. As described in greater detail below, Defendant collects Biometric Data of Plaintiffs and other Illinois citizens by collecting the face geometries of persons who appear in photographs on an Apple Device, and storing those face geometries in a database on the Apple Device.

Second, Defendant violates Section 15(a) by possessing the Biometric Data of Plaintiffs and other Illinois Citizens. As is likewise described below, Defendant possesses Biometric Data by exercising exclusive control over the face Biometric Data of Plaintiffs and other Illinois citizens, and by prohibiting Apple Device users and nonusers from accessing, modifying, or removing their face Biometric Data.

Third, Defendant violates BIPA Section 15(c) by profiting from the Biometric Data it collects and possesses. Defendant profits from the face Biometric Data of Apple device users and nonusers because it uses the facial recognition capabilities of its Photos App, which violate BIPA, to market and sell its devices and software.

4. Through this lawsuit, Plaintiffs, on behalf of a similarly situated class, seek to enjoin Apple from collecting, possessing, and profiting from their Biometric Data in violation of BIPA, and seek to obtain actual and statutory damages for their injuries.

I. Nature of the Action

5. Plaintiffs allege that Defendant violated BIPA by collecting their biometric identifiers and biometric information.

6. Plaintiffs seek to represent a class of individuals whose face geometries were collected, stored, and/or used by Defendant, including through the use of Defendant's Photos App.

7. Plaintiffs have suffered significant damage, as more fully described herein, because Defendant has collected their Biometric Data without their knowledge, consent, or understanding, thereby materially decreasing the security of this intrinsically inalterable information, and substantially increasing the likelihood that Plaintiffs will suffer as victims of fraud and/or identity theft.

8. Plaintiffs seek actual damages in addition to statutory damages, as provided below in the Prayer for Relief.

9. The remedies Plaintiffs seek are remedial, and not penal, in nature.

II. Parties

10. Plaintiff Roslyn Hazlitt is a resident of Belleville in St. Clair County, Illinois.

11. Plaintiff Jane Doe, a minor, is a resident of O'Fallon in St. Clair County, Illinois. John Doe, Jane Doe's next friend, is also a resident of O'Fallon in St. Clair County, Illinois.

12. Plaintiff Richard Robinson is a resident of Troy in Madison County, Illinois.

13. Plaintiff Yolanda Brown is a resident of Godfrey in Madison County, Illinois.

14. Plaintiffs' face geometries have been scanned by Defendant, and their Biometric Data were collected, stored, and used by Defendant, as more fully described herein.

15. Defendant is a California corporation that is registered to and does conduct business throughout Illinois and in St. Clair County.

16. Defendant is a "private entity" under the meaning of BIPA. 740 ILCS 14/10.

III. Jurisdiction and Venue

17. This Court has personal jurisdiction over Defendant because, during the relevant time period, Defendant was registered to do business in Illinois, conducted business in Illinois, committed the violations alleged in Illinois, and purposefully availed itself of the laws of Illinois for the specific transactions and occurrences at issue.

18. St. Clair County is an appropriate venue for this litigation because Defendant does business in St. Clair County, and is therefore a resident of St. Clair County. 735 ILCS 5/2-102.

19. In addition, the transactions and occurrences out of which the causes of action pleaded herein arose or occurred, in part, in St. Clair County.

IV. The Biometric Information Privacy Act

20. "Biometrics" refers to "biology-based set[s] of measurements." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017). Specifically, "biometrics" are "a set of measurements of a specified physical component (eye, finger, voice, hand, face)." *Id.* at 1296.

21. BIPA was enacted in 2008 in order to safeguard Biometric Data due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA is codified as Act 14 in Chapter 740 of the Illinois Compiled Statutes.

22. As set forth in BIPA, biologically unique identifiers, such as scans of individuals' facial geometry, cannot be changed. 740 ILCS 14/5(c). As is likewise explained in BIPA, the inalterable nature of individuals' biologically unique identifiers presents a materially heightened risk of serious harm when Biometric Data is not protected in a secure and transparent fashion. 740 ILCS 14/5(d)–(g).

23. As a result of the need for enhanced protection of Biometric Data, BIPA imposes various requirements on private entities that collect or possess individuals' biometric identifiers, including scans of individuals' facial geometries.

24. Among other things, BIPA regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g).

25. BIPA applies to entities that interact with two forms of Biometric Data: biometric "identifiers" and biometric "information." 740 ILCS 14/15(a)–(e).

26. "Biometric identifiers" are physiological, as opposed to behavioral, characteristics. Examples include, but are not limited to, face geometry, fingerprints, voiceprints, DNA, palmprints, hand geometry, iris patterns, and retina patterns. As the Illinois General Assembly has explained:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

740 ILCS 14/5(c). Moreover,

> A person cannot obtain new DNA or new fingerprints or new eyeballs for iris recognition, at least not easily or not at this time. Replacing a biometric identifier is not like replacing a lost key or a misplaced identification card or a stolen access code. The Act's goal is to prevent irretrievable harm from happening and to put in place a process and rules to reassure an otherwise skittish public.

Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 59, 115 N.E.3d 1080, 1093, *appeal denied*, 119 N.E.3d 1034 (Ill. 2019).

27. In BIPA's text, the General Assembly provided a non-exclusive list of protected "biometric identifiers," including "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. In this case, the biometric identifiers at issue are the scans of face geometries of individuals, including Plaintiffs, collected by Defendant via its proprietary software without any notice to or consent from the individuals whose biometric identifiers are collected.

28. "Biometric information" consists of biometric identifiers used to identify a specific person. BIPA 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.*[1] (emphasis added).

29. In BIPA, the General Assembly identified four distinct activities that may subject private entities to liability:

(1) collecting Biometric Data, 740 ILCS 14/15(b);

(2) possessing Biometric Data, 740 ILCS 14/15(a);

(3) profiting from Biometric Data, 740 ILCS 14/15(c); and

(4) disclosing Biometric Data, 740 ILCS 14/15(d).

BIPA also created a heightened standard of care for the protection of Biometric Data. 740 ILCS 14/15(e).

[1] As set forth below, in this case the biometric identifiers at issue are the facial geometries of individuals, including Plaintiffs, collected by Defendant. These biometric identifiers become biometric information when Defendant's facial recognition algorithms identify individuals based on biometric identifiers.

30. As the Illinois Supreme Court has held, BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 (Ill. 2019). The Illinois Supreme Court further held that when a private entity fails to comply with BIPA "that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." *Id.*

A. Collecting Biometric Data Under Section 15(b)

31. BIPA establishes categories of prohibited conduct related to Biometric Data, and establishes requirements that parties must follow when interacting with Biometric Data. As Section 15(b) provides:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b).

32. To "collect" means "to bring together into one body or place," or "to gather or exact from a number of persons or sources."[2]

[2] Definition of "collect", Merriam-Webster, https://www.merriam-webster.com/dictionary/collect (last visited Feb 28, 2020).

33. Collection, therefore, is the act of gathering together, and is separate from possession, which is not an element of collection.

34. BIPA imposes three requirements that must be satisfied before any private entity may "collect" biometric information:

(a) First, the private entity must inform the individual in writing that the individual's biometric information is being collected or stored. 740 ILCS 14/15(b)(1).

(b) Second, the private entity must inform the individual in writing of the purpose and length of time for which their biometric information is being collected, stored, and used. 740 ILCS 14/15(b)(2).

(c) Finally, the private entity must receive a written release executed by the individual. 740 ILCS 14/15(b)(3).

35. BIPA defines a "written release," outside the employment context, to mean "informed written consent." 740 ILCS 14/10.

B. Possessing Biometric Data Under Section 15(a)

36. With respect to possession of Biometric Data, BIPA provides as follows:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a). Entities in possession of Biometric Data therefore must develop and make public a written policy containing a retention schedule for Biometric Data, as well as guidelines for the destruction of Biometric Data. *Id.*

37. BIPA requires that the required public, written policy include information about how the entity will destroy Biometric Data. *Id.*

38. The plain and ordinary meaning of the word "possession" is "the act of having or taking into control" or "control or occupancy of property without regard to ownership."[3]

39. A private entity that controls Biometric Data, therefore, possesses Biometric Data under Section 15(a).

40. Section 15(a) regulates Biometric Data that is controlled by a private entity regardless of whether that entity owns the Biometric Data.

41. Here, for example, Defendant controls Plaintiffs' Biometric Data, even though Defendant does not own that data. Therefore, as alleged in further detail below, Defendant possesses Plaintiffs' Biometric Data under Section 15(a).

C. BIPA's Unqualified Prohibition on Profiting from Biometric Data Under Section 15(c)

42. BIPA additionally bars private entities from profiting from Biometric Data. Section 15(c) provides as follows:

> No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

740 ILCS 14/15(c).

43. Section 15(c) is an unqualified prohibition on profiting from Biometric Data. Section 15(c) applies to this case, for among other reasons, because Defendant developed the face recognition "feature" of its Photos App in order to competitively position its devices and software in the marketplace, compete with other software applications, and thereby profit.

[3] Definition of "possession", Merriam-Webster, https://www.merriam-webster.com/dictionary/possession (last visited Feb. 28, 2020).

V. The Serious Threats Posed by Biometric Data

44. Extracting an individual's face geometry data in order to confirm a subsequent match of the individual's face—also known as "facial recognition" or "faceprinting"—uses biological characteristics to verify an individual's identity.

45. Use of facial recognition technology can be highly lucrative. The global facial recognition market size is expected to grow dramatically—according to one source, from $3.2 billion in 2019 to $7 billion by 2024.[4]

46. However, the potential dangers of the use of facial recognition technology and other biometric identifiers are widely known.

47. "Stolen biometric identifiers . . . can be used to impersonate consumers, gaining access to personal information."[5]

48. Unlike other identifiers such as Social Security or credit card numbers, which can be changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot be modified—ever. These unique and permanent biometric identifiers, once exposed, leave victims with no means to prevent identity theft and unauthorized tracking. Recognizing this, the Federal Trade Commission has urged companies using facial recognition technology to ask for consent before scanning and extracting Biometric Data from photographs.[6]

---

[4] *Facial Recognition Market Worth $7.0 Billion by 2024*, Markets and Markets, https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp (last visited Mar. 3, 2020).

[5] Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 629 (2019).

[6] *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), https://www.ftc.gov/

49. The threats posed by facial recognition technology can be more insidious than the threats posed by the use of other biometric information, such as fingerprints. Indeed, as commentators have recognized, "facial recognition creates acute privacy concerns that fingerprints do not."[7] Once a person or entity has an individual's facial Biometric Data:

> [T]hey can get your name, they can find your social networking account, and they can find and track you in the street, in the stores that you visit, the . . . buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you, and facial recognition technology can allow others to access all of that information from a distance, without your knowledge, and in about as much time as it takes to snap a photo.[8]

50. Researchers have even demonstrated the ability to "infer personally predictable sensitive information through face recognition."[9]

51. Further, facial recognition technology may "be abused in ways that could threaten basic aspects of our privacy and civil liberties[:]"[10]

> Biometrics in general are immutable, readily accessible, individuating, and can be highly prejudicial. And facial recognition takes the risks inherent in other biometrics to a new level. Americans cannot take precautions to prevent the collection of their image. We walk around in public. Our image is always exposed to the public. Facial recognition allows for covert, remote, and mass capture and

---

sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[7] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. On Privacy Tech & the Law of the S. Comm. On the Judiciary*, 112th Cong. 1 (2012) (statement of Sen. Al Franken, Chairman, Subcomm. On Privacy, Tech. & the Law of the S. Comm. On the Judiciary), *available at* https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf.

[8] Franken, *supra*.

[9] Alessandro Acquisti et al., *Face Recognition and Privacy in the Age of Augmented Reality*, J. Privacy and Confid. (2014), *available at* https://www.heinz.cmu.edu/~acquisti/papers/AcquistiGrossStutzman-JPC-2014.pdf.

[10] Franken, *supra*.

> identification of images, and the photos that may end up in a data base include not just a person's face but also what she is wearing, what she might be carrying, and who she is associated with. This creates threats to free expression and to freedom of association that are not evident in other biometrics.[11]

52. Many experts believe that "facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented."[12]

53. Because of these dangers, "privacy protections," such as those found in BIPA, are necessary for "all facial recognition technologies, including those that do not individually identify consumers."[13]

54. Indeed, the Illinois Supreme Court has held that in BIPA the Illinois "General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 129 N.E.3d at 1206.

55. In so holding, the Court explicitly recognized the "difficulty in providing meaningful recourse once a person's biometric identifiers or biometric information has been compromised." *Id.* As it further held, "[t]he situation is particularly concerning, in the

---

[11] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. On Privacy Tech & the Law of the S. Comm. On the Judiciary*, 112th Cong. 1 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), *available at* https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf.

[12] *See, e.g.*, Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

[13] *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

legislature's judgment, because [t]he full ramifications of biometric technology are not fully known.'" *Id.* (citing BIPA).

56. Storing Biometric Data on personal devices (as opposed to on a server) does not remove the substantial dangers associated with Biometric Data, because personal devices are intrinsically vulnerable to hackers and other malicious bad actors.[14] Instead, storing Biometric Data on personal devices creates an independent threat of serious harm that is associated with each personal device that contains Biometric Data.

57. Moreover, Biometric Data may persist on discarded devices. "Realistically, unless you physically destroy a device, forensic experts can potentially extract data from it."[15] The Federal Trade Commission has recognized that sensitive data on individual devices poses grave risks, including of identity theft.[16]

---

[14] *See, e.g.*, Taylor Telford, *Google Uncovers 2-Year iPhone Hack That Was 'Sustained' and 'Indiscriminate'*, Washington Post (Aug. 30, 2019, 8:52 AM), https://www.washingtonpost.com/business/2019/08/30/google-researchers-uncover-year-iphone-hack-tied-malicious-websites/ (citing Ian Beer, *A Very Deep Dive Into iOS Exploit Chains Found in the Wild*, Google Project Zero Blog (Aug. 29, 2019), https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html); Jeb Su, *Apple Issues 3 Emergency Security Fixes To Block Hackers From Taking Over iPhones, Macs, Apple TVs*, Forbes (Aug. 26, 2019, 7:17 PM), https://www.forbes.com/sites/jeanbaptiste/2019/08/26/apple-issues-3-emergency-security-fixes-to-block-hackers-from-taking-over-iphones-macs-apple-tvs/#6fc6f3a76da2.

[15] Josh Frantz, *Buy One Device, Get Data Free: Private Information Remains on Donated Tech*, Rapid7 Blog (Mar. 19, 2019), https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/.

[16] How to Protect Your Phone and the Data On It, https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it (last visited Mar. 3, 2020).

58. The use of Biometric Data "leads to the fear that a data breach or sale by one holder of a piece of a person's biometric information would compromise the security of all relationships that are verified by that same piece."[17]

59. This fear is not based on mere conjecture. Biometric Data has been illicitly targeted by hackers. For example, a security firm recently uncovered a "major breach" of a biometric system used by banks, police, defense firms, and other entities.[18] This breach involved exposure of extensive biometric and other personal data, including facial recognition data and fingerprints. *Id.*

60. Even anonymized Biometric Data poses risks. For example, according to a recent report:

> In August 2016, the Australian government released an "anonymized" data set comprising the medical billing records, including every prescription and surgery, of 2.9 million people. Names and other identifying features were removed from the records in an effort to protect individuals' privacy, but a research team from the University of Melbourne soon discovered that it was simple to re-identify people, and learn about their entire medical history without their consent, by comparing the dataset to other publicly available information, such as reports of celebrities having babies or athletes having surgeries.[19]

---

[17] Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 UC Irvine L. Rev. 107, 132 (2019).

[18] Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, The Guardian (Aug. 14, 2019, 3:11 PM), https://www.theguardian.com/technology/ 2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

[19] Olivia Solon, *'Data Is A Fingerprint': Why You Aren't as Anonymous As You Think Online*, The Guardian (Jul. 13, 2018, 4:00 PM) https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy.

Indeed, "[t]here is a growing skepticism in the field of data protection and privacy law that biometric data can never truly be deidentified or anonymized."[20]

61. The collection and use of Biometric Data is especially problematic in relation to the collection of Biometric Data from minors, who cannot provide informed consent and may be unaware of the serious harms that can result from the release of Biometric Data.

62. The heightened sensitivity of minors' personal data has been recognized by the federal government in the Children's Online Privacy Protection Act, which provides special protections for children's personal data.[21]

63. "The monetization of children's biometric . . . data is also concerning even if such data are anonymized."[22] Even "before minors come of age their immutable biometric or health-related data could be collected[.]"[23] Once a minor's biometric information is compromised, the damage can be permanent.

---

[20] Justin Banda, *Inherently Identifiable: Is It Possible To Anonymize Health And Genetic Data?*, International Association of Privacy Professionals Privacy Perspectives (Nov. 13, 2019), https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/.

[21] *See* Child Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506; 16 C.F.R. § 312.2 (defining personal information as including "[a] photograph, video, or audio file where such file contains a child's image or voice"; *see also Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FTC (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[22] Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. Rev. 423, 447 (2018).

[23] *Id.*

VI. Defendant Violated BIPA and Exposed Plaintiffs to Serious Harms

A. Defendant Collected Plaintiffs' Biometric Data

64. Defendant's facial recognition technology is offered as a "feature" of its Photos App that is included by default in its operating systems as well as pre-installed on its devices sold to customers.

65. Defendant began automatically collecting Biometric Data through iPhones via its Photos App with the release of its operating system iOS, version 10, on June 13, 2016. This operating system included the Photos App.[24]

66. Defendant's Photos App is included on iOS[25], iPadOS[26], and MacOS[27] operating systems, and is present on Apple Devices. These operating systems and the Photos App come preinstalled on Apple Devices.

67. The facial recognition "feature" of Defendant's Photos App functions by scanning a user's photo library for faces, and then, using facial recognition technology that extracts

---

[24] *See, e.g.*, Jackie Dove, *iOS 10 Photos: All the New Features and How to Use Them*, Tom's Guide (Sept. 15, 2016), https://www.tomsguide.com/us/ios-photos-features-and-tutorial,review-3817.html; Jason Cipriani, *Photos App on iOS 10: Albums, Searching and Memories*, CNET (Sept. 12, 2016), https://www.cnet.com/how-to/whats-new-with-photos-on-ios-10/.

[25] Photos for iOS and iPadOS, https://www.apple.com/ios/photos/ (last visited Mar. 3, 2020).

[26] *Id.*

[27] *Id.*

biometric identifiers from photographs, adding frequently found faces to the user's People album.[28]

68. In U.S. Patent No. 9,977,952 (filed Oct. 31, 2016), Defendant explained this process as follows:

> Facial recognition (or recognition) relates to identifying a person represented in an image. Recognition can be accomplished by comparing selected facial features from a graphical face to a facial database. Facial recognition algorithms can identify faces by extracting landmarks corresponding to facial features from the image. For example, an algorithm may analyze the relative position, size, and shape of the eyes, nose, cheekbones, and jaw.

Id. at 1:32–40.

69. Accordingly, the Photos App creates a scan of face geometry, which BIPA defines as a "biometric identifier." *See* 740 ILCS 14/10.

70. Defendant's facial recognition algorithms are run on Apple Devices.[29]

---

[28] Find People in Photos on iPhone, https://support.apple.com/guide/iphone/find-people-in-photos-iph9c7ee918c/ios (last visited Mar. 3, 2020); People – iPhone User Guide https://help.apple.com/iphone/10/#/iph9c7ee918c (last visited Mar. 3, 2020); Find and Identify Photos of People Using Photos on Mac, https://support.apple.com/guide/photos/view-photos-by-whos-in-them-phtad9d981ab/mac (last visited Mar. 3, 2020).

[29] *See* U.S. Patent No. 9,977,952 (filed Oct. 31, 2016). The system described in Fig. 2 of the '952 Patent represents "an exemplary system for correlating graphical faces." *Id.* at 3:23–24. Note that the computer system (labeled 204) performing the facial correlations "can be embedded in another device, such as a mobile telephone, a digital camera, a digital scanner, a digital video recorder, a personal digital assistant (PDA) . . . ." *Id.* at 19:16–20. Thus, the '952 Patent describes embodiments wherein the facial correlation algorithm is executed on desktops and laptops as well as on smart phones and tablets. *See also* Computer Vision Machine Learning Team, *An On-device Deep Neural Network for Face Detection*, Apple Machine Learning Journal, Nov. 2017, *available at* https://machinelearning.apple.com/2017/11/16/face-detection.html (describing how Defendant developed machine learning algorithms to perform facial recognition locally on Apple Devices.)

71. Biometric Data taken from an Apple Device user's image library are stored in what Defendant calls a facial recognition database,[30] or facial database,[31] in the solid state memory on the user's Apple Device.

72. Not only does Defendant use face geometries to identify individuals, with iOS version 11 it uses face geometries to model users faces[32] and track the users' expressions in real time.[33] Defendant calls this "intelligent face recognition."[34]

73. Defendant has published the following visualization of the face geometry it creates from pictures in users' photo libraries:[35]

---

[30] *See* U.S. Patent No. 9,600,483 (filed Sep. 26, 2012) at 10:64.

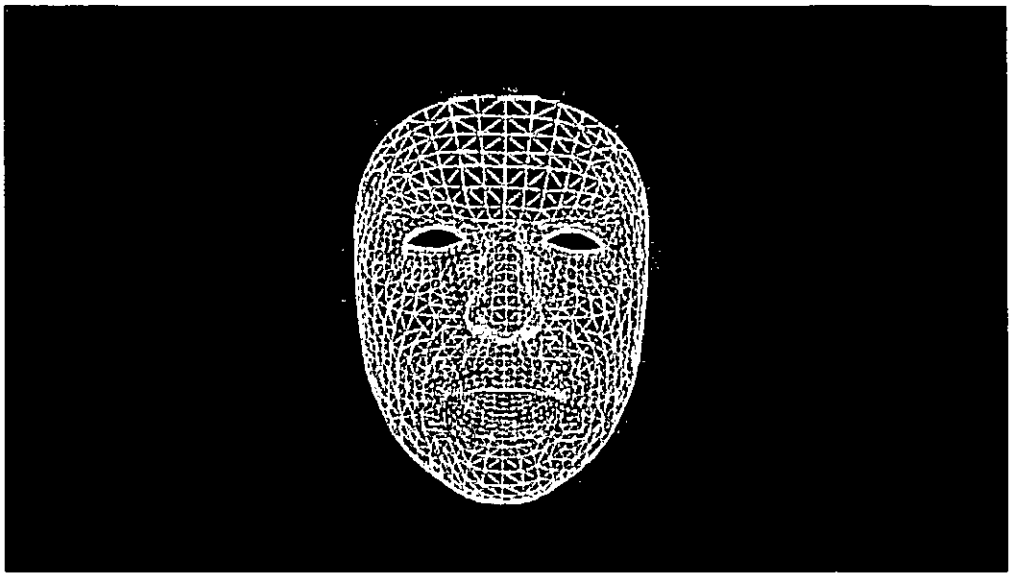
[31] *See* '952 Patent at 1:36; U.S. Patent No. 9,818,023 (filed Jan. 26, 2017) at 1:26; U.S. Patent No. 9,589,177 (filed Mar. 22, 205) at 1:24; U.S. Patent No. 9,514,355 (filed Dec. 6, 2016) at 1:34; U.S. Patent No. 9,495,583 (filed May 5, 2009) at 1:26–27; U.S. Patent No. 8,989,455 (filed Jan. 28, 2013) at 1:21–22.

[32] Tracking and Visualizing Faces | Apple Developer Documentation, https://developer.apple.com/documentation/arkit/tracking_and_visualizing_faces (last visited Mar. 3, 2020) ("Use Face Geometry to Model the User's Face").

[33] Face Tracking with ARKit – Tech Talks – Videos – Apple Developer, https://developer.apple.com/videos/play/tech-talks/601/ (last visited Mar. 3, 2020); Tracking the User's Face in Real Time | Apple Developer Documentation, https://developer.apple.com/documentation/vision/tracking_the_user_s_face_in_real_time (last visited Mar. 3, 2020) ("In order to visualize the geometry of observed facial features, the code draws paths around the primary detected face and its most prominent features.").

[34] Photos for iOS and iPadOS, https://www.apple.com/ios/photos/ (last visited Mar. 3, 2020).

[35] https://devimages-cdn.apple.com/wwdc-services/images/8/1998/1998_wide_250x141_2x.jpg (last visited Mar. 3, 2020).



74. After creating facial templates, Defendant uses facial recognition algorithms to analyze digital photographs stored on its devices and automatically group photographs into albums based on whether a person's face is in the photograph. Children and minors are included among those whose facial geometries are analyzed and grouped by Defendant.

75. Defendant's facial recognition algorithms calculate a unique digital representation of faces based on geometric attributes, such as distance between the eyes, width of the nose, and other features.

76. Defendant's software collects Biometric Data to group all photographs that include a particular person's face into an album or folder.

77. Defendant creates a unique faceprint for every person appearing in any photograph stored using its Photos App.

78. Defendant collects this face Biometric Data without obtaining consent, let alone the "informed written consent" required by BIPA.

79. Defendant's devices, further, collect Biometric Data from *all* individuals, including minors, whose faces appear in Apple Device users' photographs—*not just from Apple Device users*.

80. Defendant confirms these capabilities and seeks to profit from its collection of Biometric Data by advertising its Photos App as being able to "recognize the people, scenes, and objects in [photographs]."[36]

81. Defendant further advertises that its Photos App "uses advanced computer vision to scan all of your photos" so that users can "[s]ort your images by your favorite subjects — the people in your life."[37]

82. In order to sort photos, Defendant admits that its Photos App uses "[i]ntelligent face recognition and location identification."[38]

83. Defendant advertises to users the ability "to find the exact photos you're looking for, based on who you were with or where you were when you took them."[39]

84. Defendant collects biometric identifiers and biometric information for individuals whose faces appear in photographs stored on Apple Devices. These Biometric Data are catalogued on the Photos App.

---

[36] About People in Photos on Your iPhone, iPad, or iPod Touch, https://support.apple.com/en-us/HT207103 (last visited Mar. 3, 2020).

[37] *Id.*

[38] Photos for iOS and iPadOS, https://www.apple.com/ios/photos/ (last visited Mar. 3, 2020).

[39] *Id.*

85. Defendant's collection of biometric identifiers and biometric information through its Photos App is automatic and occurs without the involvement or consent of an Apple Device user whenever a new photograph is stored on an Apple Device.

86. Apple Device users cannot disable Defendant's facial recognition technology, and cannot prevent Defendant's collection of Biometric Data from occurring.

87. Defendant provides no mechanism by which users or nonusers may opt out of the collection of their Biometric Data.

88. Consumers who buy Apple Devices own the hardware but merely license the software necessary for the device to function. That software is wholly owned and controlled by Defendant.[40]

89. Defendant's applicable End User License Agreements ("EULAs") provide as follows: "The software . . . [is] licensed, not sold, to you by Apple Inc. ('Apple') for use only under the terms of this License. Apple and its licensors retain ownership of the Apple Software itself and reserve all rights not expressly granted to you."[41]

90. The Apple Device user is granted "a limited non-exclusive license to use the Apple Software on a single Apple-branded Device" and cannot alter the software. [42]

91. Because disabling facial recognition is not permitted by Defendant, the use of Apple Devices to take or store photographs is *conditioned* on the collection of Biometric Data.

---

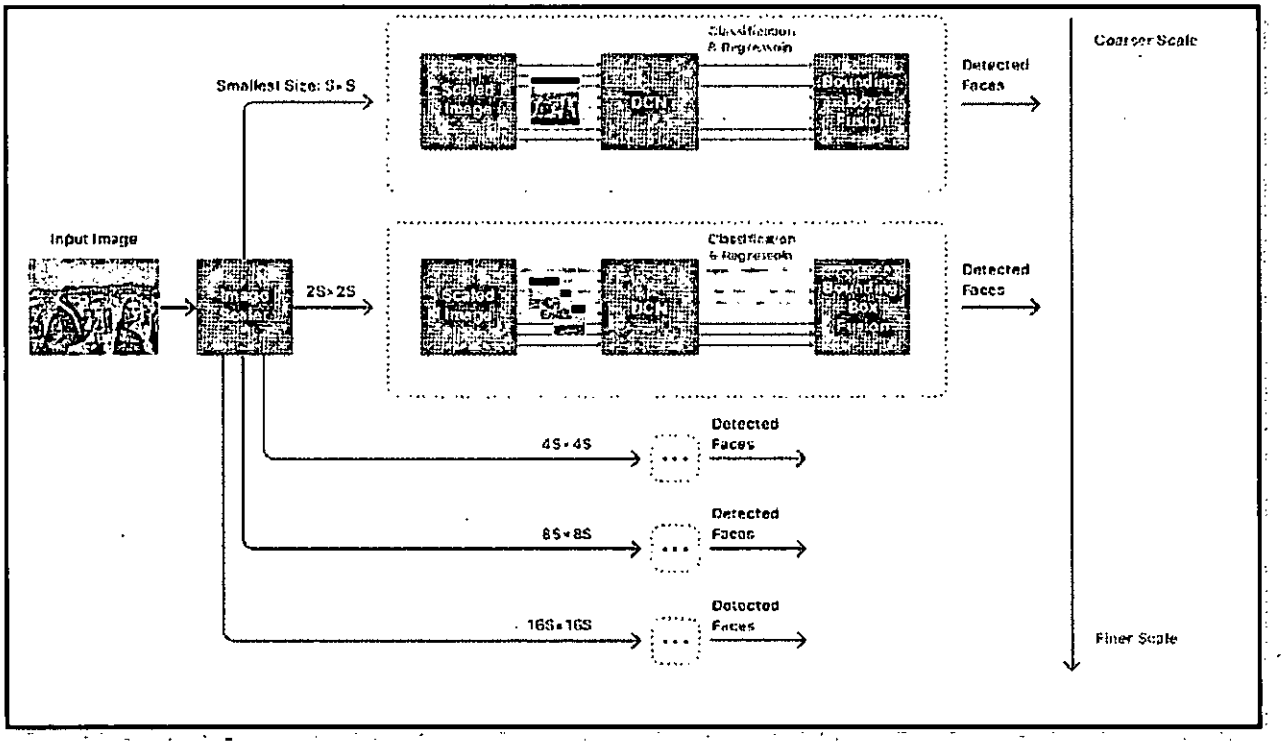
[40] *See, e.g.* iOS and iPad OS Software License Agreement, 1, https://www.apple.com/legal/sla/docs/iOS13_iPadOS13.pdf (last visited Mar. 3, 2020) ("iOS EULA"); Software License Agreement for macOS Catalina, 1, https://www.apple.com/legal/sla/docs/macOSCatalina.pdf (last visited Mar. 3, 2020).

[41] iOS EULA at 1.

[42] *Id.* at 2.

92. Defendant indiscriminately collects Biometric Data for all photographic subjects, including customers, non-customers, and minors incapable of providing informed consent.

93. Defendant publishes the "Machine Learning Journal," which contains posts dedicated to describing the development of various of Defendant's products. In one such post from November 2017, Defendant described the use of deep learning to facilitate the facial recognition feature used by the Photos App as packaged in iOS version 10.[43] Defendant describes the below figure as a "[f]ace detection workflow."[44]



[43] Computer Vision Machine Learning Team, *An On-device Deep Neural Network for Face Detection*, Apple Machine Learning Journal, Nov. 2017, *available at* https://machinelearning.apple.com/2017/11/16/face-detection.html.

[44] *Id.*

94. As this diagram demonstrates, the Photos App receives a photograph as input and employs an algorithm that iterates its face detection process in increasingly finer detail in an effort to create a "final prediction of the faces in the image."[45]

95. At minimum, this demonstrates that when Defendant's Photos App utilizes its facial recognition "feature," Defendant collects "biometric information" as defined by BIPA.

96. However, Defendant failed to obtain informed written consent prior to collecting this biometric information as required by BIPA.

97. In its '952 Patent, Defendant describes a method "for organizing images, such as digital images, by correlating one or more faces represented in the images." U.S. Patent No. 9,977,952 (filed Oct. 31, 2016) at 1:18–20.

98. Defendant explains in the '952 Patent that its invention relates to "[f]acial recognition algorithms." *Id.* at 1:36–38.

99. On information and belief, Defendant has implemented the methods and embodiments described in the '952 Patent in its Photos App in collecting Biometric Data from Plaintiffs and other Illinois residents.

100. Defendant has explained the "advantages" of its automatic collection of biometric identifiers and automatic population of albums by persons in photographs on Apple Devices. One such advantage that Defendant has identified involves helping Apple Device users to understand the functionality of Defendant's Photos App:

> Organizing images by the people represented in the media provides several potential advantages. For example, such an organizational scheme can be intuitive for users of an image system, enabling users to quickly understand the functioning of the system. Further, the burden of manually organizing many images can be substantially eliminated or reduced. In addition, images can be accurately grouped

[45] *Id.*

> based on a person represented in the images. Accurately grouping images can provide improved accessibility, organization and usability of the images by users.

Id. at 3:4–13.

101. After biometric identifiers are collected and Defendant's software has a sufficient sampling of images, the Photos App applies an algorithm to identify the Apple Device user, thereby creating biometric information. The algorithm also uses biometric identifiers collected from images to create individualized groupings of all photographs that include a particular person, such as a friend or family member of the user.

102. Contrary to the requirements of BIPA, Defendant has not, despite its collection of Biometric Data, developed any written policy, made available to the public, establishing a retention schedule or guidelines for permanently destroying Biometric Data.

103. Consequently, Apple Devices are currently incapable of lawful use in Illinois, because they automatically collect biometric information without consent in violation of BIPA, and because the Apple Device user is prohibited by Defendant's EULAs from altering Defendant's software, which Defendant alone owns and controls, to prevent the unlawful collection of the Biometric Data of the user and those whose photographs appear on the user's device.

104. Defendant intentionally designed and licensed the Apple Devices to be incapable of lawful use in Illinois.

B. Defendant Possesses Plaintiffs' Biometric Data

105. Although, on information and belief, Defendant does not store or transfer all user Biometric Data on or by means of its servers, it has complete and exclusive control over the Biometric Data on Apple Devices. To be clear, Defendant controls:

- Whether biometric identifiers are collected;

- What biometric identifiers are collected;
- The type of Biometric Data that are collected and the format in which they are stored;
- The facial recognition algorithm that is used to collect Biometric Data;
- What Biometric Data are saved;
- Whether biometric identifiers are used to identify users (creating biometric information);
- Whether Biometric Data are kept locally on users' Apple Devices;
- Whether Biometric Data are encrypted or otherwise protected; and
- How long Biometric Data are stored.

106. The user of an Apple Device, in contrast, has no ability to control the Biometric Data on the user's Apple Device.

107. The user has no control over whether Biometric Data is collected from the user's photo library.

108. On Defendant's iPhone and iPad devices, the Photos App automatically collects biometric identifiers while running in the background.[46]

109. On Macintosh computers, the Photos App collects biometric identifiers from a user's image library as soon as the Photos App is opened.[47]

110. Users cannot disable the collection of Biometric Data, cannot limit what information is collected or from whom information is collected, cannot remove the People folder, and cannot delete the database of facial recognition information that Defendant creates or any information in that database.

---

[46] Find People In Photos On iPhone – Apple Support, https://support.apple.com/guide/iphone/find-people-in-photos-iph9c7ee918c/ios (last visited Mar. 3, 2020); U.S. Patent No. 9,977,952 at 5:56–57.

[47] Find and Identify Photos of People Using Photos on Mac – Apple Support, https://support.apple.com/guide/photos/view-photos-by-whos-in-them-phtad9d981ab/mac (last visited Mar. 3, 2020).

111. Indeed, Defendant's EULAs specifically *prohibit* users from modifying Defendant's software to prevent the collection of Biometric Data.[48]

112. Defendant only allows users to use Apple Devices on the condition that Defendant collects Biometric Data.

113. Defendant fully controls the Biometric Data on Apple Devices, and therefore possesses it because, for among other reasons, Defendant forbids users from disabling the Biometric Data collection of Apple Devices.

C. Defendant Profits from Plaintiffs' Biometric Data

114. Defendant profits from the Biometric Data collected by Apple Devices through the sale of those devices.

115. Defendant uses the face recognition "feature" of its Photos App in order to advertise its operating systems and Apple Devices to potential users.

116. Defendant advertises its Photos App as being able to "recognize the people, scenes, and objects in [photographs],"[49] and that it "uses advanced computer vision to scan all of your photos" so that users can "[s]ort your images by your favorite subjects — the people in your life.[50] Defendant also advertises that users have the ability "to find the exact photos you're looking for, based on who you were with or where you were when you took them."[51]

---

[48] *See, e.g.*, iOS EULA at 1.

[49] About People in Photos on Your iPhone, iPad, or iPod Touch, https://support.apple.com/en-us/HT207103 (last visited Mar. 3, 2020).

[50] *Id.*

[51] Photos for iOS and iPadOS, https://www.apple.com/ios/photos/ (last visited Mar. 3, 2020).

117. Defendant developed these "features" for its Photos App to compete with similar features being offered on other devices, giving Defendant a competitive edge that allowed Defendant to profit from the sale of Apple Devices.

118. For the reasons set forth above, among others, Defendant profits from Biometric Data.

119. Defendant is prohibited from profiting from any "person's or . . . customer's biometric information" because Defendant is "a private entity in possession of a biometric identifier." 740 ILCS 14/15(c). Therefore, the fact that Defendant profits from the Biometric Data it collects is unlawful.

D. Defendant's Conduct Violates BIPA

120. Defendant has failed to comply with BIPA's requirements concerning the collection and possession of Biometric Data. With respect to its collection of Biometric Data, Defendant failed to:

(1) inform the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) inform the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; or

(3) receive a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b).

121. With respect to its possession of Biometric Data, Defendant failed 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, whichever occurs first.

740 ILCS 15(a).

122. Defendant's failure to comply with BIPA extends to nonusers of its devices. This is because Defendant's Photos App collects and possesses the Biometric Data of *everyone* who appears in images stored on a user's Apple Device.

123. Defendant does not have commercial relationships with the nonusers whose Biometric Data it collects, and does not know which nonusers' Biometric Data it is collecting. Therefore, Defendant cannot obtain informed written consent from nonusers.

124. Furthermore, many of the nonusers from whom Defendant collects Biometric Data are minors who cannot give informed written consent.

125. Defendant also does not comply with BIPA's prohibition on profiting from Biometric Data.

126. Defendant developed the facial recognition feature of its Photos App in part to compete with other electronic device vendors and software developers, and in order to sell Apple Devices.

127. Defendant did, in fact, profit from the sale of Apple Devices as a result of Defendant's facial recognition "feature."

E. Defendant's BIPA Violations Expose Plaintiffs and Other Illinois Residents to Threats of Serious Harm

128. Defendant's BIPA violations present an imminent threat of serious harm to Plaintiffs and the proposed class.

129. When Biometric Data is stored on personal electronic devices, persons from whom Biometric Data has been collected face a multiplicity of threats.

130. Defendant does not delete the Biometric Data it collects, which are located on numerous devices in this State. Moreover, an Apple Device user's Biometric Data may be stored

on one or more iPhones, iPads or MacBooks, as well as discarded Apple Devices. Furthermore, nonusers' Biometric Data that Defendant collects may be stored on one or more Apple Devices.

131. For example, an Illinois resident's Biometric Data may be stored on the Apple Devices of his or her family, his or her relatives, his or her friends, his or her coworkers, and anyone else who photographed him or her using an Apple Device.

132. Apple Device users cannot prevent their devices from collecting their unique and sensitive Biometric Data, and nonusers cannot control whether Apple Devices containing this unique and sensitive information are lost, stolen, discarded improperly, given to vendors for repair work, or recycled. Nonusers likewise cannot control whether their Biometric Data is extracted, decrypted, or sold.

133. Information stored in a central location, such as a server, presents a single breach threat. A sophisticated entity may take measures to securely and centrally store information, guarding against the threat of a data breach. By contrast, as the result of the fact that the Biometric Data that Defendant collects are stored on numerous devices, Plaintiffs and members of the Class face the imminent threat of disclosure of their Biometric Data as a result of a data breach on any one of the Apple Devices on which their Biometric Data are stored.

134. Defendant has greater than a 40% market share of the smartphone market in the United States,[52] around 10% of the laptop market,[53] and approximately 17% of the desktop

---

[52] S. O'Dea, *iPhone Users As Share of Smartphone Users In The United States 2014–2021*, Statista (Feb. 27, 2020) https://www.statista.com/statistics/236550/percentage-of-us-population-that-own-a-iphone-smartphone/; Chance Miller, *Canalys: Apple Shipped 14.6M iPhones in North America During Q1, Securing 40% Marketshare,* 9to5Mac (May 9, 2019 3:23 PM), https://9to5mac.com/2019/05/09/iphone-north-america-marketshare/.

[53] I. Mitic, *Laptops by the Numbers: Market Share and More*, Fortunly (Nov. 5, 2019), https://fortunly.com/blog/lap-top-market-share/.

market. 96% of adult Americans use smartphones and approximately 75% percent of Americans own a desktop or laptop.[54]

135. Many of the Apple Devices used in this State have collected the Biometric Data of multiple individuals other than the Apple Device user. Consequently, numerous Illinois residents have their Biometric Data stored on one or more Apple Devices outside their control.

136. The durability of the memory in Apple Devices creates a nearly permanent risk of a data breach of biometric identifiers and information for both device users as well as nonusers whose Biometric Data have been collected. Apple Devices utilize solid state memory, which can withstand drops, extreme temperatures, and magnetic fields.[55] Unless corrupted, this solid state memory and the information it contains can last in perpetuity. Thus, the Biometric Data on Apple Devices will likely outlast the device battery, the functionality of the device screen, and the natural life of the device user.

137. Apple Devices, like all computing devices, are vulnerable to hackers and other malicious bad actors. For example, the Washington Post recently reported that security researchers discovered a "'sustained' . . . and indiscriminate campaign to hack iPhones through certain websites, allowing attackers to steal messages, files and track location data every 60 seconds."[56] Just days prior to that report's publication, Defendant released an "emergency fix"

---

[54] *Mobile Fact Sheet*, Pew Research Center (Jun. 12, 2019), *available at* https://www.pewresearch.org/internet/fact-sheet/mobile/.

[55] Roderick Bauer, *SSD 101: How Reliable are SSDs?*, BackBlaze (Feb. 21, 2019), https://www.backblaze.com/blog/how-reliable-are-ssds/.

[56] Taylor Telford, *Google Uncovers 2-Year iPhone Hack That Was 'Sustained' and 'Indiscriminate'*, Washington Post (Aug. 30, 2019, 8:52 AM), https://www.washingtonpost.com/business/2019/08/30/google-researchers-uncover-year-iphone-hack-tied-malicious-websites/ (citing Ian Beer, *A Very Deep Dive Into iOS Exploit Chains Found*

to a *different* vulnerability that allowed "malicious hackers to take control of all Apple desktop and laptop computers [and] mobile devices."[57]

138. Biometric Data may persist on discarded Apple Devices, which could be extracted by malicious actors using methods of removal that may or may not currently exist.[58] The risk of illicit harvesting of biometric information from discarded Apple Devices therefore extends far into the future.

F. Defendant Is Liable for Its BIPA Violations both Directly and Vicariously

139. Defendant is directly liable for the BIPA violations based on the functionality of its proprietary software, which it wholly owns and exclusively controls, and which Apple Device users are prohibited from owning, controlling, or modifying.

140. Furthermore, Defendant is vicariously liable for BIPA violations because its software operated as a "software agent:"

> A software agent is essentially a software version of a concept familiar in the law: an entity that performs a task, with some degree of autonomy, on behalf of someone else. An agent in the physical world can perform its task without input from the principal; this is equally true when an agent is a machine, such as a robot on a

---

in the Wild, Google Project Zero Blog (Aug. 29, 2019), https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html).

[57] Jeb Su, *Apple Issues 3 Emergency Security Fixes To Block Hackers From Taking Over iPhones, Macs, Apple TVs*, Forbes (Aug. 26, 2019, 7:17 PM), https://www.forbes.com/sites/jeanbaptiste/2019/08/26/apple-issues-3-emergency-security-fixes-to-block-hackers-from-taking-over-iphones-macs-apple-tvs/#6fc6f3a76da2.

[58] *See, e.g.*, Josh Frantz, *Buy One Device, Get Data Free: Private Information Remains on Donated Tech*, Rapid7 Blog (Mar. 19, 2019), https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/; William Gallagher, *Wipe Your iPhone Before Selling It, Because If You Don't You Might Get Your Data Stolen*, Apple Insider (Jul 26, 2018), https://appleinsider.com/articles/18/07/26/wipe-your-iphone-before-selling-it-because-if-you-dont-you-might-get-your-data-stolen.; How to Protect Your Phone and the Data On It, https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it (last visited Mar. 3, 2020).

> factory floor, which can perform its repetitive task without needing constant human guidance. A software agent operates in the same way—it can perform its task without human input. For example, a software agent useful to shoppers could scan a large number of websites for a certain product, and identify the website offering the product at the lowest price; to the text of the note without such a program, the human user would have to look at each website herself.

NetFuel, Inc. v. F5 Networks, Inc., No. 13-7895, 2017 WL 2834538, at *1 (N.D. Ill. June 29, 2017); *see also Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005) (technology distributor contributorily and vicariously liable for the unlawful use of technology where the technology has an "unlawful objective"); *Akamai Techs., Inc. v. Limelight Networks, Inc.*, 797 F.3d 1020, 1024 (Fed. Cir. 2015) (software designer liable for infringing conduct of software where use of software "conditioned" on infringing behavior); *Shaw v. Toshiba Am. Info. Sys., Inc.*, 91 F. Supp. 2d 926 (E.D. Tex. 1999) (software designer liable for harm to third party caused by software).

141. In this case, Defendant, in addition to being directly liable, is also vicariously liable for BIPA violations caused by the use of Apple Devices because, under principles of agency law, Defendant's Apple Devices functioned as software agents subject to the actual authority of Defendant, because Defendant acted negligently in controlling its proprietary software installed on Apple Devices, or both. Restatement (Third) Of Agency §§ 7.04; 7.05 (2006).

142. Further, Defendant is vicariously liable because the use of its Apple Devices was conditioned on unlawful use and had an objective that was unlawful under Illinois law.

VII. Plaintiffs' Experiences with Defendant's Products

143. Each Plaintiff has used one or more Apple Device to take or store photographs of themselves and other people. No Plaintiff was aware Defendant's facial recognition technology would collect Biometric Data and organize photographs based on facial geometries. However,

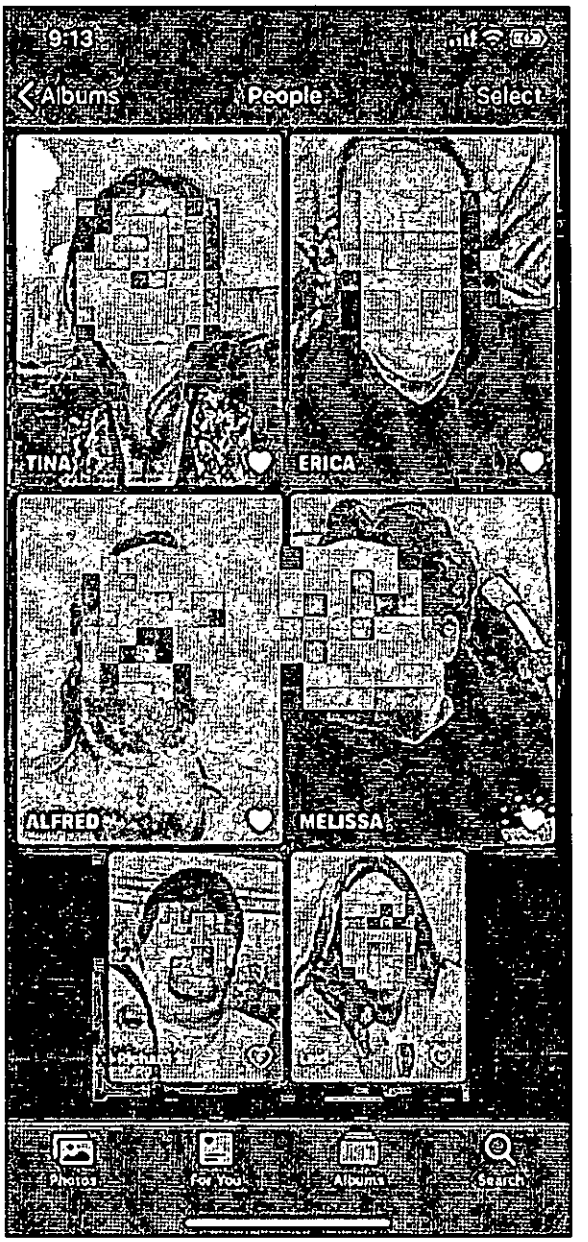
Defendant's facial recognition technology has collected Biometric Data not only from Plaintiffs, but also from individuals appearing in photographs on Plaintiffs' Apple Devices, including parents, grandchildren, siblings, cousins, friends, and/or co-workers of Plaintiffs.

144. Plaintiff Roslyn Hazlitt has owned an iPhone for several years; her phone has contained pictures of herself since that time. She is not aware of the People and Places facial recognition "feature." She never agreed to allow Defendant to collect her Biometric Data. Nevertheless, the People and Places feature of the Photos App on Ms. Hazlitt's iPhone has automatically generated albums that contain photographs of herself as well as her father based on Defendant's collection of her Biometric Data and her father's Biometric Data.

145. Plaintiff Jane Doe is an eight-year-old minor. She owns an iPad, which she has used to take photos, including of herself. She also appears in the photographs of her relatives who own various Apple products. She has not, and cannot, give consent for her biometric information to be collected or possessed by Defendant. Further, Jane Doe's parents have not given informed written consent to allow Defendant to collect or possess Jane Doe's Biometric Data. The People and Places "feature" of the Photos App on Jane Doe's iPad has automatically generated a photo album that contains photographs of Jane Doe based on Defendant's collection of her Biometric Data.

146. Plaintiff Richard Robinson has owned an iPhone for several years. Mr. Robinson also has previously owned an iPad. Mr. Robinson has taken photos with his iPhone, including of himself and other family members. Although he has "tagged" individuals in the photographs that Defendant has organized by facial geometry, Mr. Robinson is unsure whether he has ever actually used Defendant's People and Places "feature" in the Photos App, and has never provided consent, let alone informed written consent, for his Biometric Data to be used or

collected. Nevertheless, the People and Places feature in the Photos App on his iPhone has created various albums for individuals appearing in his photographs:



The above screenshot is from Mr. Robinson's iPhone and shows the people-specific albums automatically generated by Defendant's software. From left to right, top to bottom, the albums in the above screenshot correspond to Mr. Robinson's wife, daughter-in-law, brother, daughter, himself, and granddaughter.

147. Plaintiff Yolanda Brown has had an iPhone for several years, and has taken various photographs throughout that period. The earliest photos of herself that are currently stored on her iPhone date from approximately ten years ago. She was not aware of Defendant's People and Places "feature" of the Photos App, though she has "tagged" individuals in the photographs that Defendant has organized by facial geometry. The People and Places feature of the Photos App on Ms. Brown's phone has automatically generated photo albums for photographs containing each of her three nieces, six aunts, five cousins, and brother. Ms. Brown never consented to Defendant's collection of her Biometric Data.

148. On information and belief, Defendant applies its facial recognition technology to *every picture* that a user saves on his or her Apple Device running Defendant's Photos App.

149. When an Illinois resident purchases an Apple Device, Defendant does not inform them that Biometric Data will be collected from every person whose picture is stored on the device, including the Apple Device user and any other person whose face appears in a photograph stored on the Photos App. Defendant has not informed Plaintiffs that Biometric Data has been and is being collected from the individuals whose faces appear in photographs stored on users' Photos Apps.

150. Moreover, Defendant has not informed Plaintiffs that the Photos App is installed on their devices by default and will operate on mobile devices whenever a photograph is added to the Photos App or when the Photos App is started on laptop or desktop computers.

151. As a result, Defendant did not obtain consent from Plaintiffs in any form prior to collecting their facial geometry data, let alone written, informed consent as required by BIPA. Nor has Defendant obtained consent from other members of the proposed class, including minors whose photos appear in the Photos App.

152. Defendant has collected biometric information and biometric identifiers from Plaintiffs in violation of BIPA.

VIII. Class Allegations

153. Plaintiffs seek to represent the following similarly situated individuals (collectively, the "Class"):

Subclass 1: All Illinois citizens whose faces appeared in one or more photographs taken or stored on their own Apple Devices running the Photos App from March 4, 2015 until present.

Subclass 2: All Illinois citizens whose faces appeared in one or more photographs taken or stored on an Apple Device other than their own running the Photos App from March 4, 2015 until present.

154. Numerosity. The Class includes thousands of people, such that it is not practicable to join all Class members into one lawsuit.

155. Commonality. The issues involved with this lawsuit present common questions of law and fact, including:

- whether Defendant collected and/or possessed the Class's biometric identifiers or biometric information;
- whether Defendant profited from biometric identifiers or biometric information;
- whether Defendant properly informed Class members that it captured, collected, used, and stored their biometric identifiers and/or biometric information;
- whether Defendant obtained "informed written consent" (740 ILCS 14/10) to capture, collect, use, and store Class members' biometric identifiers and/or biometric information;
- whether Defendant used Class members' biometric identifiers and/or biometric information to identify them; and
- whether Defendant' violations of BIPA were committed recklessly or negligently.

156. Predominance. The common questions of law and fact predominate over any individual issue that may arise on behalf of an individual Class member.

157. Typicality. Plaintiffs, the members of the Class, and Defendant have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

158. Adequacy. Plaintiffs and counsel will fairly and adequately protect the interests of Class members. Plaintiffs' counsel, Schlichter Bogard & Denton, LLP, will fairly and adequately represent the interests of the Class. Schlichter Bogard & Denton, LLP has a well-documented track record of serving as class counsel in this State and elsewhere. Schlichter Bogard & Denton's pioneering work in class actions brought on behalf of citizens of this State and others has been covered by numerous national publications, including the New York Times and Wall Street Journal, among other media outlets. By way of limited example, courts in this State have noted in reference to the work of Schlichter Bogard & Denton, LLP in class action litigation:

- "This Court is unaware of any comparable achievement of public good by a private lawyer in the face of such obstacles and enormous demand of resources and finance." Order on Attorney's Fees, *Mister v. Illinois Central Gulf R.R.*, No. 81-3006 (S.D. Ill. 1993).

- "This Court finds that Mr. [Jerome J.] Schlichter's experience, reputation and ability are of the highest caliber. Mr. Schlichter is known well to the District Court Judge and this Court agrees with Judge Foreman's review of Mr. Schlichter's experience, reputation and ability." Order on Attorney's Fees, *Wilfong v. Rent-A-Center*, No. 0068-DRH (S.D. Ill. 2002).

- "Class Counsel performed substantial work . . . investigating the facts, examining documents, and consulting and paying experts to determine whether it was viable. This case has been pending since September 11, 2006. Litigating the case required Class Counsel to be of the highest caliber and committed to the interests of the [class]." *Will v. General Dynamics*, No. 06-698, 2010 WL 4818174, at *2 (S.D. Ill. Nov. 22, 2010).

- "Schlichter, Bogard & Denton has achieved unparalleled results on behalf of its clients, . . . has invested . . . massive resources and persevered in the face of . . . enormous risks[.]" *Nolte v. Cigna Corp.*, No. 07-2046, 2013 WL 12242015, at *2 (C.D. Ill. Oct. 15, 2013).

- "Litigating this case against formidable defendants and their sophisticated attorneys required Class Counsel to demonstrate extraordinary skill and determination."

Beesley v. Int'l Paper Co., No. 06-703, 2014 WL 375432, at *2 (S.D. Ill. Jan. 31, 2014).

- "Schlichter, Bogard & Denton demonstrated extraordinary skill and determination in obtaining this result for the Class." *Abbott v. Lockheed Martin Corp.*, No. 06-701, 2015 WL 4398475, at *2 (S.D. Ill. July 17, 2015).

Plaintiffs' counsel Christian Montroy is also an experienced class action practitioner who will adequately represent the Class.

159. Superiority. A class action is the appropriate vehicle for fair and efficient adjudication of Plaintiffs' and Class members' claims because if individual actions were required to be brought by each member of the Class, the result would be a multiplicity of actions, creating a hardship to the Class, to the Court, and to Defendant.

COUNT I – VIOLATION OF 740 ILCS 14/15(b)

160. Plaintiffs incorporate paragraphs 1 through 159 as though fully realleged herein.

161. BIPA created statutory duties for Defendant with respect to the collection of biometric identifiers and biometric information of Plaintiffs and the Class. *See* 740 ILCS 14/15(b).

162. Defendant violated BIPA section 15(b)(1) by collecting Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, without first informing Plaintiffs and Class members that Defendant was collecting this information.

163. Defendant violated BIPA section 15(b)(2) by collecting Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, without informing Plaintiffs and Class members in writing of the purpose for the collection. Further, Defendant violated BIPA section 15(b)(2) by failing to inform Plaintiffs and Class members in writing of the length of time Defendant would collect

Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information.

164. Defendant violated BIPA section 15(b)(3) by collecting Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, without first obtaining informed written consent authorizing Defendant to collect Plaintiffs' and Class members' biometric identifiers and/or biometric information.

165. Defendant's BIPA violations are violations of Defendant's duty of ordinary care owed to Plaintiffs and the Class.

166. In the alternative, Defendant's BIPA violations were willful and wanton. Defendant knowingly, intentionally, and/or recklessly violated the duty it owed to Plaintiffs and the Class.

167. Plaintiffs incurred injuries that were proximately caused by Defendant's conduct. Through its actions, Defendant exposed Plaintiffs and the Class to imminent threats of serious harm.

168. Plaintiffs in this Count I hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

COUNT II – VIOLATION OF 740 ILCS 14/15(a)

169. Plaintiffs incorporate paragraphs 1 through 168 as though fully realleged herein.

170. BIPA created statutory duties for Defendant with respect to the possession of the biometric identifiers and biometric information of Plaintiffs and the Class. *See* 740 ILCS 14/15(a).

171. Defendant violated BIPA section 15(a) by possessing Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of face geometry and related biometric information, without creating and following a written policy, made available to the public, establishing and following a retention schedule and destruction guidelines for Defendant's possession of biometric identifiers and information.

172. Defendant's BIPA violations are violations of Defendant's duty of ordinary care owed to Plaintiffs and the Class.

173. In the alternative, Defendant's BIPA violations were willful and wanton. Defendant knowingly, intentionally and/or recklessly violated the duty it owed to Plaintiffs and the Class.

174. Plaintiffs incurred injuries that were proximately caused by Defendant's conduct. Through its actions, Defendant exposed Plaintiffs and the Class to imminent threats of serious harm.

175. Plaintiffs in this Count II hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

COUNT III – VIOLATION OF 740 ILCS 14/15(c)

176. Plaintiffs incorporate paragraphs 1 through 175 as though fully realleged herein.

177. Under BIPA, Defendant owed a duty to Plaintiffs and the Class not to profit from their Biometric Data. *See* 740 ILCS 14/15(c).

178. Defendant is subject to BIPA section 15(c) because it is a "private entity in possession of a biometric identifier or biometric information."

179. Defendant possesses the Biometric Data stored locally on the electronic devices of Plaintiffs and the Class because, as alleged herein, Defendant exclusively controls that Biometric Data.

180. In addition, on information and belief, Defendant possesses, among other Biometric Data, scans of facial geometry that are stored on devices owned by Defendant. This includes, but is not limited to, scans of facial geometry that are present on devices owned by Defendant, including those used by employees of Defendant.

181. Defendant violated BIPA section 15(c) by profiting from Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, by, among other things, marketing and selling its devices based upon claims of their ability to sort photographs, as alleged in more detail herein.

182. Defendant's BIPA violations are violations of Defendant's duty of ordinary care owed to Plaintiffs and the Class.

183. In the alternative, Defendant's BIPA violations were willful and wanton. Defendant knowingly, intentionally and/or recklessly violated the duty it owed to Plaintiffs and the Class.

184. Plaintiffs incurred injuries that were proximately caused by Defendant's conduct. Through its actions, Defendant exposed Plaintiffs and the Class to imminent threats of serious harm.

185. Plaintiffs in this Count III hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, pray for judgment against Defendant Apple Inc. as follows:

A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class counsel;

B. Finding that Defendant's conduct violates BIPA;

C. Awarding actual damages caused by Defendant's BIPA violations;

D. Awarding statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), and damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1);

E. Awarding injunctive and/or other equitable or non-monetary relief as appropriate to protect the Class, including by enjoining Defendant from further violating BIPA pursuant to 740 ILCS 14/20(4);

F. Awarding Plaintiffs reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as this Court deems appropriate and as equity and justice may require.

JURY DEMAND

Plaintiffs request trial by jury of all claims asserted herein.

Dated: March 4, 2020

Respectfully submitted,

/s/ Jerome J. Schlichter

Jerome J. Schlichter (IL 2488116)
Andrew D. Schlichter*
Alexander L. Braitberg (IL 6320350)
Brett Rismiller*
SCHLICHTER BOGARD & DENTON LLP
100 South Fourth St., Ste. 1200
St. Louis, MO 63102
Phone: (314) 621-6115
Fax: (314) 621-5934
jschlichter@uselaws.com
aschlichter@uselaws.com
abraitberg@uselaws.com
brismiller@uselaws.com
**pro hac vice forthcoming*

Christian G. Montroy (IL 6283566)
2416 North Center
P.O. Box 369
Maryville, Illinois 62062
Phone: (618) 223-8200
Fax: (314) 558-9161
cmontroy@montroylaw.com

Attorneys for Plaintiffs