IN THE CIRCUIT COURT OF MACON COUNTY, ILLINOIS
COUNTY DEPARTMENT, LAW DIVISION

DANIEL BUTLER, individually and on behalf of all others similarly situated, Plaintiff, v. APPLE, INC., Defendant.	**Case No.** 2023LA1

CLASS ACTION COMPLAINT

Plaintiff Daniel Butler brings this Class Action Complaint against Defendant Apple, Inc. ("Apple" or "Defendant"), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys, as follows:

I. NATURE OF THE ACTION

1. This class action lawsuit involves violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq. ("BIPA"), an Illinois law that regulates private companies that collect, store, and use Illinois citizens' biometric data, such as fingerprints, scans of facial geometry, voiceprints, and information derived therefrom.

2. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Apple in collecting, storing, and using Plaintiff's and other

similarly situated individuals' biometric identifiers[1] without, among other violations detailed in this complaint, informed written consent in direct violation of the BIPA.

3. Biometrics refer to unique personally identifying features such as a person's facial geometry, voiceprint, fingerprint, and iris, among other features.

4. Apple is one of the most ubiquitous consumer technology product companies in the world. Apple brands itself as privacy-focused, blanketing consumers with statements like "Privacy is a fundamental human right. It's also one of our core values. Which is why we design our products and services to protect it. That's the kind of innovation we believe in."[2]:

5. Despite its avowed commitment to privacy, using a system called "HomeKit," Apple unlawfully creates a vast reservoir of biometric data that it collects from both its customers and people who pass within range of "HomeKit Secure Video" cameras with active facial

[1] "Biometric identifiers" covered by BIPA include retina or iris scans, fingerprints, voiceprints, and scans of human or face geometry, none of which can be readily changed if compromised. 740 ILCS 14/10.
[2] https://www.apple.com/privacy/ (last accessed December 22, 2022).

recognition features.[3] These cameras are known colloquialy as "smart cameras" because they utilize motion sensors, and send a notification to the device owners (an other individuals authorized by the device owner) when someone has triggered the camera's motion sensor. Unlike tradional security cameras where a video feed is sent to stationary viewing screens, the video feed from smart cameras is viewed on mobile personal computing devices, including smartphones and tablets. Some cameras have facial recognition features. Apple's HomeKit Secure Video-enabled cameras will, if the facial recognition feature has been enabled through the Apple Home app on iPhones, iPads, Apple TV, or Mac computers, Apple will scan the facial geometry of anyone within range of the camera.

6. Some HomeKit Secure Video cameras, like the Logitech Circle View Doorbell camera purchased by Plainitff, also function as doorbells, chiming when a visitor presses the doorbell button, in addition to notifying the camera owner via their iPhone or iPad that someone is at the door. The cameras scan the facial geometry of anyone who passes within view of the camera, including the customers who bought the camera, members of the customers' household, and anyone who comes within range. Apple also refers to this system of facial recognition-enabled cameras as " HomeKit Secure Video."

7. Scans of facial geometry are a type of biometric identifier pursuant to the Illinois BIPA. Scans of facial geometry may not be collected without customer consent and other compliance measures, as required by the statute. *See* 740 ILCS 14/10.

[3] Apple's HomeKit system works with numerous home appliances besides cameras, including lights, thermostats, and garage door openers. HomeKit Secure Video is the name Apple gives to cameras compatible with its HomeKit system that can perform facial scans. This action is concerned only with biometric identifiers collected by Apple using HomeKit Secure Video-compatible cameras. On Apple's iPhones, iPads, Macs, and Apple TV devices, the HomeKit app is called the "Home" app.

8. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "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." *Id.* In recognition of these concerns over the security of individuals' biometrics, the Illinois legislature enacted the BIPA to protect biometric privacy.

9. Under the Illinois BIPA, Apple was and is required, but has 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 14/15(a).

10. Under the Illinois BIPA, Apple was and is required, but fails, to inform individuals whose facial geometry it collects, captures, or otherwise obtains through its HomeKit Secure Video camera system, in writing, that their biometric identifiers or biometric information is being collected or stored. 740 ILCS 14/15(b)(1).

11. Under the Illinois BIPA, Apple was and is required, but fails, to inform individuals whose facial geometry it captures or stores using HomeKit Secure Video cameras, in writing, of the length of the term for which it will collect, store, and/or use their biometric data. 740 ILCS 14/15(b)(2).

12. Under the Illinois BIPA, Apple also was and is required, but fails, to obtain a written release from individuals whose facial geometry it captures and stores using its HomeKit

Secure Video devices. 740 ILCS 14/15(b)(3). Under the BIPA, a "written release" means "informed written consent." 740 ILCS 14/10.

13. The BIPA's compliance requirements are straightforward and easily satisfied. Nevertheless, Apple is actively collecting, storing, and using the facial scans and biometrics of many thousands of individuals in Illinois without providing those individuals with requisite notices, obtaining their informed written consent, or publishing data retention policies, all in direct violation of 740 ILCS 14/15(a) and 14/15(b).

14. Plaintiff brings this action individually and on behalf of all others similarly situated to prevent Apple from further violating the biometric privacy rights of Illinois residents, and to recover statutory damages for Apple's unauthorized, intentional, and reckless collection, storage, and use of these individuals' biometrics in violation of the BIPA.

15. On behalf of himself and all other similarly situated Illinois residents, Plaintiff Butler seeks statutory damages pursuant to the BIPA, injunctive relief, and other appropriate relief for the privacy violations set forth herein.

II. JURISDICTION AND VENUE

16. This is a class action complaint for violations of the Illinois BIPA, seeking statutory and actual damages.

17. No federal question is presented by this complaint. Plaintiff brings this complaint solely under state law and not under federal law, and specifically not under the United States Constitution, nor any of its amendments, nor under 42 U.S.C. § 1981 or 1982, nor any other federal statute, law, rule, or regulation. Plaintiff believes and alleges that a cause of action exists under state law for the conduct complained of herein.

18. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because Defendant is a corporation that transacts substantial business within Illinois and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant captured, collected, or otherwise obtained Plaintiff's and class members' biometric identifiers in Illinois.

19. Venue is proper under 735 ILCS 5/2-101 of the Illinois Code of Civil Procedure, as a substantial portion of the transactions giving rise to the claims pleaded herein occurred in Cook County, Plaintiff resides in Macon County, Illinois, and because Defendant conducts substantial business in and thus is deemed to reside in Cook County under 735 ILCS 5/2-102.

III. PARTIES

Plaintiff Daniel Butler

20. Plaintiff Butler lives in, and is a resident and citizen of, Decatur Illinois. Plaintiff's biometric identifiers were unlawfully collected by Apple by way of a HomeKit Secure Video camera installed at his home.

21. Plaintiff Butler purchased and installed a Logitech Circle View Doorbell camera, which is a HomeKit Secure Video-enabled camera, as his smart home camera in or about January, 2022. He purchased the camera from Apple, through Apple's Store App, and paid $199.95

22. After being appropriately set-up on the Home app, the camera collected scans of facial geometry without the proper disclosures regarding retention, purpose, and deletion. Nor did Apple obtain (or even ask for) a written release from Plaintiff prior to collecting his facial geometry. Accordingly, Plaintiff has been harmed.

Defendant Apple, Inc.

23. Defendant Apple, Inc. is a Cupertino, California-based corporation and technology product company. Apple is publicly traded under the stock symbol APPL, and is one of the most profitable company in the world with a market capitalization exceeting 2 trillion.

IV. FACTUAL ALLEGATIONS

A. Background on Biometric Information and the BIPA

24. Biometric data is extremely sensitive. Facial recognition technology increasingly is being used by businesses, giving rise to concerns for biometric privacy and the capturing, storing, and use of biometric identifiers in the commercial context.

25. There are two main classes of biometrics data that can be collected from individuals: (1) behavioral characteristics and (2) physiological characteristics. Behavioral characteristics concern the behavior of an individual, while physiological characteristics concern the shape or composition of the individual's body. Behavioral biometrics include an individual's keystroke, signature, and voice recognition. Physiological biometrics include facial recognition, fingerprint scanning, hand geometry, iris scanning, and DNA. Facial recognition systems use an individual's physiological information, such as facial structure, eye color, size, and shape.[4]

26. Biometric identifiers come in a variety of forms, including fingerprints, palm prints, iris/retinal scans, and scans of the facial geometry (facial recognition), which are unique to each person. There is a critical need for protecting and securing biometric identifiers because biometric identifiers:

- create a specific link between an individual and a data record;

[4] Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589, 589–92 (2018).

- can be used to create fake digital identities for fraudulent purposes;
- create a form of identification which is not exchangeable; and
- are immutable, and, if compromised by, for example, hacking, the biometric identifiers cannot be changed.

27. Consumer businesses, like Defendant, can use biometric identifiers to identify consumers and link data to that consumer, including linking a consumer's biometric identifier to methods of payment, such as their credit cards and debit cards. The result is the creation of a vast repository of information (consumer purchasing history, purchasing habits, medical history for services paid with that credit card, etc.) that is tied to customer biometric information.

28. "Verification and identification are the two ways in which an individual's identity can be determined using biometric technology. Verification confirms that a person is indeed who they claim to be and performs a one-to-one comparison of the individual's [biometric] sample with a stored reference template. Identification, on the other hand, performs a one-to-many comparison to confirm an individual's identity. The identification process compares the individual's [] sample against all the reference templates stored on file. An individual is positively identified if the individual's [] image matches any of the stored templates."

29. Legislatures have correctly identified that the privacy rights tied to biometric identifiers is a worthy right warranting statutory protection. As such, state legislatures and city councils across the country have either passed or are considering passing biometric privacy statutes in order to protect the privacy rights of their constituents.

30. In 2008, prior to the passage of BIPA, the Illinois legislature stated the following in their findings regarding the collection of biometric information by private businesses, "[t]he use of biometrics is growing . . . . The full ramifications of biometric technology are not fully known.

The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." *Illinois House Transcript*, 2008 Reg. Session No. 276.

31. As such, BIPA, the Biometric Information Privacy Act (740 ILCS 14/1, *et seq*.), was passed by the Illinois legislature in 2008 because biometric identifiers can function as a unique digital "fingerprint" or set of data that allows the subject to be identified by various types of biometric scanning. Per the statute, a "biometric identifier," which is what is collected by a biometric scanner – like a camera, or a digital fingerprint collector – "means a retina, iris scan, a fingerprint, a voiceprint, or a scan of the hand or facial geometry." Additionally, under the statute, "biometric information" is defined as "any information, regardless of how it is captured, converted, stored, or based on an individual's biometric identifier to identify an individual. 740 ILCS 14/5. The biometric identifier at issue in this case is a scan of face geometry, which Apple performs using its HomeKit Secure Video system.

32. Because people cannot change their biometric identifiers, they will *always* be identifiable by biometric scanner.

B. Illinois' Biometric Information Privacy Act

33. The Illinois BIPA establishes standards of conduct for private entities that collect or possess biometric identifiers and biometric information. This legislation was enacted 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.

34. The Illinois General Assembly noted that the BIPA was carefully crafted to protect biometric data because "unlike other unique identifiers that are used to access finances or other sensitive information," one's own biometric information cannot be changed; "[t]herefore, 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.

35. The BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . 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)(1)-(3).

36. The Illinois BIPA, 740 ILCS 14/15(a), also provides:

> 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.

740CS 14/15(a).

37. BIPA also provides that "[n]o 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).

38. "Biometric identifiers" covered by BIPA include retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry, none of which can be altered by the individual if compromised. 740 ILCS 14/10.

39. "Biometric information" covered by BIPA includes "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.*

40. BIPA provides for a private right of action: "Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." 740 ILCS 14/20.

41. The Illinois Supreme Court has explained that a person whose biometric identifiers are the subject of violations of section 15 of BIPA is "aggrieved" by the entity's failure to comply with BIPA and is "entitled to seek recovery" under Section 14/20. *Rosenbach v. Six Flags Ent. Corp.,* 2019 IL 123186, 129 N.E.3d 1197, 1206 ("[W]hen a private entity fails to comply with one of section 15's requirements, 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. Consistent with the authority cited above, such a person or customer would clearly be 'aggrieved' within the meaning of section 20 of the Act (*id.* § 20) and entitled to seek recovery under that provision. No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action.").

42. Under the Illinois BIPA, "[a] prevailing party may recover *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." *Id.* (emphasis added).

43. Under the Illinois BIPA, each instance of collecting, capturing, or obtaining a person's biometric data without consent constitutes a separate violation for which recovery can be had. *See Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 732–34 (N.D. Ill. 2020) ("[The statutory] text is unambiguous and therefore dispositive. A party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection. . . . In sum, the Court concludes that [the plaintiff] has alleged multiple timely violations of both Section 15(b) and Section 15(d). According to BIPA Section 20, she can recover 'for each violation.' 740 ILCS 14/20.").

44. This Action alleges that the Defendant, Apple, violated BIPA each and every time it scanned the facial geometry of Plainitff, and anyone that came within range of the HomeKit enabled camera purchased by Plaintiff (the Logitech Circle View Doorbellcamera) while the Homekit-enable camera's facial recognition feature was operating.

C. Apple, the HomeKit Secure Video Cameras, and the Collection of Biometric Information and Identifiers

45. Defendant Apple, a Cupertino, California based corporation, is one of the biggest technology companies in the world.

46. Apple designs, manufactures, and markets smartphones, personal computers, tablets, wearables, and accessories, and sells a variety of related services. These products are part of the same software ecosystem, often called the "iOS" ecosystem, which means that they all run on Apple's unique operating system that operates across these various types of technology

products. Apple's iOS operated devices include the ubiquitous iPhone smartphone, and its popular tablet, the iPad. Apple brands itself as privacy-centric, and in this way seeks to distinguish itself from other companies selling smartphones, tablets, and other personal computing devices.

47. As explained by Apple, HomeKit is essentially an operating software and control center that works with many home accessories, including cameras. The accessories themselves are, for the most part, manufactured by third parties, such as Logitech. The HomeKit compatible devices must be part of Apple's "MFi Program" through which Apple "offers a broad range of wireless and wired technologies that can be used in accessories that [the third party manufacturer] plans to develop or manufacture."[5] The MFi Program gives third parties access to technological specifications, and resources necessary to create Apple-compatible products. Apple describes HomeKit as follows:

> The HomeKit framework enables your app to coordinate and control supported smart home accessories from multiple vendors to present a coherent, user-focused interface. Learn how your apps on iOS, iPadOS, macOS, watchOS, and tvOS can seamlessly integrate with supported accessories.[6]

48. One such smart home product that can be linked to HomeKit is the Logitech Circle View Doorbell camera purchased by Plaintiff. The camera is manufactured by Logitech, not Apple, but the camera requires Apple's HomeKit to work as intended. The facial recognition feature of the camera, and the biometric identifiers collected with it, are collected, stored, controlled, and used by Apple through HomeKit. Once the Logitech Circle View Doorbell cameras are set up, they offer an additional technological feature: facial recognition. After the release of

[5] https://mfi.apple.com/ (last accessed December 29, 2022).
[6] https://developer.apple.com/apple-home/ (last accessed December 29, 2022).

iOS software update 14, any HomeKit Secure Video camera can be used with Apple's HomeKit facial recognition feature.[7]

49. Currently, there are 27 HomeKit Secure Video cameras that perform facial recognition scans utilizing Apple's system; these models are identified by Apple on its website: Aqara Camera Hub G2H, Aqara Camera Hub G3, Arlo Baby 1080p HD Monitoring Camera, Arlo Pro 2 Wire-Free HD Security Camera, Arlo Pro 3 Floodlight Camera, Arlo Pro 3 Wire-Free 2K Security Camera, Arlo Po Wire-Free HD Security Camera, Arlo Ultra Wire-Free Security Camera, D-Link Omna 180 CAM HD, ecobee SmartCamera with voice control, eufySecurity eufyCam 2 series, eufySecurity eufyCam 2C series, eufySecurity Indoor Cam 2K, eufySecurity Indoor Cam 2K Pan and Tilt, Eve Cam - Secure Indoor Camera, Kidde RemoteLync Camera with RemoteLync bridgeAnnounced, Logitech Circle 2, Logitech Circle View Camera, Netatmo Smart Indoor Camera, Netatmo Smart, Outdoor CameraAnnounced, Onvis Smart Camera C3, Somfy Indoor Camera, Somfy One, Somfy One Plus, Somfy Outdoor Camera, WACIAO Jupiter One 360 Zorachka - Homam 64GB.[8]

50. In addition to the foregoing, HomeKit Secure Video cameras also include several "doorbell cameras," including the Logitech model purchased by Plaintiff. Apple identifies the following 4 doorbell cameras as compatible with HomeKit Secure Video: Logitech Circle View Doorbell, Netatmo Smart Video Doorbell, Robin ProLine Doorbell, and Yobi Video Doorbell B3.

51. The Logitech Circle View Doorbell camera is available at many retailers, including Apple. On its website, Apple states that the camera was "Developed exclusively for Apple

[7] Alessandro Eric Russo, *Logitech Circle View: now with activity zones and face recognition*, AI Time Journal (Apr. 21, 2021), https://www.aitimejournal.com/@alessandro.eric.russo/logitech-circle-view-now-with-activity-zones-and-face-recognition.
[8] https://www.apple.com/home-app/accessories/#section-cameras (last accessed Dec. 29, 2022).

HomeKit. Enjoy a seamless viewing experience with two-way audio in the Home app on iPhone, iPad, Apple Watch, Mac, and Apple TV."[9] In addition, the camera is described as follows:

> Present a smarter welcome with the Logitech Circle View Wired Doorbell. Circle View Doorbell is an easy-to-use video doorbell featuring HomeKit Secure Video with Face Recognition, best-in-class Logitech TrueView™ video, a 160° field of view with head-to-toe HD optics, and color night vision. Designed to fit any home, the seamless glass face and slim silhouette add a touch of elegance and intelligence to your entrance.[10]

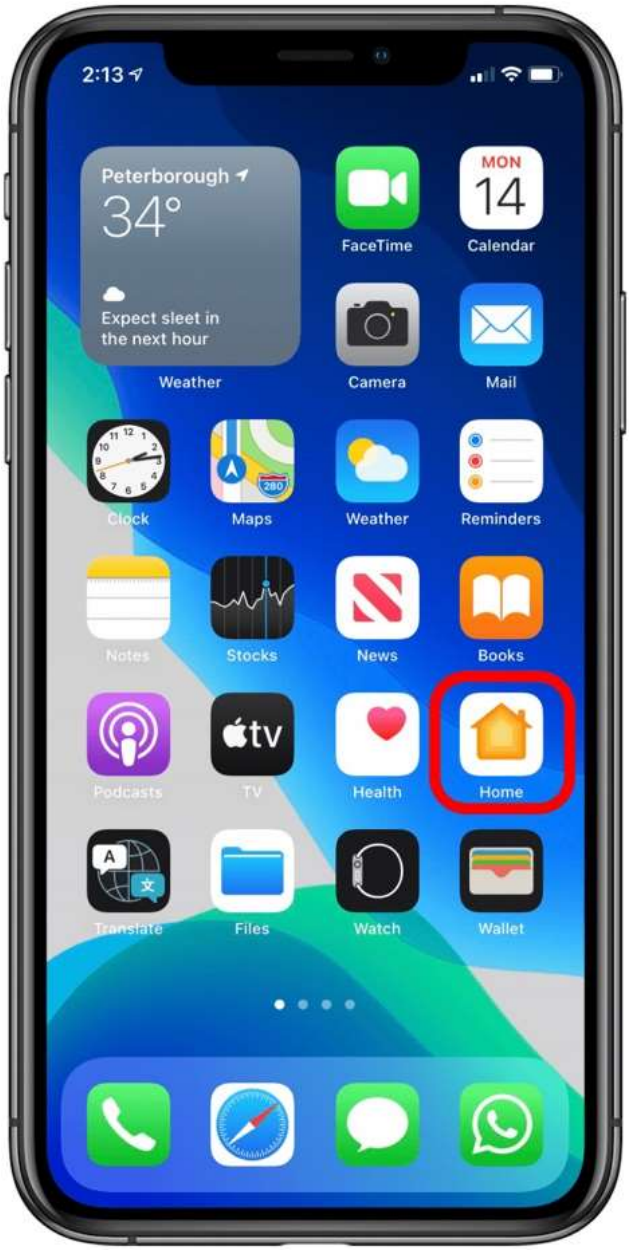
52. HomeKit Secure Video cameras allow the owner of the camera to see the camera feed on their Apple devices including iPhones and iPads, and to receive notifications on these devices when a person, a vehicle, or even an animal comes to the door, or, if it is not installed near an entrance, anyone that otherwise comes within the camera's range. Plainitff installed his Circle View Doorbell camera at the front door of his home in Decatur, Illinois.

53. Apple collects facial recognition data from customers that utilize HomeKit's facial recognition feature, and unwitting persons who have their facial images collected by a HomeKit Secure Video camera. HomeKit Secure VideoApple then creates a database of faces that can be identified by name within the HomeKit app.

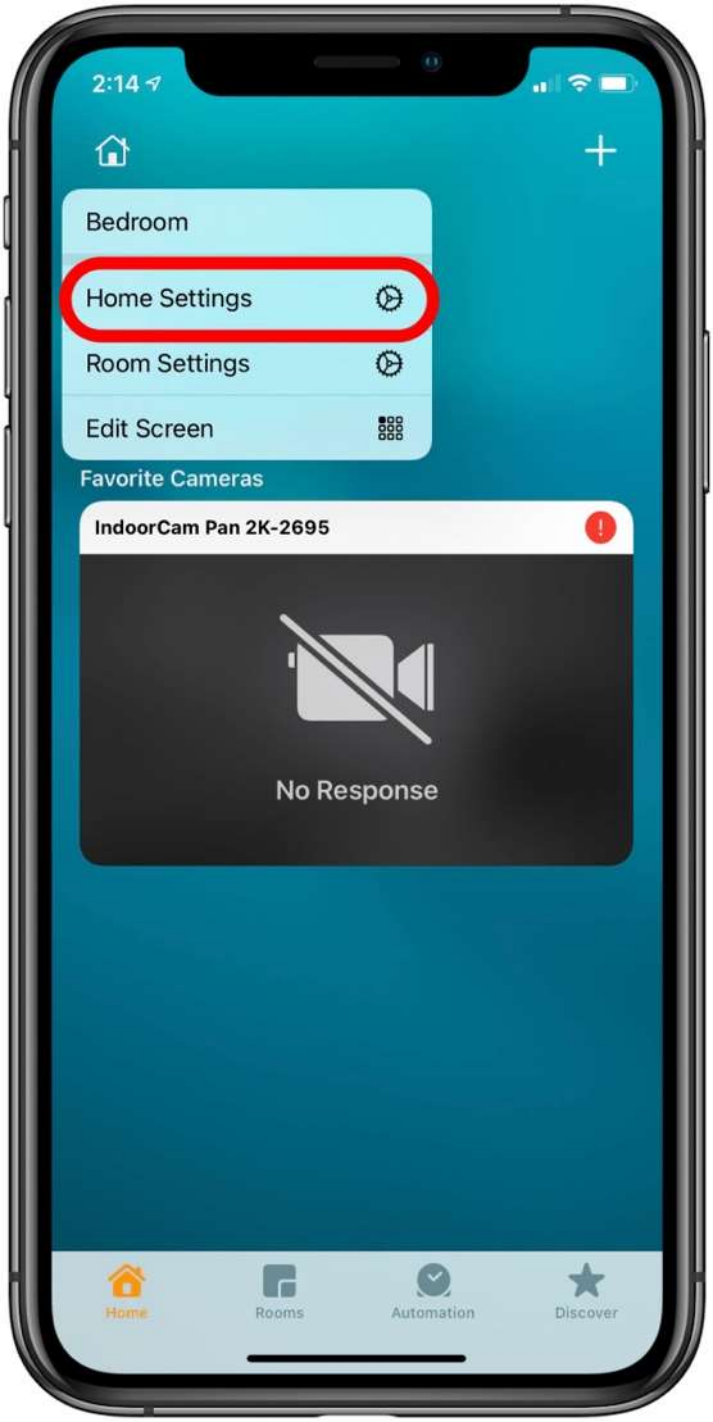
54. HomeKit's facial recognition feature is enabled as follows[11]:

[9] https://www.apple.com/shop/product/HPGS2VC/A/logitech-circle-view-wired-doorbell (last accessed December 29, 2022).
[10] *Id*.
[11] Amy Spitzfaden-Both, *Face Recognition: Level Up Your HomeKit Security*, iPhoneLife (Feb. 11, 2021), https://www.iphonelife.com/content/face-recognition-level-your-homekit-security.

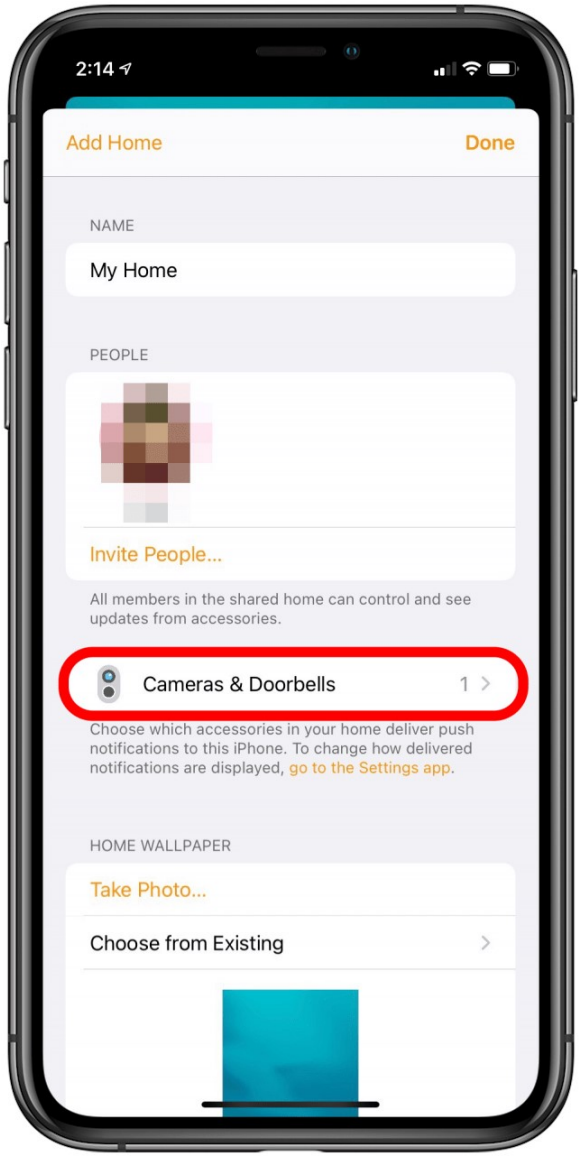
a. The User opens the “Home” app on their iPhone, iPad, Mac, or Apple TV:



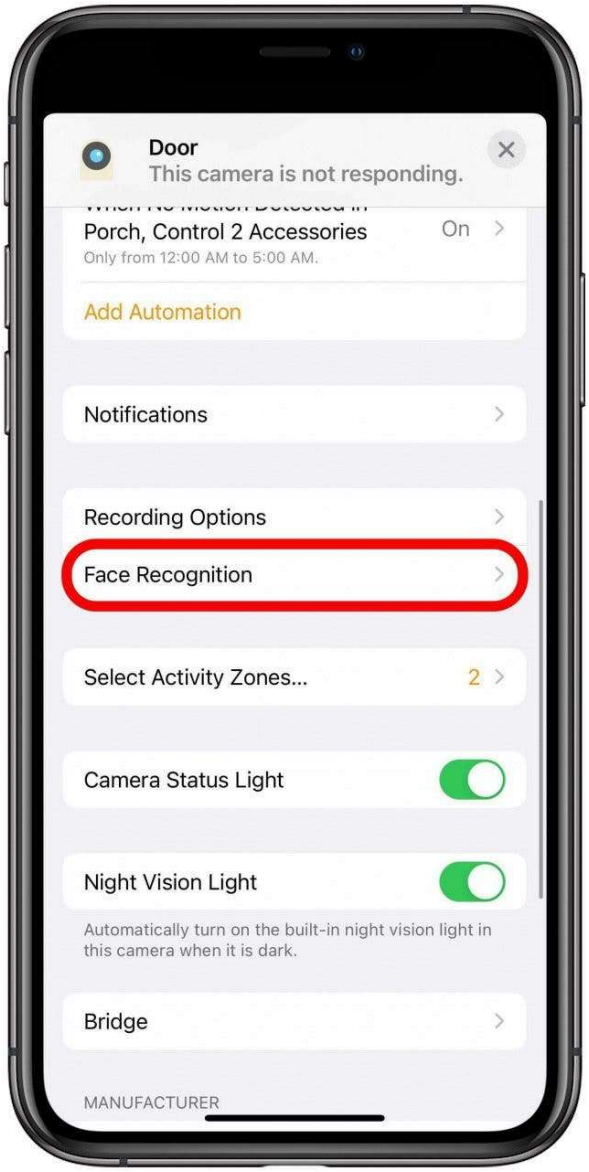
b. The User accesses “Home Settings”:



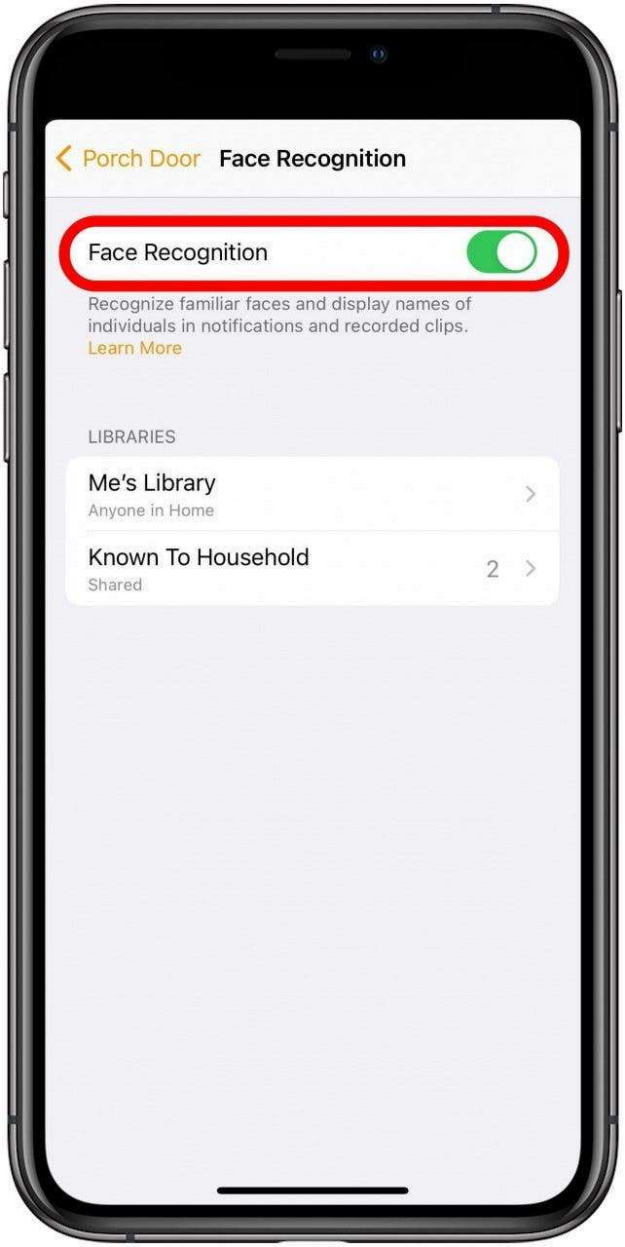
c. The User Selects “Cameras & Doorbells”:



d. The User Selects “Face Recognition”:



e. The User Turns on “Face Recognition”:



55. Plaintiff activated the facial recognition features on Apple’s Home app, and observed that Apple was scanning faces of people who came near his front door, seiding him a pop-up notification on his iPhone when this occurred.

56. In addition, at the time the user sets up the HomeKit, they provide Apple with their name, email address, and other personally identifiable information ("PII"). Accordingly, Apple can pair the User's facial scan with PII thus making Apple capable of determining users' identities.

57. In direct contravention to BIPA, there are no releases when the user turns on facial recognition through the Apple Home app. Apple fails to disclose that it is collecting scans of facial geometry, does not make available to the public a retention schedule or the purpose for which their information is being collected, and does not get written releases from the subjects of the data collection or from their legal representatives – all of which are violations of BIPA.

58. HomeKit collects the facial template data of each face photographed or otherwise collected by the camera that has facial recognition enabled.[12]

59. All of this allows Apple to collect a massive amount of facial geometry data without the proper consent or even knowledge by the subjects to pass by the camera. This is invasive and violates biometric privacy.

60. Apple's collection of facial recognition data through HomeKit Secure Video cameras fundamentally violated and continues to violate the privacy rights of Illinois residents because it collects their highly sensitive biometric information for little other utility other than to add to Apple's deep reservoir of harvested biometric data, off of which Apple profits.

V. CLASS ALLEGATIONS

61. Plaintiff seeks to certify a class of persons who fall under the following definition (collectively, the "Class"):

> **Class Definition.** All Illinois residents who had their biometric identifiers, in the form of scans of their facial geometry, collected, captured, received, or otherwise obtained by Apple through a HomeKit Secure Video camera.

[12] *Id.*

62. Excluded from the Class are: (1) the Judges presiding over the action, class counsel, and members of their families; (2) Apple, its subsidiaries, parent companies, successors, predecessors, and any entity in which Apple or its parents have a controlling interest, and any of Apple's current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

63. Numerosity: Members of the class are so numerous that their individual joinder is impracticable. While records adequate to identify the number of putative Class members are within Apple's possession, on information and belief, the proposed class includes many thousands of persons in the state of Illinois.

64. Typicality: Plaintiff's claims are typical of Class members' claims. Plaintiff and all Class members were injured through Apple's uniform misconduct, namely its violations of the Illinois BIPA, and Plaintiff's claims are identical to the claims of the Class members they seek to represent. Accordingly, Plaintiff's claims are typical of Class members' claims.

65. Adequacy: Plaintiff's interests are aligned with the Class he seeks to represent, and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged biometric and data privacy violations. Neither Plaintiff nor his counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff is able to fairly and adequately represent and protect the interests of such a Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. The Class's interests are well-represented by Plaintiff and undersigned counsel.

66. Superiority: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class member's claims. The injury suffered by each

individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class members individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

67. Commonality and Predominance: There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member include, but are not limited to, the following:

(a) whether Apple collected or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

(b) whether Apple properly informed Plaintiff and the Class that it collected, used, and stored their biometric identifiers or biometric information;

(c) whether Apple obtained a "written release" (as defined in 740 ILCS 1410) to collect, use, and store Plaintiff's and the Class's biometric identifiers or biometric information;

(d) whether Apple developed 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 their last interaction, whichever occurs first;

(e) whether Apple used Plaintiff's and the Class's biometric identifiers or biometric information to identify them;

(f) whether Apple's conduct violates the Illinois BIPA;

(g) whether Apple's violations of the BIPA were committed willfully or recklessly, or alternatively, negligently;

(h) whether Apple profited from Plaintiff's and Class members' biometric identifiers and information; and

(i) whether, as a result of Apple's violations of the BIPA, Plaintiff and members of the Class are entitled to damages (and if so, in what amount), injunctive relief, or other relief.

68. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*
(On behalf of Plaintiff and the Class)

69. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

70. The BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a

biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . 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 . . . ." 740 ILCS 14/15(b)(1)-(3).

71. Apple is a California corporation and is a "private entity" under the BIPA. *See* 740 ILCS 14/10.

72. Plaintiff and Class members are individuals who had their "biometric identifiers" collected, captured, received, or otherwise obtained by Apple through HomeKit Secure Video cameras. *See* 740 ILCS 14/10.

73. Plaintiff and Class members are individuals who had their "biometric information" collected by Apple through Apple's collection and use of their "biometric identifiers," specifically Apple collected, stored, and possessed scans of Plaintiff and Class Members' facial geometry.

74. Apple failed (and fails) to inform Plaintiff or the Class in writing that their biometric identifiers and/or biometric information are or were being "collected or stored," as required by and in violation of 740 ILCS 14/15(b)(1).

75. Apple failed (and fails) to inform Plaintiff or Class members in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being "collected, stored and used," as required by and in violation of 740 ILCS 14/15(b)(2).

76. Apple collected, obtained, used, and stored Plaintiff's and Class members' biometric identifiers and/or biometric information without first obtaining the written release, as required by and in violation of 740 ILCS 14/15(b)(3).

77. In addition, Apple possesses scans of facial geometry of Plaintiff and Class members but does not publicly provide a retention schedule or guidelines for permanently destroying the biometric identifiers, or explain the purpose of such collection and possession, as required by and in violation of 740 ILCS 14/15(a).

78. Each time Plaintiff and the other Class members had their facial geometry scanned on a HomeKit Secure Video camera, Apple captured, collected, obtained, stored, and/or used Plaintiff's and Class members biometric identifiers (scans of their facial geometry) without valid consent and without complying with, and thus in violation of, the Illinois BIPA.

79. Apple knew, or was reckless in not knowing, that the biometric technology it utilizes and which, on information and belief, many thousands of individuals within Illinois interacted with, would be subject to the provisions of the Illinois BIPA, yet it failed to comply with the statute. In the alternative, Apple negligently failed to comply with the Illinois BIPA.

80. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Apple violated the rights of Plaintiff and each Class member to keep private these biometric identifiers and biometric information, as set forth in BIPA.

81. Individually and on behalf of the proposed Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Apple to comply with the Illinois BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) statutory damages of $5,000.00 for the intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000.00 pursuant to 740 ILCS 14/20(1) if the Court finds that Apple's violations were negligent; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Butler, individually and on behalf of the proposed Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing their undersigned counsel as Class Counsel;

B. Declaring that Apple's actions, as set forth herein, violate the Illinois BIPA, 740 ILCS l4/1, *et seq.*;

C. Awarding statutory damages of $5,000.00 for each and every intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000.00 pursuant to 740 ILCS 14/20(1) if the Court finds that Apple's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an order requiring Apple to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees pursuant to 740 ILCS 14/20(3);

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

Dated: January 5, 2023

Respectfully Submitted,

By: */s/ Gary M. Klinger*

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Andrei V. Rado (*pro hac vice* to be filed)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Telephone: (212) 594-5300
Email: arado@milberg.com

Andrew W. Ferich (*pro hac vice* to be filed)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Robert Ahdoot (*pro hac vice* to be filed)
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Attorneys for Plaintiff and the Class