IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

DEBORAH ZALUDA, CATHERINE COOKE, DAVID COOKE, JAMES COOKE, LORI COOKE, SAVANNA COOKE, and PAUL DARBY, individually and on behalf of all others similarly situated,	
Plaintiffs,	No. 2019-CH-11771
v.	JURY TRIAL DEMANDED
APPLE INC.,	Hon. Michael T. Mullen
Defendant.	

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Deborah Zaluda, Catherine Cooke, David Cooke, James Cooke, Lori Cooke, Savanna Cooke, and Paul Darby (collectively "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class"), brings the following Class Action Complaint pursuant to Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Apple Inc. ("Apple" or "Defendant") to redress and curtail Defendant's unlawful collection, capture, use, and storage of Plaintiff's biometric data. Plaintiffs allege upon knowledge as to themselves and their own acts and experiences, and upon the investigation of counsel, and upon information and belief as to all other matters against Defendant as follows:

NATURE OF THE ACTION

1. This action arises from Apple's unlawful collection, capture, retention, and disclosure of individuals' biometric information in Illinois from approximately September 19, 2014 to the present (the "Class Period) in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/, *et seq.* The conduct complained of in this action occurred primarily and substantially in Illinois.

2. Apple is a leading technology company that designs and manufactures internet technology devices used by consumers worldwide. Apple designs and manufactures smartphones (iPhone), tablet computers (iPads), wearable technology (Apple Watch), laptop computers (MacBook), desktop computers (iMac), and more. Apple also designs and develops software, including operating systems and other programs for each of its devices.

3. Siri is an artificial intelligence-driven software program developed by Apple that allows individuals to, *inter alia*, use their voice to retrieve information from the internet, interact with internet-connected devices ("Smart Devices"), place calls, send texts, and schedule reminders. Apple preloads Siri on devices it designs and manufactures, including Apple's iPhone smartphones, iPad tablets, Apple Watches, AirPod headphones, HomePod smart speakers, MacBook laptops, and iMac computers ("Siri Devices").

4. Before an individual can use a Siri Device, Siri asks the user to repeat a set of five phrases. Siri records the individual as she or he utters the phrases and analyzes the unique features of the speaker's voice. Apple calls this process "User Enrollment." Siri also records and analyzes the user's first forty requests in the same way and stores the resulting data. Apple refers to this dataset as a "User Profile." These User Profiles are voiceprints.

5. The Illinois Biometric Information Privacy Act, 740 ILCS 14/, *et seq*. ("BIPA") regulates the collection, capture, retention, and dissemination of biometric identifiers and biometric information by private entities such as Apple. Pursuant to BIPA, biometric identifiers specifically include voiceprints. Biometric information is defined by BIPA as information based on an individual's biometric identifier used to identify an individual.

6. BIPA prohibits a private entity such as Apple from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining an individual's biometric information or biometric identifier 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.

7. BIPA also prohibits private entities from sharing an individual's biometric identifier or biometric information unless:

(1) The subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) The disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) The disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

8. BIPA also requires companies in possession of biometric identifiers or biometric information to develop and make available to the public a written policy 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. Private entities are required by BIPA to comply with such written policy.

9. Apple collects, captures, stores and disseminates voiceprints of each individual who uses Siri. Apple does not inform Siri users prior to or after User Enrollment that it will capture, collect, store, and/or disseminate their voiceprints, and does not obtain Siri user consent to such capture, collection and storage of their voiceprints, as BIPA requires.

10. Additionally, Apple has not developed or made available to the public or implemented and complied with a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information (*i.e.*, voiceprints of each individual who uses Siri) 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, in violation of BIPA.

11. Accordingly, Plaintiffs, on behalf of themselves as well as the putative Class, seeks an order: (1) declaring that Apple's conduct violates BIPA; (2) requiring Apple to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiffs and the proposed Class.

12. Upon information and belief, given the concealed and secretive nature of Apple's conduct, more evidence supporting the allegations in this complaint will be uncovered after a reasonable opportunity for discovery.

JURISDICTION AND VENUE

13. This Court has jurisdiction over Apple pursuant to 735 ILCS § 5/2-209 because Apple conducts business in Illinois, committed the statutory violations alleged herein in Cook County and throughout Illinois, and is registered to and does conduct business in Illinois.

14. Venue is proper in Cook County because Apple conducts business in this State, conducts business in Cook County, and committed the statutory violations alleged herein in Cook County and throughout Illinois.

PARTIES

A. Plaintiffs

15. Plaintiff Deborah Zaluda is a natural person and is a resident and citizen of the State of Illinois.

16. Plaintiff Catherine Cooke is a natural person and was, at the material times described herein, a resident and citizen of the State of Illinois.

17. Plaintiff David Cooke is a natural person and is, and at all material times during the Class Period has been, a resident and citizen of the State of Illinois.

18. Plaintiff James Cooke is a natural person and is, and at all material times during the Class Period has been, a resident and citizen of the State of Illinois.

19. Plaintiff Lori Cooke is a natural person and is, and at all material times during the Class Period has been, a resident and citizen of the State of Illinois.

20. Plaintiff Savanna Cooke is a natural person and was, at the material times described herein, a resident and citizen of the State of Illinois.

21. Plaintiff Paul Darby is a natural person and is, and at all material times during the Class Period has been, a resident and citizen of the State of Illinois.

B. Defendant

22. Defendant Apple Inc. is a business incorporated under the laws of the State of Delaware with its principal place of business in Cupertino, California. At all times mentioned herein, Apple has been engaged in the State of Illinois in the business of designing, manufacturing, distributing, and selling, *inter alia*, smartphones, tablet computers, wearable computers, headphones, laptops, and desktop computers that come with software Apple develops pre-installed.

FACTUAL BACKGROUND

I. Biometric Identifiers and Biometric Data

23. Biometrics is the measurement and analysis of unique physical or behavior characteristics. Biometric data is frequently used to identify individuals, for example through the use of fingerprint scans, facial recognition, or voice patterns. A dataset that corresponds to a person's unique physical or behavioral characteristic that is used for identification purposes, (*e.g.*, data corresponding to a fingerprint, voice pattern, retina, or facial features) is commonly referred to as a "biometric identifier."

24. Despite consumers' ever-growing concerns with privacy, the use of biometric data by private companies is accelerating, with much of this growth attributable to the increased capability of smartphones and other internet-connected devices to capture and collect an individual's biometric data.

25. Since an individual's physical characteristics cannot be easily changed (if at all), the use of biometric identifiers has serious implications for an individual's privacy. An entity that obtains possession of an individual's biometric identifier is able to track that individual wherever a device capable of capturing biometric identifiers is present. Additionally, because

many financial institutions and healthcare providers use biometric identifiers for authentication, possession of a person's biometric identifier can provide access to an individual's bank accounts or medical records.

II. The Illinois Biometric Information Privacy Act

26. In recognition of the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information[,]"[1] the Illinois General Assembly passed the Biometric Information Privacy Act, 740 ILCS 14/ ("BIPA") in 2008. Because biometric identifiers cannot be changed if they are compromised or misused, the General Assembly has provided citizens of Illinois, through the protections afforded by BIPA, the ability – and statutory right – to control their biometric identifiers and biometric information by requiring private companies to obtain their consent before creating and collecting such identifiers and information, including the right to prevent such creation and collection by refusing to withholding consent.

27. In enacting BIPA, the General Assembly recognized that the full extent of the damage that can result from the compromise or misuse of an individual's biometric data cannot be ascertained in advance. The General Assembly thus sought to head off such problems before they occur by imposing safeguards to protect individuals' privacy rights in their biometric identifiers and biometric information.

28. BIPA ensures that individuals' privacy rights in their biometric identifiers and biometric information are protected by making it unlawful for a private company to "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;

[1] Illinois House Transcript 2008 Reg. Sess. No. 276.

> (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."[2]

29. BIPA's definition of "biometric identifiers" expressly includes a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[3]

30. BIPA further protects consumer's right to privacy in their biometric identifiers and biometric information by making it unlawful for a private entity to "disclose, redisclose, or otherwise disseminate" an individual's biometric identifier and/or and biometric information unless:

> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
>
> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.[4]

31. BIPA further requires private entities in possession of biometric identifiers or biometric information to:

> develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for

[2] 740 ILCS 14/15 (b).

[3] 740 ILCS 14/10 (emphasis added).

[4] 740 ILCS 14/15 (d).

> 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.[5]

32. BIPA further provides that, absent a valid warrant or subpoena, a private entity in possession of biometric identifiers or biometric information "must comply with its established retention schedule and destruction guidelines."[6]

33. The General Assembly intended the relief provided to aggrieved individuals to have substantial force by subjecting private entities that fail to comply with BIPA to liability, including statutory damages, to prevent unforeseen problems that cannot be undone before they occur. Thus, private entities that fail to adhere to the safeguards imposed by BIPA are subject to statutory damages, injunctions, attorneys' fees, and litigation expenses for each violation of BIPA.[7] In particular, BIPA provides for statutory damages for each violation as follows:

> (1) $1,000 or actual damages, whichever is greater, for negligent violations; or
>
> (2) $5,000 or actual damages, whichever is greater, for intentional or reckless violations.[8]

III. Apple and Siri

34. Apple is an internet technology company that designs and manufactures consumer devices used by billions of consumers worldwide. Apple designs, manufactures, and sells computer technology such as smart phones (iPhone), tablet computers, (iPad), smart speakers (HomePod), music players (iPod), laptops (MacBook), desktop computers (iMac), wearable

[5] 740 ILCS 14/15 (a).

[6] *Id*.

[7] 740 ILCS 14/20.

[8] *Id*.

devices (Apple Watch), headphones (AirPods), and more (*e.g.*, iPod touch, AirPod headphones, CarPlay, Apple Watch, and Apple TV).

35. Apple also develops operating system software for their consumer devices, including: iOS (iPhone, iPad, and iPod), watchOS (Apple Watch), macOS (iMac and MacBook), tvOS (Apple TV), and audioOS (HomePod). Each of these operating systems includes a feature known as Siri.

36. Apple has developed three "biometric authentication" features that use individuals' biometric identifiers to provide access to devices or device features: Touch ID (fingerprint), Face ID (facial scans), and Siri (voiceprints). Apple's Touch ID feature allows users to access an Apple device using his or her fingerprint. Touch ID first "enrolls" a user – through notice and consent – by scanning his or her fingerprint and creating "mathematical representation" of the user's fingerprint and storing it. The device can then be unlocked when a fingerprint scan generates a mathematical model that matches the model stored on the phone during user enrollment.

37. Similarly, Apple's Face ID allows users to secure their phones using geometric scans of their face. Like Touch ID, Face ID requires user enrollment (through notice and consent). To enroll, a user must go through a sequence of facial "poses" which are captured by the device's camera. The captured poses are converted into a "mathematical representation of [the user's] face[.]" Subsequently, the device can be unlocked when the mathematical representation of an individual looking into the camera of the device matches the mathematical representation created and stored during user enrollment.

38. Apple refers to both Touch ID and Face ID as "biometric authentication" in literature written for iOS application developers and encourages developers to incorporate biometric authentication into their applications.

39. In contrast to Touch ID and Face ID, Apple has not disclosed to individuals that Siri's user enrollment process results in the creation, collection, and storage of users' biometric voiceprint identifiers. Nor has Apple obtained consent.

40. Siri is a voice-activated virtual personal assistant feature that is included with devices running Apple operating systems iOS, watchOS, macOS, tvOS, and audioOS. Siri uses the internet to help users with a variety of tasks, including providing users with information in response to questions, play music, and interact with other internet-connected devices, among other things.

41. Siri has been pre-installed on devices running iOS since October 12, 2011, but initially could only be used when the user pressed the device's home button. Apple introduced a voice-activated "wake" feature for Siri, utilizing a voice command, with the launch of iOS8 and the iPhone 6 on September 19, 2014. Today, Siri is an operating system feature on the following Apple devices: iPhone, iPad, iPod touch, AirPod headphones, CarPlay, Apple Watch, HomePod, iMac, MacBook, and Apple TV.

42. Since September 19, 2014, users have activated Siri through the utterance of the pre-programmed wake phrase "Hey Siri" or by a physical gesture such as the pushing of the home button or a wrist movement. In order to recognize the utterance of a wake phrase, Siri Devices' speech recognizer constantly records and analyzes short snippets of audio within range of the device's microphone and analyzes those clips to determine whether the wake phrase "Hey Siri" has been uttered ("Passive Listening").

43. According to Apple, when a Siri Device is in Passive Listening mode, the short audio clips that are recorded are stored locally on the Siri Device's random-access memory ("RAM") to be analyzed. These snort snippets are continuously overwritten as a Siri Device analyzes new audio clips during Passive Listening.

44. When a Siri Device determines "Hey Siri" has been uttered within range of its microphone, it "wakes up" or activates Siri. Once activated, Siri records an individual's speech to determine what Siri is being asked to do. These recordings are sent to Apple's servers for analysis to determine (1) whether the Siri Device accurately detected a wake phrase; and (2) confirm what Siri is being asked to do so Apple can respond to the command. For example, if a user says, "Hey Siri, what is the weather in Chicago?" Siri will transmit that audio to Apple for analysis. Apple analyzes audio by converting what is said into text so that Apple's computers can determine what is being requested. Users can also ask Siri to perform other tasks, such as set alarms, reminders, read text message aloud, or interact with other internet connected smart devices.

45. The development of virtual assistants that record individuals' voices has raised numerous privacy concerns. For example, some individuals have voiced concerns that rather than only activating in response to a wake phrase, virtual assistants are always recording, resulting in the recording of personal and confidential communications.

46. Apple has used its privacy practices as a marketing tool to distinguish itself from competitors such as Google, Amazon, and Facebook that have been implicated in collecting, exploiting, and sharing sensitive customer data. For example, Apple has put up billboards stating "What happens on your iPhone stays on your iPhone." Apple's CEO Tim Cook has commented

that Apple "believes privacy is a human right," and that "we also recognize that not everyone sees things as we do."[9]

47. Despite positioning itself as a privacy leader, Apple – along with Amazon, Google, Facebook, and Microsoft – was recently revealed to have shared recordings made by Siri with contractors who then listened to the conversations for purposes of evaluating Siri's performance.[10] The contractors regularly heard conversations where no wake phrase was uttered. These conversations included "private discussions between doctors and patients, business deals, seemingly criminal dealings, sexual encounters and so on."[11] These recordings were accompanied by user data showing location, contact details, app data, and more, which could allow contractors to identify the users they were listening to. Apple had represented that any recordings made by Siri were completely anonymized.

48. On information and belief, Apple has disclosed biometric information to third parties about Plaintiffs and the Class members. The conduct complained of in the Amended Class Action Complaint occurred primarily and substantially in Illinois.

[9] Ian Bogost, *Apple's Empty Grandstanding About Privacy: The company enables the surveillance that supposedly offends its values*, The Atlantic, Jan. 31, 2019, https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/ (last accessed Oct. 8, 2019).

[10] Alex Hern, *Apple contractors 'regularly hear confidential details' on Siri recordings*, The Guardian, July 26, 2019, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings (last accessed Oct. 8, 2019).

[11] *Id*.

SUBSTANTIVE ALLEGATIONS

I. Apple is Capturing, Collecting, and Disclosing Consumers' Voiceprints without Consent.

49. In developing Siri, Apple focused on developing software capable of *speech* recognition (to recognize the key phrase "Hey Siri") and *speaker* recognition (to recognize that the individual speaking is someone that has consented to be recorded).

50. According to Apple, "[t]he overall goal of speaker recognition [] is to ascertain the identity of a person using his or her voice."[12] Speaker recognition is therefore interested in "who is speaking," as opposed to "what was spoken."[13] To give Siri speaker recognition capabilities, Apple developed a process it calls "User Enrollment." When an individual first attempts to use Siri on a Siri Device, the individual is asked to repeat the following five phrases:

1. "Hey Siri"
2. "Hey Siri"
3. "Hey Siri"
4. "Hey Siri, how is the weather today?"
5. "Hey Siri, it's me."[14]

51. According to Apple, "[t]hese phrases are used to create a statistical model for the user's voice"[15] through the following process: First, Siri "converts the incoming speech utterance to a fixed-length speech (super)vector, which can be seen as a summary of the acoustic information present in the 'Hey Siri' utterance; this includes information about the phonetic content, the background recording environment, *and the identity of the speaker*."[16] Second, Siri

[12] *Personalized Hey Siri – Apple*, 1 Apple Machine Learning Journal 9, April 2018, at 4 (hereinafter "*Personalized Hey Siri*").

[13] *Id.*

[14] *Id.*

[15] *Id.* at 4.

[16] *Id.* at 6 (emphasis added).

"attempts to transform the speech vector in a way that focuses on speaker-specific characteristics and deemphasizes variabilities attributed to phonetic and environmental factors."[17]

52. Apple refers to the voice data captured and collected from the Siri User Enrollment as a "User Profile." User Profiles are voiceprints, and Apple has collected, captured, and stored the voiceprints of millions of Illinois consumers, including Plaintiffs, without acquiring informed consent in accordance with BIPA.

53. In contrast to Apple's treatment of the biometric identifiers, such as facial scans and fingerprint scans that it collects from users through notice and consent, Apple has not disclosed to individuals that Siri's user enrollment process results in the creation, collection, and storage of users' biometric voiceprint identifiers.

54. BIPA requires Apple to obtain informed consent from Siri users in writing *before it* collects an individual's voiceprint. But, contrary to BIPA, nowhere in Apple's terms of service, privacy policy, or other disclosures does Apple state it is collecting an individual's biometric identifier, biometric information, or voiceprint. This runs afoul of the intention of the Illinois General Assembly in enacting BIPA: to require private companies to explicitly state they are collecting biometric identifiers and biometric information before doing so, so that consumers can make informed decisions about whether to enter into transactions with the companies or use the companies' products.

55. BIPA also requires Apple to obtain Siri users' informed written consent before disclosing, redisclosing, or otherwise disseminating biometric identifiers and/or biometric information. According to published reports, Apple has disclosed, redisclosed, or otherwise

[17] *Id.*

disseminated user data affiliated with voiceprints to third party contractors. [18] Nowhere in its terms of service, privacy policy, or other disclosures has Apple given Siri users notice of such disclosures.

II. Apple Collected, Captured, and Stored Plaintiffs' Biometric Identifier or Biometric Information without Consent

56. As detailed below, each Plaintiff owned a Siri Device during the Class Period, went through Siri's User Enrollment, and had their voiceprint created, collected, and stored by Defendant Apple.

57. For a number of years prior hereto and to the present time, Plaintiff Deborah Zaluda has owned and used a number of Apple Devices with the Siri function, including Apple iPhones, an Apple Watch and two Apple iMac computers. At the present time (and since 2018), Plaintiff has owned and used an Apple iPhone XS with a Siri function.

58. At all times mentioned herein, Plaintiff Deborah Zaluda has been a Siri user and underwent Siri's User Enrollment and has used the Siri function on her Apple Devices. Siri has recorded her initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff Zaluda's voice, and collected, captured and stored a voiceprint of Plaintiff Zaluda's voice.

59. Plaintiff Catherine Cooke owns an iPhone XR, underwent Siri's User Enrollment, and has used the Siri function on her iPhone XR since approximately June 2019. Siri has recorded her initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff Catherine Cooke's voice, and collected, captured and stored a voiceprint of Plaintiff Catherine Cooke's voice.

[18] Alex Hern, *Apple contractors 'regularly hear confidential details on Siri recordings*, The Guardian, July 26, 2019, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings (last accessed Oct. 8, 2019).

60. Plaintiff David Cooke owns an iPhone 8, underwent Siri's User Enrollment, and has used the Siri function on his iPhone 8 since approximately November 2018. Siri has recorded his initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff David Cooke's voice, and collected, captured and stored a voiceprint of Plaintiff David Cooke's voice.

61. Plaintiff James Cooke owns an iPhone 8, underwent Siri's User Enrollment, and has used the Siri function on his iPhone 8 since approximately June 2018. Siri has recorded his initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff James Cooke's voice, and collected, captured and stored a voiceprint of Plaintiff James Cooke's voice.

62. Plaintiff Lori Cooke owns an iPhone 6, underwent Siri's User Enrollment, and has used the Siri function on her iPhone 8 since approximately March 2015. Siri has recorded her initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff Lori Cooke's voice, and collected, captured and stored a voiceprint of Plaintiff Lori Cooke's voice.

63. Plaintiff Savanna Cooke owns an iPhone 8 Plus, underwent Siri's User Enrollment, and has used the Siri function on her iPhone 8 since approximately September 2018. Siri has recorded her initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff Savanna Cooke's voice, and collected, captured and stored a voiceprint of Plaintiff Savanna Cooke's voice.

64. For a number of years prior hereto and to the present time, Plaintiff Paul Darby has owned and used a number of Apple Devices with the Siri function, including Apple iPhones (an iPhone 8 and XI) and an iWatch that he purchased for a minor family member and an Apple

iPad that he purchased for himself. At the present time, he owns and uses an Apple iPad with a Siri function and his minor family uses an iPhone XI and an iWatch.

65. At all times mentioned herein, Plaintiff Paul Darby has been a Siri user and underwent Siri's User Enrollment and has used the Siri function on his Apple Devices. Siri has recorded his initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff Darby's voice, and collected, captured and stored a voiceprint of Plaintiff Darby's voice.

66. At no point did Plaintiffs have knowledge that Apple was creating and capturing a voiceprint of their voices and collecting and storing such voiceprints. At no point did Plaintiffs consent to the unlawful collection, capture, and storage of their voiceprint. Apple did not inform Plaintiffs in writing that it was collecting, capturing, and storing their biometric identifier or biometric information, Apple did not inform Plaintiffs in writing of the specific purpose and length of term which their biometric identifier or biometric information was being collected, stored, and used, and Apple did not obtain a written release by which Plaintiffs consented to the collection, capture, and storage of their biometric identifier and biometric information as required by BIPA.

67. At no point did Plaintiffs consent to the unlawful disclosure, redisclosure, or dissemination of their biometric identifier or biometric information. Apple did not inform Plaintiffs that it was disclosing, redisclosing, or otherwise disseminating their biometric identifier and/or biometric information.

68. Apple unlawfully captured, collected and disclosed Plaintiffs' biometric identifier and biometric information, without consent, in violation of BIPA.

69. Additionally, Apple has not developed and made available to the public, nor implemented and complied with, a written policy outlining Apple's handling of Plaintiffs' biometric identifiers and biometric information as required by BIPA, and has thus violated BIPA requirements that such a policy be adopted and that Apple comply with the retention and destruction provisions of such a policy.

70. Plaintiff and the proposed Class had no way of knowing about Apple's conduct detailed herein.

71. Apple concealed that it was creating voiceprints, and that it was capturing, collecting and storing this biometric identifier of Plaintiffs and the Class members. Thus, neither Plaintiffs nor any other reasonable member of the Class could have discovered the conduct.

72. For these reasons, any statute of limitations or statute of repose that otherwise may apply to the claims of Plaintiffs of members of the Class should be tolled.

CLASS ACTION ALLEGATIONS

73. Plaintiffs bring this action pursuant the Illinois Code of Civil Procedure, 735 ILCS 5/2-801, on their own behalf and as representatives of all other similarly-situated individuals, defined as follows (the "Class"):

> All Illinois residents who used the Siri function on an Apple device and had their voiceprints collected, captured, received, or otherwise obtained and/or disseminated by Apple from September 19, 2014 to the present.[19]

74. This action is properly maintained as a class action under 735 ILCS 5/2-801 because: (1) the class is so numerous that joinder of all member is impracticable ("Numerosity"); (2) there are questions of law or fact that are common to the class ("Commonality"); (3)

[19] Plaintiff has defined the Class based on currently available information and hereby reserves the right to amend the definition of the Class, including, without limitation, the Class Period.

Plaintiff's claims are typical of the claims of the class ("Typicality"); and (4) Plaintiff will fairly and adequately protect the interest of the class ("Adequate Representation").

75. **Numerosity**. The Class likely consists of thousands, if not millions, of individuals, and the members can be identified through Apple's records. The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable.

76. **Predominant Common Questions**. The Class's claims present common questions of law and fact and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Apple has collected, captured, or otherwise obtained, stored and/or disseminated Plaintiffs' and the Class's biometric identifiers or biometric information;

b. Whether Apple properly informed Plaintiffs and the Class that it collected, captured, used, stored and/or disclosed their biometric identifiers or biometric information;

c. Whether Apple obtained a written release (as defined in 740 ILCS 14/10) to collect, capture, use, store and/or disclose Plaintiffs' and the Class's biometric identifiers or biometric information;

d. Whether Apple developed, made available to the public, and complied with a written policy, establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever comes first;

e. Whether Apple used Plaintiffs' and the Class's biometric identifiers or biometric information to identify them;

f. Whether Apple's collection, capture, storage, and/or sharing of Plaintiffs' and the Class's biometric identifiers or biometric information violated BIPA.

g. Whether Apple's failure to develop, make available to the public, and comply with a written policy, establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever comes first, violated BIPA; and

h. Whether Apple's violations of BIPA were committed intentionally, recklessly, or negligently.

77. **Typicality**. Plaintiffs' claims are typical of the claims of the other members of the proposed Class. Plaintiffs and Class members were aggrieved as a result of Apple's wrongful conduct that is uniform across the Class.

78. **Adequate Representation**. Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel that is competent and experienced in complex litigation and class actions. Plaintiffs have no interest that is antagonistic to those of the Class, and Apple has no defenses unique to Plaintiffs. Plaintiffs and Plaintiffs' counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiffs nor Plaintiffs' counsel have any interest adverse to those of the other members of the Class.

79. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. It would be unduly burdensome to the Court for each class member to pursue their claims individually. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

80. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Violation of the Illinois Biometric Information Privacy Act, 740 ILCS § 14/15(b)
Failure to Obtain Informed Written Consent and Release before
Obtaining Biometric Identifiers or Biometric Information
(On Behalf of Plaintiffs and the Class)

81. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

82. BIPA requires companies to obtain informed written consent from individuals before collecting or capturing their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] 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).

83. Apple is a "private entit[y]" pursuant to 740 ILCS § 14/10.

84. Plaintiffs and the Class are individuals who have had their "biometric identifiers" (voiceprints) collected and captured by Apple.

85. Plaintiffs' and the Class's biometric identifiers were used to identify them and therefore constitute "biometric information" as defined by 740 ILCS § 14/10.

86. Apple systematically and automatically collected, used, stored and disseminated Plaintiffs' and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

87. Apple did not inform Plaintiffs and the Class in writing that their biometric identifiers and/or biometric information were being collected, stored, and used nor did Apple inform Plaintiffs and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

88. By collecting, storing, and using Plaintiffs' and the Class's biometric identifiers and/or biometric information as described herein, Apple violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers or biometric information.

89. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Apple to comply with BIPA's requirements for the collection, capture, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CLAIM FOR RELIEF

Violation of the Illinois Biometric Information Privacy Act, 740 ILCS § 14/15(d)
Failure to Obtain Consent before Disclosing, Redisclosing,
or otherwise Disseminating Biometric Identifiers or Biometric Information
(On Behalf of Plaintiffs and the Class)

90. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

91. BIPA requires companies to obtain consent from individuals before disclosing, redisclosing, or otherwise disseminating their biometric identifier and/or biometric information. 740 ILCS 14/15(d). Apple has used Plaintiffs' and the Class's biometric identifiers to identify them and such identifiers therefore constitute "biometric information" as defined by 740 ILCS § 14/10.

92. Plaintiffs and the Class are individuals who have had their "biometric identifiers" (voiceprints) disclosed, redisclosed, or otherwise disseminated by Apple.

93. Apple did not obtain consent from Plaintiffs and the Class before disclosing, redisclosing, or otherwise disseminating their biometric identifiers and/or biometric information as required by 740 ILCS 14/15(d)(1).

94. By disclosing, redisclosing, or otherwise disseminating Plaintiffs' and the Class's biometric identifiers and/or biometric information as described herein, Apple violated BIPA.

95. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Apple to comply with BIPA's requirements for the collection, capture, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant

to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CLAIM FOR RELIEF

Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a)
Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

(On Behalf of Plaintiffs and the Class)

96. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

97. BIPA requires that private companies in possession of biometric identifiers and biometric information develop, make available to the public, and comply with a written policy setting forth 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.

98. Plaintiffs and the Class are individuals who have had their "biometric identifiers" (voiceprints) collected and captured by Apple.

99. Plaintiffs' and the Class's biometric identifiers were used to identify them and therefore constitute "biometric information" as defined by 740 ILCS § 14/10.

100. Apple systematically and automatically collected, captured, used, stored and disseminated Plaintiffs' and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

101. Apple has failed to develop, make available to the public, and comply with a written policy setting forth retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and will not destroy Plaintiffs' or the Class's biometric

data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company, in violation of BIPA.

102. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Apple to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the proposed Class respectfully request that the Court enter an order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs Deborah Zaluda, Catherine Cooke, David Cooke, James Cooke, Lori Cooke, and Savanna Cooke as Class Representatives, and appointing Silver Golub & Teitell LLP, Miller Shakman Levine & Feldman LLP, and Forde LLP as Class Counsel;

B. Declaring that Apple's actions, as set out above, violate BIPA;

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

D. Declaring that Apple's actions, as set forth above, were intentional and/or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Apple to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiffs and the Class their reasonable attorneys' fees and 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;

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: December 23, 2019

Respectfully submitted,

DEBORAH ZALUDA
CATHERINE COOKE
DAVID COOKE
JAMES COOKE
LORI COOKE
SAVANNA COOKE
PAUL DARBY

/s/ Daniel M. Feeney
One of their attorneys

Daniel M. Feeney
Zachary J. Freeman
Miller Shakman Levine & Feldman LLP
Firm ID: 90236
180 North LaSalle Street, Suite 3600
Chicago, IL 60601
Tel. (312) 263-3700
Fax (312) 263-3270
Email: dfeeney@millershakman.com
zfreeman@millershakman.com

David S. Golub (*pro hac vice*)
Steven L. Bloch (*pro hac vice*)
Ian W. Sloss (*pro hac vice*)
Silver Golub & Teitell LLP
184 Atlantic Street
Stamford, CT 06901
Tel. (203) 325-4491
Fax (203) 325-3769
Email: dgolub@sgtlaw.com
sbloch@sgtlaw.com
isloss@sgtlaw.com

Kevin M. Forde
Kevin R. Malloy
Brian P. O'Meara
Forde Law Offices LLP
111 West Washington Street
Suite 1100
Chicago, IL 60602
Tel. (312) 641-1441
Email: kforde@fordellp.com
kmalloy@fordellp.com
bomeara@fordellp.com

SUPREME COURT RULE 222(b) DAMAGES AFFIDAVIT

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that this civil action seeks in excess of $50,000 on behalf of the Plaintiff and the proposed Class.

Dated: December 23, 2019

/s/ Daniel M. Feeney
One of Plaintiffs' attorneys

Daniel M. Feeney
Zachary J. Freeman
Miller Shakman Levine & Feldman LLP
Firm ID: 90236
180 North LaSalle Street, Suite 3600
Chicago, IL 60601
Tel. (312) 263-3700
Fax. (312) 263-3270
Email: dfeeney@millershakman.com
zfreeman@millershakman.com

David S. Golub (*pro hac vice*)
Steven L. Bloch (*pro hac vice*)
Ian W. Sloss (*pro hac vice*)
Silver Golub & Teitell LLP
184 Atlantic Street
Stamford, CT 06901
Tel. (203) 325-4491
Fac. (203) 325-3769
Email: dgolub@sgtlaw.com
sbloch@sgtlaw.com
isloss@sgtlaw.com

Kevin M. Forde
Kevin R. Malloy
Brian P. O'Meara
Forde Law Offices LLP
111 West Washington Street
Suite 1100
Chicago, IL 60602
Tel. (312) 641-1441
Email: kforde@fordellp.com
kmalloy@fordellp.com
bomeara@fordellp.com

CERTIFICATE OF SERVICE

The undersigned attorney hereby certifies that he served the foregoing **AMENDED CLASS ACTION COMPLAINT** on counsel of record via e-mail on December 23, 2019:

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

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

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

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this Certificate of Service are true and correct, except as to matters therein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that he verily believes the same to be true.

/s/David S. Golub
David S. Golub