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,

v.

APPLE INC.,

Defendant.

Hon. Michael T. Mullen

No. 2019 CH 11771

APPLE INC.'S MEMORANDUM IN SUPPORT OF ITS COMBINED SECTION 2-619.1 MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

DLA Piper LLP (US)—Firm No. 43034

Isabelle L. Ord*
555 Mission Street, Suite 2400
San Francisco, California 94105
isabelle.ord@dlapiper.com

Amanda Fitzsimmons*
401 B Street, Suite 1700
San Diego, California 92101
amanda.fitzsimmons@dlapiper.com

Raj N. Shah (ARDC # 06244821)
Eric M. Roberts (ARDC # 6306839)
Matt Freilich (ARDC # 6332688)
444 West Lake Street, Suite 900
Chicago, Illinois 60606
raj.shah@dlapiper.com
eric.roberts@dlapiper.com
matt.freilich@dlapiper.com

* Appearing *pro hac vice*

Attorneys for Apple Inc.

Dated: January 24, 2020

I. INTRODUCTION

The Amended Class Action Complaint ("Complaint") speculates that Apple Inc. ("Apple") creates, collects, or disseminates "voiceprints" through the plaintiffs' interactions with Siri, in violation of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq*. Apple simply does not create, collect, or disseminate "voiceprints," and the plaintiffs' failure to state any well-pleaded facts to support their allegations is fatal to their claims; BIPA is not implicated by activity that occurs solely on users' devices. Indeed, the plaintiffs' unwarranted assumptions that Apple must be collecting and using the plaintiffs' "voiceprints" directly contradicts the very article they rely upon in the Complaint. Simply put, the Complaint lacks the factual support required at this stage and must be dismissed.

This case arises from the plaintiffs' knowing, voluntary, and intentional interaction with Siri. Siri is an optional function that the user must enable from the device. If enabled, Siri offers many beneficial features, including an optional hands-free activation function commonly known as "Hey Siri." To enable "Hey Siri," users must expressly consent to a "User Enrollment" process and speak "Hey Siri" into their devices several times, after reading on their screens that this will "help[] Siri recognize your voice when you say 'Hey Siri.'" During User Enrollment, an on-device speaker recognition system uses these utterances to train a personalized "Hey Siri" user profile, which is further refined and used by the device to identify "Hey Siri" commands. The user controls the whole process, and Apple does not have access to this user profile. Instead, the user profile remains on the user's device and simply allows Siri to recognize the "Hey Siri" command. Despite this, the plaintiffs allege that the user profile created during User Enrollment is a "voiceprint"—a biometric identifier subject to BIPA. The plaintiffs also allege that Apple collects user profiles and disseminates them to third parties without users' consent.

The Complaint must be dismissed because it relies on several unfounded logical leaps to imply a violation of BIPA where none exists. First, BIPA does not apply because the Siri user profile is not a "voiceprint," a fact ascertainable from the sources cited in the Complaint as well as other Apple disclosures appropriately before this Court. The personalized "Hey Siri" only enables the device to pick out "Hey Siri" utterances that sound similar to the samples used to train the user profile. Siri does not (and cannot) identify the actual individual who trained the user profile (*e.g.*, "John Smith"). Moreover, the user profile does not meet the plain language definition of a voiceprint:[1] Siri cannot distinguish between voices using other phrases, and it sometimes accepts "Hey Siri" commands from another person (an "imposter accept"). In sum, the user profile is not the sort of immutable and personal biometric identifier that is regulated under BIPA.

Second, the Complaint cannot invoke BIPA through unfounded speculation that Apple collects, possesses, or disseminates the user profile when, in fact, that speculation contradicts the sources from which the Complaint purports to draw its allegations. Apple's approach to privacy by design means that the user profile is created and stored ***on the user's device***. This makes sense. The "Hey Siri" user profile is used only to let the device know when to activate Siri. Once the user profile is trained, if it were not stored on the device, the device would have no way of accepting a "Hey Siri" command. While ***audio recordings*** of Siri requests (*e.g.*, "What's the weather?") may leave the device in certain instances ***after*** activation—to respond to the user's Siri request—such audio recordings are not voiceprints, and the process does not require the user profile to leave the device. The Complaint's vague and conclusory allegations that attribute the collection of user

[1] *E.g.*, Black's Law Dictionary: a "distinctive pattern of curved lines and whorls . . . that measures human vocal sounds for the purpose of identifying an individual speaker."

profiles to Apple are not supported by well-pleaded facts, are contradicted by the materials the plaintiffs themselves cite, and do not sustain a cause of action under BIPA.

Beyond these faulty logical leaps, the claims should be dismissed for three independent reasons. The "first claim for relief" fails because it is barred by the informed written consent each plaintiff provided while creating the user profile during the User Enrollment process. The "second claim for relief" fails because the plaintiffs have not adequately alleged facts demonstrating that Apple disseminated Siri user profiles to third parties, as required to sustain the claim. Finally, the request for enhanced statutory damages should be stricken because the plaintiffs have not asserted *any* facts, much less well-pleaded facts, that would tend to establish that Apple's conduct was "intentional and reckless."

For these reasons and those set forth below, Apple respectfully requests dismissal of the Complaint with prejudice.

II. BACKGROUND

A. Siri and the "Hey Siri" feature.

Siri is "an artificial intelligence-driven software program developed by Apple" that gives Apple device users like the plaintiffs the ability to use their voices to retrieve information from the Internet and interact with their Internet-connected devices, such as by asking Siri to make a phone call, play music, send a text message, or schedule a reminder. Compl. ¶ 3. A user must activate Siri to use Siri, for example by pushing the home or side button on an iPhone or, if enabled, by uttering the pre-programmed wake phrase "Hey Siri." *Id.* ¶¶ 41-44. Users can enable or disable Siri and the "Hey Siri" feature at any time. *Id.* ¶¶ 4, 42, 50. Disabling Siri results in the deletion of data associated with the random Siri identifier, and the learning process must be restarted by the user if they later re-enable Siri. *See* Ex. 1 to Roberts Decl.

B. User Enrollment and "Hey Siri" user profiles.

Each plaintiff went through User Enrollment to enable "Hey Siri." Compl. ¶¶ 4, 9, 50, 56-65. At the beginning of User Enrollment, the "Set Up 'Hey Siri'" screen appears with the text, "This helps Siri recognize your voice when you say 'Hey Siri.'" Ex. 2 to Roberts Decl. A user always has the option to stop by pressing "Cancel." *Id.* When users click "Continue," they are asked to repeat five phrases that include the wake phrase "Hey Siri." *Id.*; *see also* Compl. ¶¶ 4, 50. The plaintiffs allege that User Enrollment results in the creation of a voiceprint. Compl. ¶¶ 52, 56.

The Complaint's description of User Enrollment selectively cites an article on Apple's Machine Learning Journal website titled "Personalized Hey Siri," a complete copy of which Apple submits as Exhibit 3 to the Roberts Declaration. *See* Compl. ¶¶ 49-51, nn. 12-17. The article states that User Enrollment is "***on-device*** personalization in the form of a speaker recognition system." Ex. 3 to Roberts Decl. at 2 (emphasis added). The user's device records the user's five "Hey Siri" utterances during User Enrollment, and an "***on-device speaker recognition system*** trains a [personalized "Hey Siri"] speaker profile from these utterances." *Id.* 4 (emphasis added). This speaker (or user) profile is later enhanced by additional, subsequent "Hey Siri" utterances. *Id; see also* Compl. ¶ 4. The user profile created during User Enrollment is stored on the user's device. *See, e.g.,* Compl. ¶ 4 ("Siri . . . records and analyzes . . . and stores the resulting data."); Ex. 3 to Roberts Decl. at 6 ("[O]n each 'Hey Siri'-enabled device, we store a user profile consisting of a collection of speaker vectors"; "In addition to the speaker vectors, we also store on the phone the 'Hey Siri' portion of [the user's] corresponding utterance waveforms.").

When "Hey Siri" is enabled, the user's device stores and analyzes "short audio clips" to "determine whether the wake phrase 'Hey Siri' has been uttered." Compl. ¶¶ 42-43. These audio clips are compared to the Siri user profile on the device. *See* Ex. 4 to Roberts Decl. at 10.[2] Only after "the various stages ***on the iPhone*** pass [the utterance] on" does "the waveform [*i.e.*, an audio recording of the Siri request] arrive[] at the Siri Server." *Id.* (emphasis added); *see also* Compl. ¶ 44 ("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 . . . ."). When a device sends an audio recording of a Siri request, it is accompanied by a random identifier and is not linked to a user's Apple ID, email address, or other data Apple may have from the user's use of other Apple services. Ex. 1 to Roberts Decl.

In accordance with its Privacy Policy, Apple previously sent a small fraction of audio recordings of Siri requests, and Siri's responses, to contractors to "evaluat[e] Siri's performance," improve Siri, and prevent the inadvertent recording of users "where no wake phrase was uttered." Compl. ¶ 47. Without any other facts, the plaintiffs allege "on information and belief" that Apple also "disclosed biometric information," *i.e.*, something other than the audio recording of the Siri request, "to third parties about Plaintiffs and the Class members." *Id.* ¶ 48.

C. The plaintiffs' claims.

The plaintiffs assert that Apple collected, captured, and stored their user profile "voiceprints" without their knowledge or consent during User Enrollment, and later disseminated the user profiles to third parties. *Id.* ¶¶ 4, 9, 57-65. The plaintiffs also allege that Apple possesses these alleged "voiceprints" and violated BIPA by failing to make available to the public the retention schedule required by BIPA. *Id.* ¶¶ 10, 69, 101.

[2] Exhibit 4 is another Machine Learning Journal article titled "Hey Siri: An On-device DNN-powered Voice Trigger for Apple's Personal Assistant," which is linked to, cited in, and relied on in the "Personalized Hey Siri" article.

III. LEGAL STANDARD

Section 2-619.1 of the Code of Civil Procedure permits a defendant to file a combined motion under both section 2-615 and section 2-619. 735 ILCS 5/2-619.1.[3] A motion under section 2-615 challenges the complaint's legal sufficiency based on facially apparent defects. 735 ILCS 5/2-615; *Doe v. Coe*, 2019 IL 123521, ¶ 31. Because Illinois is a fact-pleading jurisdiction, each cause of action must be supported by specific factual allegations, or the Court must dismiss it. *Doe*, 2019 IL 123521, ¶ 32. In evaluating the Complaint, the Court may disregard unsupported legal conclusions. *Id*. Furthermore, the Court should not "draw unwarranted or unreasonable inferences in order to sustain" the Complaint. *Douglas Theater Corp. v. Chicago Title & Tr. Co.*, 288 Ill. App. 3d 880, 886 (1st Dist. 1997).

Under section 2-619, a court must dismiss the complaint if "other affirmative matter" defeats the plaintiffs' claims, accepting both the complaint's factual allegations and legal sufficiency. 735 ILCS 5/2-619(a)(9); *McIntosh v. Walgreens Boots Alliance, Inc.*, 2019 IL 123626, ¶ 16. "Affirmative matter" means a defense that either completely negates the claim or refutes conclusions in the complaint unsupported by specific factual allegations. *McIntosh*, 2019 IL 123626, ¶ 16. Because the Complaint incorporates and is based on the "Personalized Hey Siri" article, which incorporates and is based on a second Machine Learning Journal article, the Court may consider the complete content of both articles in ruling on this motion. *See Goral v. Kulys*, 2014 IL App (1st) 133236, ¶ 44 (affirming dismissal under section 2-619 where defendant attached online records referenced in articles forming the basis of the plaintiff's defamation claim).

[3] Apple brings the motion pursuant to section 2-619 as to Section IV.D, below. All other sections are brought under section 2-615.

IV. ARGUMENT

BIPA was never intended to apply to the "Hey Siri" user profiles because they are not voiceprints, and they remain at all times within the possession and control of the person who (ostensibly) creates them, to assist the person who creates them. By contrast, BIPA protects citizens of Illinois against unauthorized collection, storage, and disclosure of certain types of biometric data. 740 ILCS 14/1 *et seq*. A private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" unless it has provided notice and obtained informed written consent. 740 ILCS 14/10; 740 ILCS 14/15(b). BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and "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." 740 ILCS 14/10. BIPA also forbids an entity in "possession" of a person's biometric identifier or biometric information from disclosing it to a third party unless the entity has provided notice and obtained informed written consent. 740 ILCS 14/15(d). Finally, BIPA requires that any private entity "in possession" of a person's biometric identifier or biometric information develop and make available to the public a retention schedule meeting certain requirements. 740 ILCS 14/15(a). For the reasons explained below, the plaintiffs fail to allege any BIPA violation.

A. BIPA does not apply because the user profile is not a voiceprint.

The plaintiffs cannot sustain a cause of action against Apple under BIPA because the user profile is not a voiceprint, biometric identifier, or biometric information. BIPA does not define "voiceprint." Thus, dictionary definitions are appropriate "to ascertain the plain and ordinary meaning of [this] statutory term." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 32 (citation omitted). A "voiceprint" is a representation of vocal sounds (as opposed to the sounds themselves) that ***identify an individual speaker***. *See, e.g.*, Black's Law Dictionary (11th ed. 2019) ("[a] distinctive pattern of curved lines and whorls made by a machine that measures human vocal sounds for the purpose of identifying an individual speaker."); Merriam-Webster Dictionary (2018) ("an individually distinctive pattern of certain voice characteristics that is spectrographically produced"); *see also United States v. Williams*, 583 F.2d 1194, 1197 (2d Cir. 1978) (describing a voiceprint as spectrographic analysis designed to "confirm the identity of the speaker"). The Office of the Illinois Attorney General, in analyzing the language of BIPA, has reached a similar conclusion, stating that a voiceprint "represents a unique physical or behavioral characteristic that identifies a person." Ex. 5 to Roberts Decl. at *3. This is also consistent with BIPA's legislative findings and intent, which highlight that the ability to identify an individual is what makes something like a voiceprint a biometric identifier. BIPA is intended to protect the privacy of information that is "biologically unique to the individual," because once this type of information is "compromised, the individual has no recourse [and] is at heightened risk of identity theft . . . ." 740 ILCS 14/5(c); *see also* Compl. ¶ 23 (a "biometric identifier" "corresponds to a person's unique physical or behavioral characteristics . . . used for identification purposes").

Under these definitions, the "Hey Siri" user profile does not constitute a voiceprint. First, the user profile is nothing more than a disembodied collection of text-dependent "speaker vectors" for whomever trained Siri (who may or may not be the device owner), and those vectors are stored on a device and work only with the phrase "Hey Siri." Ex. 3 to Roberts Decl. Neither the Complaint nor the sources it cites contain any suggestion that Apple, Siri, or the device have any ability to use the user profile to identify an individual. Given Apple's market-leading stance on privacy and its view that privacy is a fundamental human right, Compl. ¶¶ 46, 47, Apple embraces privacy by design to avoid precisely the types of violations complained of here. Thus, any information that the user generates by choosing to use Siri, to the extent it is sent to Siri servers to respond to a Siri request, is first intentionally disassociated from the user's Apple ID and attached to a random identifier that the user can reset at any time simply by turning off Siri. Ex. 1 to Roberts Decl. Apple cannot and does not use that information to identify a speaker or user.

Second, the user profile is not precise enough to identify an individual speaker as would be required to qualify as a voiceprint. This is common sense to anyone who has triggered "Hey Siri" on someone else's device or has had "Hey Siri" on their own device triggered by someone else. The Complaint, and the literature incorporated therein, acknowledge the ongoing issue of "false-alarm[s] (when Siri turns on without the user saying 'Hey Siri') and imposter-accept[s] (when Siri turns on when someone other than the user who trained the detector says 'Hey Siri') . . . ." Ex. 4 to Roberts Decl. at 13-14; *see also* Compl. ¶ 47. If the technology cannot fully prevent others from activating Siri, it cannot be said to generate a voiceprint. The user profile does not qualify as a biometric identifier under BIPA because it is not ***biologically unique*** to the individual or capable of being ***used to identify*** an individual. 740 ILCS 14/5; 740 ILCS 14/10.

The intent behind BIPA is to give Illinois citizens a choice before they turn over biometric information that may find its way into the wrong hands. Apple agrees that people should have choice over their private data, and gives users choice and control over their use of Siri and the "Hey Siri" feature. The text-dependent "Hey Siri" user profile, which has use only in summoning Siri and cannot qualify as a voiceprint, biometric identifier, or biometric information, is not what the Legislature meant to protect through BIPA. Accordingly, the Court should dismiss the Complaint, with prejudice.

B. BIPA does not apply because the user profile is stored on the device.

The plaintiffs also cannot sustain a cause of action under BIPA because they do not (and cannot) allege, other than in conclusory terms that contradict the sources on which the Complaint relies, that Apple collects or possesses the user profile "voiceprints." BIPA's requirements apply only to those in "possession" of, or who "collect, capture, purchase, receive through trade, or otherwise obtain," biometric identifiers and biometric information. 740 ILCS 14/15. To state a cause of action against Apple under the plain text of BIPA, the plaintiffs must allege that Apple obtained or gained control over their voice biometrics. *See, e.g.*, Merriam-Webster Dictionary (2020) (defining "collect" as "to gain or regain control of" and defining "capture" as "to take captive" or "to gain control of especially by force"). Accordingly, the few courts to consider this issue have determined that a defendant cannot be liable under BIPA where it provides equipment capable of collecting biometric identifiers or biometric information, but where another person or entity physically controls and operates the equipment. *See, e.g.*, *Namuwonge v. Kronos, Inc.*, 2019 WL 6253807, at *5 (N.D. Ill. Nov. 22, 2019) (dismissing BIPA claim to the extent it alleged unlawful collection against vendor who supplied system used by employer to collect fingerprints; vendor did not collect); *Bernal v. ADP, LLC*, 2019 WL 5028609, at *1-2 (Ill. Cir. Ct. Aug. 23, 2019) (same).

Here, the sources on which the Complaint is based state that user profiles are created and stored exclusively ***on the user's device*** while it (ostensibly) is in the user's control, and nothing in the Complaint supports any other conclusion. The plaintiffs ignore the portion of the "Personalized Hey Siri" article on which the Complaint relies, which states that an "***on-device*** speaker recognition system trains" the user profile "from [the User Enrollment] utterances." Ex. 3 to Roberts Decl. at 4. The user profile remains on the device. *E.g.*, *id.* at 6 ("***[O]n each 'Hey Siri'-enabled device***, we store a user profile consisting of a collection of speaker vectors") (emphasis added). The whole article describes activity that takes place exclusively on the user's device. There is no discussion of the device transmitting the user profile to Apple or its servers. To the contrary, the "Personalized Hey Siri" article cites—by name—the earlier article "Hey Siri: An ***On-device*** DNN-powered Voice Trigger for Apple's Personal Assistant." *Id.* (emphasis added).

The earlier article confirms that the user profile stays on the device after a process that takes place only on the device. The "specialized speech recognizer which is always listening just for its wake-up phrase (on a recent iPhone with the 'Hey Siri' feature enabled)" "***runs on your local device***." Ex. 4 to Roberts Decl. at 1-2 (emphasis added). It is designed so that only after an on-device comparison to the user profile determines that the "enrolled user" has spoken "Hey Siri" does Siri activate and pass on the audio recording of the Siri request (not the user profile) to the Siri server. *Id.*; *see also* Compl. ¶ 44. The audio recording of the Siri request that is transmitted to the Siri server does not qualify as a "biometric identifier" under BIPA because recorded audio is not a "voiceprint." 740 ILCS 14/10. The audio recording also does not constitute "biometric information" because it is not "based on an individual's biometric identifier." *Id.* As one court noted, BIPA is not triggered by "record[ing] a person's voice without generating a voiceprint." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1097 (N.D. Ill. 2017).

Like in *Namuwonge* and *Bernal*—where the courts dismissed BIPA claims—even under the most generous inference, all the Complaint alleges is that the plaintiffs' possessed Apple devices that the plaintiffs used to generate their user profiles, which is not a basis for BIPA liability. Each allegation that Apple collected, captured, received, obtained, or possessed the user profiles is not only vague, speculative, and conclusory, but contradicts the sources relied on in the Complaint. For this independent reason, the Complaint should be dismissed with prejudice.

C. The plaintiffs consented to the creation of the user profile.

The plaintiffs' claim under 740 ILCS 14/15(b) fails for the further reason that the plaintiffs consented to the creation of the "Hey Siri" user profile on their device. Section 15(b) allows a private entity to collect biometric identifiers or biometric information if it: (1) informs the subject in writing of the collection, (2) informs the subject in writing of the purpose and length of time the biometric identifiers or biometric information will be stored, and (3) receives a "written release" executed by the subject. 740 ILCS 14/15(b). As applied here, "written release" means "informed written consent." 740 ILCS 14/10. The purpose of the written release requirement is to give users "the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent." *Rosenbach*, 2019 IL 123186, ¶ 34. Although biometrics are not at issue in this case, Apple provides users choice and control over their private information. Contrary to the plaintiffs' allegations, *see* Compl. ¶¶ 52-55, 66-68, Apple informs users about Siri's speaker recognition features (which are not voiceprints), and users consent before providing the utterances that are used to create the user profile. Thus, with respect to the user profile, users have the "power to say no" intended by BIPA. *Rosenbach*, 2019 IL 123186, ¶ 34.

In interpreting and applying BIPA, the Court must give the statutory language its ordinary meaning and may not read additional restrictions into the clear and unambiguous language. *Rosenbach*, 2019 IL 123186, ¶ 24. By incorporating all forms of "informed written consent" within the definition of "written release," BIPA clearly and unambiguously includes consent obtained electronically, including through pressing a touchscreen button as occurs during User Enrollment.

"Written" consent is not limited to physical documents or handwritten signatures. The Illinois Electronic Commerce Security Act states that when a rule of law requires information to be "written," an electronic record satisfies that rule. *See* 5 ILCS 175/5-115(a) (defining "electronic record" as "a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another"); *see also Knolls Condo. Ass'n v. Czerwinski*, 321 Ill. App. 3d 916, 919 (2d Dist. 2001) (explaining that even where signatures are required, "alternative forms of signatures are increasingly accepted" under this Act). For example, a website user legally consents to terms and conditions (or "clickwrap") by clicking "accept" in order to proceed with a transaction, even in the absence of a written signature. *Van Tassell v. United Mktg. Grp., LLC*, 795 F. Supp. 2d 770, 790 (N.D. Ill. 2011). Courts "regularly uphold" the validity of electronic "click" consents. *Id.*; *see, e.g., Hubbert v. Dell Corp.*, 359 Ill. App. 3d 976, 984 (5th Dist. 2005) (finding that user consented by checking an "I accept" box to proceed with a sale); *In re RealNetworks, Inc., Privacy Litig.*, 2000 WL 631341, at *3-4 (N.D. Ill. May 8, 2000) (finding that user consented by clicking to agree to terms before installing software).

"Informed" consent "[protects] an individual's right to self-determination and personal independence in making decisions of great personal importance." *In re Estate of Longeway,* 133 Ill. 2d 33, 57 (Ill. 1989) (applying the doctrine to the medical context). Informed consent presupposes that a person "has the information necessary to make an informed decision and is able to evaluate that information." *Id*. Thus, under BIPA, consent is "informed" if the user proceeds after being told what information will be collected.

Here, even though BIPA does not apply, the plaintiffs' choice and control over Siri and "Hey Siri," including the User Enrollment steps, conform to the informed written consent requirements of BIPA. During User Enrollment, the "Set Up 'Hey Siri'" screen informs users who choose to enable the "Hey Siri" feature that their devices will analyze their voices. The screen says, "This helps Siri recognize your voice when you say 'Hey Siri.'" Ex. 2 to Roberts Decl. The user then has the choice to press "Continue" or "Cancel." *Id.* This screen fulfills each requirement in section 15(b): it (1) informs the user that the device will analyze the user's voice, (2) informs the user that the purpose is to "help Siri recognize your voice," and (3) requires the user to consent by pressing “Continue” instead of “Cancel.” *See* 740 ILCS 14/15(b). The user completes the process by knowingly and intentionally giving five voice samples that include the “Hey Siri” phrase. Following User Enrollment, the user can delete the user profile and restart the learning simply by re-enabling Siri. Ex. 1 to Roberts Decl. Moreover, the Complaint asserts that three on-device “user enrollment” processes allegedly result in the creation of biometric identifiers. Compl. ¶¶ 36-37. The plaintiffs acknowledge that the processes for Touch ID and Face ID—technologies not at issue here—involve “notice and consent.” *Id.* The Complaint offers no basis for deeming the “Hey Siri” User Enrollment process insufficient to give “notice and consent.” Thus, the Court should dismiss the plaintiffs’ claims under section 15(b).

D. The plaintiffs’ allegations of disclosure are insufficient to support a claim.

The plaintiffs’ second claim for relief—unlawful disclosure of the alleged user profile “voiceprints” to third parties in violation of BIPA—should be dismissed for the independent reason that the plaintiffs fail to allege any facts supporting their conclusory, “on information and belief” allegation that Apple has “disclosed biometric information to third parties about Plaintiffs and the Class members.” Compl. ¶ 48. For the reasons stated above, the user profiles are not voiceprints. Regardless, the plaintiffs’ only allegation relating to disclosure of any information to third parties derives from an article published in the *Guardian*, which discusses Apple’s practice of “shar[ing] ***recordings*** made by Siri with contractors” for purposes of “evaluating Siri’s performance.” Compl. ¶ 47 (emphasis added). But as noted above, the audio recordings of Siri requests (*e.g.*, “What’s the weather?”) are ***not*** “voiceprints” and do not fall within the scope of BIPA. Section IV.A. In any event, the plaintiffs’ allegation that Apple disclosed voiceprints in violation of BIPA is thus entirely speculative, devoid of any factual support, and insufficient to state a claim. *See Patrick Eng’g, Inc. v. Naperville*, 2012 IL 113148, ¶ 40 (allegations “on information and belief” do not, standing alone, satisfy the fact-pleading standard).

E. The plaintiffs fail to allege that Apple acted intentionally or recklessly.

BIPA permits successful claimants to receive increased damages ($5,000 per violation) from private entities that "intentionally or recklessly" violate any of BIPA's requirements. 740 ILCS 14/20(2). "Intentional" conduct is "conduct performed with a desire to cause consequences or at least a substantially certain belief that the consequences will result." *Ziarko v. Soo Line R. Co.*, 161 Ill. 2d 267, 272 (1994) (quotation omitted). "Recklessness," on the other hand, "denotes 'a course of action which shows an utter indifference to or a conscious disregard.'" *Resolution Tr. Corp. v. Franz*, 909 F. Supp. 1128, 1141 (N.D. Ill. 1995) (quoting *Ziarko*, 161 Ill. 2d at 279). Although the plaintiffs seek the heightened statutory damages under BIPA for intentional and reckless conduct, not one paragraph of the Complaint actually puts forth any well-pleaded, factual allegation supporting *scienter* or the demand for heightened statutory damages. Accordingly, the Court should strike the plaintiffs' prayer for statutory damages of $5,000 for each intentional and/or reckless violation of BIPA. *Namuwonge*, 2019 WL 6253807, at *5 (striking heightened statutory damages demand under BIPA).

V. CONCLUSION

For the foregoing reasons, Apple respectfully requests dismissal of the Complaint and each claim asserted therein with prejudice.

Dated: January 24, 2020

Respectfully Submitted,

APPLE INC.

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

Raj N. Shah (ARDC # 06244821)
Eric M. Roberts (ARDC # 6306839)
Matt Freilich (ARDC # 6332688)
DLA Piper LLP (US)—Firm No. 43034
444 West Lake Street, Suite 900
Chicago, Illinois 60606
raj.shah@dlapiper.com
eric.roberts@dlapiper.com
matt.freilich@dlapiper.com

Isabelle L. Ord*
555 Mission Street, Suite 2400
San Francisco, California 94105
isabelle.ord@dlapiper.com

Amanda Fitzsimmons*
401 B Street, Suite 1700
San Diego, California 92101
amanda.fitzsimmons@dlapiper.com

* Appearing *pro hac vice*