UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FUMIKO LOPEZ, et al.,

Plaintiffs,

v.

APPLE, INC.,

Defendant.

Case No. 19-cv-04577-JSW

ORDER GRANTING IN PART AND DENYING IN PART APPLE'S MOTION TO DISMISS

Re: Dkt. Nos. 54, 59

Now before the Court is the motion to dismiss the amended class action complaint filed by the defendant Apple, Inc. ("Apple"). The Court has considered the parties' papers, relevant legal authority, and the record in this case, and it finds the motion suitable for disposition without oral argument. See N.D. Civ. L.R. 7-1(b). The Court GRANTS Apple's motion.

BACKGROUND

Plaintiffs Fumiko Lopez, Fumiko Lopez as guardian of minor A.L., Lishomwa Henry, and Joseph Harms (collectively, "Plaintiffs") bring this putative consumer class action against Apple for violation of federal and state privacy laws. Like many others, Plaintiffs own Apple devices, namely, Apple iPhones. (Dkt. No. 48, Amended Complaint ("AC") ¶¶ 43-46.) All Apple devices allegedly come pre-installed with a software program called "Siri," which is a voice activated "intelligent assistant." (*Id.* ¶ 2.) Plaintiffs allege the following facts:

Siri is an artificial intelligence-based virtual assistant that allows individuals to use their voice to ask questions and give instructions. (*Id.*) For instance, a user can ask Siri to provide information, set an alarm, or play music using only the voice. (*Id.* ¶ 21.) Apple launched Siri in 2011 and preinstalls it on every device it makes, from the Apple Watch to the Apple TV. (*Id.* ¶ 2.) Cognizant that users might be wary of vocal surveillance, Apple assures users that Siri will only

listen to, record, and share their conversations when they give consent by, *inter alia*, saying a "hot word," such as "Hey Siri." (*Id.* ¶ 4.) Outside of this "active listening mode," Apple assures user that its devices only listen "to recognize the clear, unambiguous audio trigger" that the user wants to activate Siri. (*Id.* ¶¶ 26, 31.)

Notwithstanding these representations, on July 26, 2019, *The Guardian* published an article reporting that Apple had intercepted and disclosed private conversations without any user consent.[1] (*Id.* ¶ 5.) The article describes two sets of facts. *First*, Siri is routinely triggered by accident without any hot word. (*Id.* ¶ 35.) Two Apple devices, the Apple Watch and the Home Pod speakers, have particularly high accidental trigger rates and can be activated by a "sound of a zip." (*Id.*) *Second*, a "small portion" of Siri recordings, both deliberate and accidental, are sent to third-party contractors for evaluation. (*Id.* ¶ 6.) The contractors grade Siri responses on "whether the activation of the voice assistant was deliberate or accidental, whether the query was something Siri could be expected to help with and whether Siri's response was appropriate." (*Id.* ¶ 34.) As the result, the third-party contractors are sometimes exposed to "private discussions between doctors and patients, confidential business deals, and sexual encounters." (*Id.* ¶ 33.)

Plaintiffs allege violations of the Federal Wiretap Act ("Wiretap Act"), 18 U.S.C. § 2510, *et seq.*, the Stored Communications Act ("SCA"), 18 U.S. C. § 2701, *et seq.*, California Invasion of Privacy Act ("CIPA"), California Penal Code §§ 631(a) and 632, intrusion upon seclusion, invasion of privacy under Article I, Section 1 of the California Constitution, breach of contract, and California Unfair Competition Law ("UCL"), California Business & Professions Code § 17200, and for declaratory and other equitable relief under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.* The Court will address additional facts as necessary in its analysis.

[1] The Court finds, *sua sponte*, that the *Guardian* article is incorporated by reference into the complaint as being the basis of Plaintiffs' claims. *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1003 (9th Cir 2018); (AC ¶¶ 5 n.1, 34-37); *see* Alex Hern, *Apple contractors 'regularly hear confidential details' on Siri recordings*, the Guardian (July 26, 2019 12:34 EDT), *available at* https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings.

ANALYSIS

A. Legal Standard on Motion to Dismiss.

A motion to dismiss is proper under Federal Rule of Civil Procedure 12(b)(6) where the pleadings fail to state a claim upon which relief can be granted. The Court's "inquiry is limited to the allegations in the complaint, which are accepted as true and construed in the light most favorable to the plaintiff." *Lazy Y Ranch LTD v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008). Even under the liberal pleading standard of Federal Rule of Civil Procedure 8(a)(2), "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)).

Pursuant to *Twombly*, a plaintiff must not merely allege conduct that is conceivable but must instead allege "enough facts to state a claim to relief that is plausible on its face." *Id*. at 570. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). If the allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. *See, e.g., Reddy v. Litton Indus., Inc.*, 912 F.2d 291, 296 (9th Cir. 1990); *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv., Inc.*, 911 F.2d 242, 246-47 (9th Cir. 1990).

As a general rule, "a district court may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion." *Branch v. Tunnell*, 14 F.3d 449, 453 (9th Cir. 1994) (overruled on other grounds by *Galbraith v. County of Santa Clara*, 307 F.3d 1119 (9th Cir. 2002) (citation omitted)). However, documents subject to judicial notice may be considered on a motion to dismiss. In doing so, the Court does not convert a motion to dismiss to one for summary judgment. *See Mack v. South Bay Beer Distrib.*, 798 F.2d 1279, 1282 (9th Cir. 1986) (overruled on other grounds by *Astoria Fed. Sav. & Loan Ass'n v. Solimino*, 501 U.S. 104 (1991)).

//

//

B. Article III Standing.

As a threshold matter, Apple challenges Plaintiffs' Article III standing. No principle is more fundamental to the role of the judiciary that the "constitutional limitations of federal-court jurisdiction to actual cases or controversies." *Raines v. Byrd*, 521 U.S. 811, 818 (1997). A party seeking the federal court's jurisdiction bears the burden of demonstrating that she has standing to sue. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). If a plaintiff fails to satisfy the constitutional requirements to establish standing, the court lacks jurisdiction to hear the case and must dismiss the complaint. *See Valley Forge Christian Col. v. Americans United for Separation of Church and State*, 454 U.S. 464, 475-76 (1982). Standing must be supported "with the manner and degree of evidence required at the successive stages of the litigation." *Lujan*, 504 U.S. at 561. Thus, at the pleading stage, the court must "accept as true all material allegations," "construe the complaint in favor of the complaining party," and "determine whether the plaintiffs have clearly alleged facts demonstrating each element of standing." *Namisnak v. Uber Techs., Inc.*, 971 F.3d 1088 (9th Cir. 2020) (citations and internal quotation marks omitted).

The "irreducible minimum" of Article III standing requires plaintiffs to show that they have "(1) suffered injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, -- U.S. --, 136 S. Ct. 1540, 1547 (2016) (citing *Lujan*, 504 U.S. at 560-61). The injury must be "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Id*. at 1548 (quoting *Lujan*, 504 U.S. at 560). To be "particularized," an injury "must affect the plaintiff in a personal and individual way." *Id*. (quoting *Lujan*, 504 U.S. at 560 n.1). To be "actual or imminent," the injury must have already occurred or be "certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013). A violation of substantive privacy rights "gives rise to a concrete injury sufficient to confer standing." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020); *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117-19 (9th Cir. 2020). But standing "requires more than an injury to a cognizable interest"; it requires "that the party seeking review be himself among the injured." *Lujan*, 504 U.S. at 563.

Here, Plaintiffs allege two theories of harm: first, Apple disclosed Plaintiffs' private

information without consent and in violation of substantive privacy laws, and second, Plaintiffs suffered an economic injury because they overpaid for, and did not receive the full benefit of, their Apple devices.

As to the first theory, the Court agrees with Apple that the harm is overly speculative. Although Plaintiffs allege, in a conclusory fashion, that their communications were intercepted and disclosed, the complaint makes clear that their allegations are based entirely on the *Guardian* article. (*See* AC at ¶¶ 43-46 (referring to interception "as described above").) The *Guardian* article does not plausibly suggest that all Apple's devices were subject to accidental triggers and review by third party contractors, much less that such interception always occurred in reasonably private settings. The article discusses frequency of accidental triggers primarily in relation to the Apple Watch and the HomePod speakers, neither of which are owned by the Plaintiffs. (*Compare id.* ¶ 35, *with id.* ¶¶ 44-46.) Moreover, the article expressly states that only a "small portion" of daily Siri activations including were sent to contractors and that they included both deliberate and accidental activations. (*Id.* ¶ 34.) Finally, although the article describes private communications among the recordings sent to contractors (*see id.* ¶ 33), Plaintiffs allege no facts to suggest that their own private communications were intercepted by accidental triggers.[2]

Thus, Plaintiffs' claims of statutory privacy harm rest on an attenuated chain of possibilities that (1) their iPhones were accidentally triggered at some point, (2) the accidental triggers occurred in a context where Plaintiffs had a reasonable expectation of privacy, and (3) (for some claims) Plaintiffs' communications were part of the "small portion" of recordings sent to third party contractors. Absent factual allegations regarding the rate of accidental triggers on devices that Plaintiffs actually own, as well as their *particular* use of those devices in contexts where they had a reasonable expectation of privacy, the injury remains too speculative for Article

[2] Indeed, Plaintiffs' primary allegation of a reasonable expectation of privacy rests on home use of devices that Plaintiffs do not themselves own. (*See* AC ¶ 30.) Even assuming that Plaintiffs sufficiently alleged accidental triggers, Plaintiffs identify no concrete injury for interception of wholly public communications. *See Campbell*, 951 F.3d at 1118 (finding injury where "*private* communications are intercepted"); *cf. In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 817 (N.D. Cal. 2020) (noting that "smartphones are by their nature mobile" and "frequently used in public spaces").

III standing. *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 960-61 (9th Cir. 2009) (finding lack of standing where the risk of injury "is not concrete and particularized *as to [plaintiffs]*"); *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955, 972 (N.D. Cal. 2015) (dismissing claims for lack of standing where plaintiffs did not allege that they themselves were affected by defendant's alleged behavior); *Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 816-17 (rejecting allegations based on third party report where "Plaintiffs do not allege that any of [the reported private] recordings covered Plaintiffs' communications"); *cf. In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011) (finding standing where defendant engaged in "dragnet" surveillance that affected all of its customers, and plaintiffs were customers).[3]

As to the economic theory of injury, Plaintiffs' theory suffers from the same defects, namely, that the allegations do not show that they themselves overpaid for the devices. Although it does not concern privacy, *Birdsong* is instructive. There, the plaintiffs alleged that Apple iPod earbuds could produce hearing loss if used for prolonged periods of time at high volume. *See* 590 F.3d at 961. The court rejected the plaintiffs' alleged injury as hypothetical because they have not alleged that they themselves suffered or were likely to suffer hearing loss. *Id*. The court then rejected the economic theory of harm because the risk of hearing loss was hypothetical, depending on how consumers chose to use the devices, and the plaintiffs thus had not alleged that they were deprived of the benefit of the bargain. *Id*. The same result follows here. Although Plaintiffs *could* have used their iPhones in private settings, they fail to allege that they *have*. Nor have Plaintiffs alleged that they purchased their devices in reliance on particular representations that Siri would not be accidentally triggered, which is necessary for the "benefit of the bargain" theory. In short, Plaintiffs simply fail to allege enough facts to show a personal injury.

At bottom, "'the gist of the question of standing' is whether [plaintiffs] have 'such a personal stake in the outcome of the controversy as to assure that concrete adverseness which

[3] The purported class action nature of the suit "adds nothing to the question of standing." *Spokeo*, 136 S. Ct. at 1547 n.6. If none of the named plaintiffs have a case or controversy, "none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974); *see also Warth v. Seldin*, 422 U.S. 490, 502 (1975) ("Petitioners must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.").

sharpens the presentation of issues upon which the court so largely depends for illumination." *Mass. v. E.P.A.*, 549 U.S. 497, 517 (2007) (quoting *Baker v. Carr*, 369 U.S. 186, 204 (1962)). Here, the complaint, read holistically, strongly suggests that Plaintiffs' claims rest solely on the *Guardian* article that reports the privacy harms of other class members that may not have affected Plaintiffs at all. That is not the type of "concrete adverseness" that creates a case or controversy.

Accordingly, the Court dismisses the complaint for lack of Article III standing.

C. Wiretap Act.

A violation of the Wiretap Act occurs where any person "intentionally intercepts . . . any wire, oral, or electronic communication" or "intentionally discloses" or "uses" the contents of any such wire, oral, or electronic communication, while "knowing or having reason to know that the information was obtained through the [unlawful] interception." 18 U.S.C. §§ 2511(1)(a), (c)-(d). Importantly, the Wiretap Act defines "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. §§ 2510(2). In other words, the Wiretap Act only protects oral communications in which the speaker has a "reasonable expectation of privacy." *United States v. McIntyre*, 582 F.2d 1221, 1223 (9th Cir. 1978).

Here, Apple seeks to dismiss for failure to allege that (1) Apple "intercepted" any communication, (2) intentionally, (3) Plaintiffs had a reasonable expectation of privacy in those communications, (4) Plaintiffs did not consent to the interception, and (5) under section 2511(1)(c), Apple intentionally disclosed the communications.

1. Interception.

The Wiretap Act defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Apple argues, citing *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001), that it has not "intercepted" communications because it was the intended recipient of the communications.

The argument is meritless. The intended recipient of "discussions between doctors and patients, confidential business deals, and sexual encounters" (AC ¶ 33) are doctors, business

counterparts and sexual partners, respectively—not Apple. In *Crowley*, the plaintiffs actually sent information to Amazon in order to make a purchase. 166 F. Supp. 2d at 1265. The court found that Amazon did not "intercept" the communication because it did not use any device other than the drive or server on which the email was received. *Id*. at 1269. Similarly, in *Yunker v. Pandora Media, Inc.*, the plaintiff actually provided information to Pandora, and this Court dismissed the claims for failure to allege interception of communications "to another party." No. 11-CV-03113 JSW, 2013 WL 1282980, at *7 (N.D. Cal. Mar. 26, 2013). Here, on the other hand, Plaintiffs allege that they did not intend Apple to receive their private communications, but that Apple "captured" such communications using the software in their devices. That sufficiently alleges interception. *See Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1007-08 (N.D. Cal. 2017) (finding sufficient allegations of interception through "audio beacon" technology).

Accordingly, the Court does not dismiss on this ground.

2. Intent.

Apple argues that because Plaintiffs admit that the Siri activations were "accidental" (*e.g.*, AC ¶ 35), they cannot allege "intentional" interception. The intent requirement of the Wiretap Act requires a defendant to act "purposefully and deliberately and not as a result of accident or mistake." *United States v. Christensen*, 828 F.3d 763, 774 (9th Cir. 2015). Although no "evil" motive is required, the defendant must have "acted consciously and deliberately with the goal of intercepting wire communications." *Id*. at 774. At the pleading stage, however, interception may be considered intentional "where a defendant is aware of the defect causing the interception but takes no remedial action." *Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 815; *see also Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014).

Although the question is close, the Court finds that Plaintiffs adequately allege intent at this stage. Plaintiffs allege that Apple knows of the accidental Siri triggers and, instead of deleting the resulting messages, sends them to contractors to improve Siri's functioning. (*Id.* ¶¶ 37-39.) To be sure, one of the purposes of the third-party contractor review is to distinguish deliberate from accidental Siri activations (and, presumably, to reduce the latter). (*Id*. ¶ 34.) It is difficult to see how Apple could intentionally allow accidental Siri triggers to proceed only to use the

intercepted information to prevent accidental triggers. Nevertheless, the Court finds that at this stage, Plaintiffs sufficiently allege that Apple fails to take remedial action while knowing of the accidental activations, sufficient to make the conduct "intentional."

Accordingly, the Court does not dismiss on this ground.

3. Confidentiality.

Apple next argues that Plaintiffs fail to allege that the intercepted communications were subject to a reasonable expectation of privacy. 18 U.S.C. §§ 2510(2). As explained above, Plaintiffs have adequately alleged that Apple intercepted class members' private communications, but not their own. Specifically, Plaintiffs allege that Apple intercepted discussions between doctors and patients, confidential business negotiations, and sexual encounters (AC ¶ 33), as well as communications that took place inside private homes (*id*. ¶ 30), which is sufficient to show communications "exhibiting an expectation" of privacy "under circumstances justifying such expectation." *See, e.g., Katz v. United States*, 389 U.S. 347, 361 (1967) (holding that "a man's home is, for most purposes, a place where he expects privacy . . . "). However, because Plaintiffs include only conclusory allegations with respect to their own communications, the Wiretap Act claim is dismissed. *See Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 816-17 (dismissing analogous claims where plaintiffs failed to allege that they used their devices in circumstances giving rise to a reasonable expectation of privacy); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (dismissing conclusory claims of confidentiality) (citing cases).

Accordingly, the Court dismisses the Wiretap Act claims with leave to amend.

4. Consent.

Interception is not unlawful under the Wiretap Act where "one of the parties to the communication has given prior consent to such interception." 18 U.S.C. §§ 2511(2)(d). Consent "may be either explicit or implied, but it must be actual." *Yahoo Mail Litig.*, 7 F. Supp. 3d at 1028. Moreover, consent may be limited where a party consents to interception "of only part of a communication" or only a "subset of its communications." *Id.* (quoting *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003)). The party seeking to establish consent has the burden of proof. *Id.* (citing *Pharmatrak*, 329 F.3d at 19).

Here, the Court finds that Apple fails to establish consent. Apple argues that Plaintiffs consented to interception because the Software License Agreement ("SLA")[4] states that Siri's operation may not be "error-free." (*See* Dkt. No. 54-5 (SLA) § 7.4.) Specifically, section 7.4 of the SLA concerns warranties and states that Apple does not warrant that iOS software and services will be "uninterrupted and error free." (*Id.*) Such general disclaimer is nowhere near specific and unambiguous enough to represent that Siri may activate by accident. *See In re Google Inc. Gmail Litig.*, Case No. 13-MD-02430-LHK, 2013 WL 5423918, at *14 (N.D. Cal. Sept 26, 2013). Even if Plaintiffs consented to use Siri generally, they allege that their consent was limited to situations where a hot word was spoken. (*See* AC ¶¶ 2, 23-24, 31.) Moreover, the allegations that Plaintiffs understand how voice assistants generally work and that Siri activates based on a "confidence score" are insufficient to show that Plaintiffs consented to being recorded after a "sound of a zip." (*Id.* ¶¶ 21, 105.) Drawing all inferences in favor of Plaintiffs, that is simply not how voice assistants "generally" work.

Accordingly, the Court does not dismiss on this ground.

5. Disclosure.

Under Section 2511(1)(c) of the Wiretap Act, a party that "intentionally discloses" to "any other person" the contents of communications while "knowing or having reason to know that the information was obtained through the interception" of communications in violation of the statute is separately liable. 18 U.S.C. § 2511(1)(c). Apple seeks to dismiss for failure to plead a predicate interception. For the reasons stated above, the Court agrees that Plaintiffs have not alleged that their own communications were intercepted and disclosed and dismisses the claim.

[4] Apple seeks judicial notice of the SLA and four other documents referenced in Plaintiffs' complaint under an incorporation by reference theory. (Dkt. No. 54-7 ("RJN").) The Court finds that exhibits A-D are properly incorporated because they are cited "extensively" in the complaint and form the basis of Plaintiffs' claims that they had a reasonable expectation of privacy in their communications. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir 2018). Exhibit E, on the other hand, is cited only once and concerns representations made years after Plaintiffs purchased their devices, which is insufficient for incorporation by reference. *Id.* Nor is judicial notice proper where Apple seeks to use Exhibit E establish that a "visual indicator" of Siri activation was present on Plaintiffs' devices. *See id.*at 999 (not every fact is noticeable for its truth). Accordingly, the Court GRANTS Apple's request for Exhibits A-D only.

D. Stored Communications Act.

The Stored Communications Act ("SCA") provides a private right of action against anyone who: "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) initially exceeds an authorization to access that facility . . . while it is in electronic storage in such system." 18 U.S.C. § 2701(a). The SCA also prohibits a person or entity providing an electronic communication service from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). Apple seeks to dismiss claims under both provisions.

1. Section 2701(a)(1).

To plead a violation of the "unlawful access" provision of Section 2701(a)(1), a plaintiff must allege that the defendant "(1) gained unauthorized access to a 'facility' where it (2) accessed an electronic communication in 'electronic storage.'" *Facebook Internet Tracking Litig.*, 956 F.3d at 608. The statute does not define a "facility." However, it specifies that the facility is one "through which an electronic communication service is provided." *See* 18 U.S.C. § 2701(a)(1). Citing that language, courts have distinguished facilities that *provide* an electronic communication service—such as an email provider's servers or an ISP—from those that merely *enable* the electronic communication service—such as a user's personal computer or phone. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057-58 (N.D. Cal. 2012); *Crowley*, 166 F. Supp. 3d at 1271; *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 792 (5th Cir. 2012). The statute defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

Here, Plaintiffs' Section 2701(a)(1) claim lacks merit. Plaintiffs claim that Siri is a "facility" through which Apple gained unauthorized access to their communications. That claim fails for three reasons. First, Siri is software and not a "facility" under any common sense of the term.[5] Second, Plaintiffs do not allege that Siri provides an "electronic communication service"—

[5] As Apple points out, Plaintiffs variously claim that Siri is both the "facility" and the "electronic communication service" provided by a facility. (*See* AC ¶¶ 104, 107.) To the extent that Plaintiffs allege their devices are the facility, the claim fails for the reasons stated in *iPhone Application Litigation*, 844 F. Supp. 2d at 1057.

they allege that it enables "a variety of tasks," such as setting alarms and responding to questions. (AC ¶ 18.) Third, the statute exempts from liability "conduct authorized [] by the person or entity providing a wire or electronic communication service." 18 U.S.C. § 2701(c). Apple is the service provider here and presumably authorized its own conduct. *See In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382-PSG, 2013 WL 6248499, at *12 (N.D. Cal. Dec. 3, 2013) ("Whatever the propriety of Google's actions, it plainly authorized the actions that it took itself.").

Ultimately, the SCA is meant to protect information "held by centralized communication providers." *Google Cookie Placement Consumer Privacy Litig.*, 806 F.3d at 147; *see Facebook Internet Tracking Litig.*, 956 F.3d at 609 ("[T]he SCA has typically only been found to apply in cases involving a centralizing data-management entity."); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) ("Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, the [SCA] protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." (citation omitted)). The statute is *not* meant to provide a "catch-all . . . to protect the privacy of stored internet communications." *Google Privacy Policy Litig.*, 2013 WL 6248499, at *12 (citation omitted). Plaintiffs interpretation stretches the SCA beyond its reasonable limits and must be rejected. *See Facebook Internet Tracking Litig.*, 956 F.3d at 609 (rejecting claims based on internet tracking because it would "stretch [the SCA] beyond its limits").

Accordingly, the Court dismisses the Section 2701(a)(1) claim.

2. Section 2702(a)(1).

Unlike Section 2701, which broadly concerns third-party attempts to access a service provider's facilities, Section 2702 concerns the service provider itself. Under the "unlawful disclosure" provision of Section 2702(a)(1), the entity providing an electronic communication service may not "knowingly divulge any personal communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). Plaintiffs claim that Apple violated the statute when it disclosed Siri recordings to third-party contractors. Apple seeks to dismiss because it is not an "electronic communication service" provider and Plaintiffs consented to the disclosure under Section 2702(b)(3).

The issues are closely related to those discussed above, and the Court dismisses the claim for the same reasons. First, Plaintiffs have not alleged that Siri is an electronic communication service. The allegation that sending information to servers qualifies (AC ¶ 104) lacks plausibility because it would expand "electronic communication service" to all online services and thus render the term meaningless. Second, Plaintiffs have not alleged that their own communications were disclosed to third party contractors. However, the Court does not dismiss on the ground of consent, for the reasons stated previously.

Accordingly, the Court dismisses the Section 2702(a)(1) claim.

E. California Penal Code.

1. Section 631(a).

Section 631(a) of CIPA provides that:

> [a]ny person who . . . intentionally taps, or makes any unauthorized connection . . . , with any telegraphic or telephone wire, line cable, or instrument . . . , or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use . . . or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable [as provided for in the statute].

Cal. Penal Code § 631(a).

The subsection prohibits three separate acts: "(1) intentional wiretapping, (2) willful attempts to learn the contents of a communication in transit, and (3) attempts to use or publicize information in either manner." *Ribas v. Clark*, 38 Cal. 3d 355, 360 (1985) (In Bank) (citing *Tavernetti v. Sup. Ct.*, 22 Cal. 3d 187, 192 (1978)). By its plain terms, the second prohibition applies to both communications "in transit over any wire, line or cable" and those "sent from, or received at any place within this state." Cal. Penal Code § 631(a). Apple thus argues that the statute does not apply to oral communications because they are neither "in transit over any wire, line or cable" nor "sent" or "received."

The Court recognizes that the law regarding oral communications under Section 631(a)

remains unsettled. *See Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 826 (noting that the question "does not appear to have been squarely considered by other courts").[6] Moreover, the Court acknowledges that California courts have tended to interpret state privacy statutes broadly. *See Google Inc. Gmail Litig.*, 2013 WL 5423918, at *21. However, viewing the statutory scheme as a whole, the Court finds that California's highest court would likely conclude Section 631(a) does not protect oral communications.

California enacted CIPA in 1967 to replace prior laws that permitted recording of telephone conversations when one party consents. *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002). CIPA was driven by concerns "that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications." Cal. Penal Code § 630. The Legislature thus enacted CIPA "to protect the right of privacy of the people of" California from what it perceived as "a serious threat to the free exercise of personal liberties [that] cannot be tolerated in a free and civilized society." *Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985) (quoting Cal. Penal Code § 630). This philosophy lies "at the heart of virtually all decisions construing [CIPA]." *Id.*

Broadly speaking, Section 631 of CIPA protects against wiretapping, while Section 632 protects against eavesdropping and recording. *See* Cal. Penal Code §§ 631, 632. Two differences between the sections are relevant here. First, Section 632 expressly protects oral communications: it prohibits eavesdropping and recording regardless of "whether the communication is carried on among the parties *in the presence of one another* or by means of a . . . device." *Id.* § 632(a). By contrast, Section 631 has no such provision and only protects communications "in transit or passing over any wire, line, or cable," and those "being sent from, or received at any place within this state." *Id.* § 631(a). The Legislature thus knew how to protect oral communications and did not do so for Section 631(a). *See, e.g.*, *Meghrig v. KFC Western, Inc.*, 516 U.S. 479, 485 (1996)

[6] In *Google Assistant Privacy Litigation*, Judge Freeman noted that the statute, on its face, does not require "wire, line, or cable" communications, but reserved judgment on the question because California courts have often distinguished sections 631 and 632 by noting that the latter requires a "connection to a transmission line" and because the California Supreme Court has suggested that the second clause requires "communication in transit over a wire." 457 F. Supp. 3d at 825.

(comparing analogous statute to conclude that Congress "knew how to provide for [a] remedy" and did not do so); *In re Young*, 32 Cal. 4th 900, 907 (2004) ("Where a statute referring to one subject contains a critical word or phrase, omission of that word or phrase from a similar statute on the same subject generally shows a different legislative intent.").

Second, Section 632 is limited to *confidential* communications. Cal. Penal Code § 632(a). Section 631 is not. *Id.* § 631(a). The difference makes sense because communications passing over a wire are already "confidential" as "confined to the parties" and not in a proceeding "open to the public" under the statute. *Id*. § 632(c). By contrast, if Section 631 was interpreted to protect oral communications, the confidentiality restrictions of Section 632 would become superfluous. Moreover, this interpretation would expand privacy liability far beyond the common law—covering a person intentionally overhearing a conversation at a public park—while doing nothing to protect individuals from "new devices and techniques," as the Legislature intended. *See id.* § 631(a) (prohibiting learning of message content in any manner). Absent express guidance that the Legislature intended such broad expansion of privacy protection beyond the stated purpose, the Court declines to read it into the statute. *See Jones v. Lodge at Torrey Pines Pnshp.*, 42 Cal. 4th 1158, 1171 (2008) ("The Legislature 'does not . . . hide elephants in mouseholes.'" (quoting *Whitman v. Am. Trucking Assns., Inc.*, 531 U.S. 457, 468 (2001))).

Furthermore, the Court finds that the plain meaning of the words in the statute supports a narrower interpretation. *See Gruber v. Yelp Inc.*, 55 Cal. App. 5th 591, 605 (2020) (California courts give words "their usual and ordinary meaning"). The word "send" is typically defined as "to dispatch *by a means of communication*." *See Send*, M-W.com, https://www.merriam-webster.com/dictionary/send (last visited Feb. 2, 2021) (emphasis added). Similarly, the word "receive" means "to come into possession of." *Receive*, M-W.com, https://www.merriam-webster.com/dictionary/send (last visited Feb. 2, 2021). Neither of these words are typically used to refer to purely oral communications. The context in which these terms are used—communications "in transit or passing over any wire, line, or cable, or [] being sent from, or received at any place within this state"—makes clear that those terms distinguish messages that have already arrived or are immediately being sent, as opposed to those "in transit." For these

reasons, the Court concludes that Section 631(a) does not protect oral communications.

Accordingly, the Court dismisses Plaintiffs' Section 631(a) claim.

2. Section 632(a)

Section 632(a) of CIPA prohibits "intentionally and without the consent of all parties" using a device to "eavesdrop upon or record" confidential communications. Cal. Penal Code § 632(a). Apple moves to dismiss on the grounds that Plaintiffs fail to allege (1) use of a device, (2) intent, and (3) a confidential communication.

With respect to the second and third arguments, the Court reaches the same conclusions as it did for the Wiretap Act. *See Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 827 (noting the similarities between the claims). Although CIPA may have a slightly higher intent requirement, requiring intent to intercept confidential communications, rather than communications generally, that standard can be shown through "knowledge to a substantial certainty that . . . use of the equipment will result in the recordation of a confidential conversation." *See Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 434-35 (2018); *cf. Christensen*, 828 F.3d at 774. Here, Plaintiffs adequately allege that Apple knew of the accidental Siri triggers, and the Court finds it plausible that some of those triggers would, with "substantial certainty," occur in confidential contexts. *See Rojas*, 20 Cal. App. 5th at 430 (finding element satisfied where company intended to record work-related calls, but designed the system to record all calls).

However, Plaintiffs have not alleged that their own confidential communications were intercepted. The California Supreme Court defines confidentiality based on an "objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan*, 27 Cal. 4th at 774-76. As already noted, iPhones are frequently used in public settings, and Plaintiffs have not alleged that they used them in private settings that justify such an expectation. Plaintiffs have therefore not sufficiently alleged confidentiality. *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1020 (9th Cir. 2013) (dismissing claims where "too little is asserted in the complaint about . . . the particular circumstances of" the communications).

With respect to the first argument, the Court rejects it. Apple argues that it does not "use[] an electronic . . . recording device to eavesdrop" because the Plaintiffs control their iPhones. But

the Court does not consider this provision to impose a stringent requirement. Plaintiffs allege that Apple used the devices by programming Siri software to intercept communications when no hot word was spoken. This states a claim for eavesdropping because it involves "secretly listening to a conversation between two other parties." *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975). Apple cites no case to show that anything more is required.

Accordingly, the Court dismisses the Section 632(a) claim for failure to plead confidential communications only.

F. California Common Law and Constitutional Privacy.

Plaintiffs brings claims for intrusion upon seclusion under California common law and invasion of privacy under the California Constitution. To state a claim for intrusion upon seclusion, a plaintiff must allege "(1) that the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy and (2) that intrusion was 'highly offensive' to a reasonable person." *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 846 (N.D. Cal. 2017) (citing *Hernandez v. Hillsdale*, 47 Cal. 4th 272, 285 (2009)). To state a claim for invasion of privacy under the California Constitution, a plaintiff must allege "(1) a specific, legally protected privacy interest, (2) a reasonable expectation of privacy, and (3) a 'sufficiently serious' intrusion by the defendant." *Id.* (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 26 (1994)).

These claims are "not unrelated" under California law. *Hernandez*, 47 Cal. 4th at 286. "[T]he California Supreme Court has moved toward treating the tort and constitutional privacy inquiries as functionally identical, although the claims do continue to exist as separate claims with technically distinct elements." *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1033 (N.D. Cal. 2019) (analyzing cases). Thus, when they are brought together, they are subject to a "combined inquiry" to determine "(1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification or other relevant interests." *Facebook Internet Tracking Litig.*, 263 F. Supp. 3d at 846. "Whether a legally recognized privacy interest is present in a given case is a question of law to be decided by the court." *Hill*, 7 Cal. 4th at 40. By contrast, whether a "plaintiff has a reasonable expectation of

privacy in the circumstances" and whether "defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact." *Id*.

The Court finds that Plaintiffs have not sufficiently alleged a legally cognizable privacy interest. California courts have not recognized a general privacy interest in communications. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1040 (N.D. Cal. 2014) (discussing email). Instead, plaintiffs must typically allege an interest in "precluding the dissemination or misuse of sensitive and confidential information" (referred to as "information privacy") or "making intimate personal decisions or conducting personal activities without observation, intrusion, or interference" (called "autonomy privacy"). *Id*. at 1039 (citing *Hill*, 7 Cal. 4th at 35); *see Hernandez*, 27 Cal. 4th at 287. Plaintiffs allege neither. As explained above, Plaintiffs have not alleged specific circumstances to show that Apple intercepted their confidential communications. Nor have they alleged that the scale or pervasiveness of the accidental triggers itself gives rise to a privacy invasion. Therefore, Plaintiffs have not alleged a legally cognizable privacy interest. *Cf. id.* at 1041 (dismissing claims where plaintiffs failed to allege interception of confidential email content).

Apple also moves to dismiss because (1) Plaintiffs continued to use Siri despite knowing of the accidental recordings, and (2) the recordings were not associated with an identifiable user. But these are only two elements of the fact-intensive inquiry for the "offensiveness" of the privacy invasion that requires examining "all of the surrounding circumstances." *Hernandez*, 47 Cal. 4th at 295; *see Facebook Internet Tracking Litig.*, 956 F.3d at 606 (listing "the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion offensive"). Notably, even if Plaintiffs cannot show a reasonable expectation of privacy after the *Guardian* article, they allegedly had some reasonable expectation prior to the publication based on Apple's own privacy policy. (*See* AC ¶¶ 31-33.) Accordingly, these factors are not dispositive for Plaintiffs' California common law and constitutional privacy claims.

For these reasons, the Court dismisses the claims for intrusion upon seclusion and invasion of privacy under the California Constitution.

//

G. Breach of Contract

To state a claim for breach of contract, plaintiffs must allege (1) the existence of a contract, (2) their performance under the contract, (3) defendants' breach of the contract, and (4) damages. *Facebook Internet Tracking Litig.*, 956 F.3d at 610 (citing *Oasis W. Realty, LLC v. Goldman*, 51 Cal. 4th 811, 821 (2011)). Here, Plaintiffs cite Apple's privacy policy, which is incorporated into Apple's software licensing agreement, which states that:

1. "Siri is designed to protect your information and enable you to choose what you share." (AC ¶ 31.)
2. "Your personal data should always be protected on [the Siri Device] and never shared without [users'] permission." (*Id.* ¶¶ 32, 186.)
3. "We're always up front about what we collect from you, and we give you the controls to adjust these settings." (*Id.*)
4. "Apple can use Siri to respond to your requests or send audio to Apple to transcribe to text – but only if you give your permission first." (*Id.*)

Apple contends that these are "broad statements of company policy" that cannot form a contract. The Court disagrees. Viewed in context, the statements make concrete representations about Apple's data collection and use practices, while disclaiming other uses. For instance, the support page for Siri provides detailed representations about when Siri sends data to Apple, and the first statement above implicitly promises that no other sharing will occur. (*See* Dkt. No. 54-4.) Similarly, the third statement, while vague when viewed in isolation, precedes concrete promises about data collection while representing that Apple will disclose any other collection not already disclosed. (*See* Dkt. No. 54-3.) And the second and fourth statements expressly promise that data recording and sharing will not occur without permission.

Apple further contends that the contract included disclaimers that software operation will not be "error-free" and that Apple "may provide third parties with certain personal information" to "improve . . . products and services." (Dkt. No. 53-2 at 6.) At this stage, there are at least disputes of fact over whether these general disclaimers defeat the broad promises Apple made elsewhere. Nevertheless, the Court agrees that Plaintiffs have not alleged breach of their contract because

they fail to allege facts showing interception and disclosure in their particular circumstances.

Accordingly, the breach of contract claim is dismissed.

H. UCL

Apple moves to dismiss Plaintiffs' UCL claims on the grounds that (1) Plaintiffs lack standing because they do not allege they lost money or property, (2) Plaintiffs fail to allege a predicate violation under the "unlawful" prong of the UCL, and (3) Plaintiffs' allegations under the "unfair" prong of the UCL are conclusory.

The UCL prohibits any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. "Each of the three 'prongs' of the UCL provides a 'separate and distinct theory of liability' and an independent basis for relief." *Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1117 (N.D. Cal. 2016) (quoting *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 858 (N.D. Cal. 2012)). The unlawful prong prohibits "anything that can be called a business practice and that at the same time is forbidden by law." *Id*. (quoting *Ferrington v. McAfee, Inc.*, No. 10-CV-01455-LHK, 2010 WL 3910169, at *14 (N.D. Cal. Oct. 5, 2010)). The unfair prong prohibits practices that "violate[] established public policy" or are "immoral, unethical, oppressive or unscrupulous and causes injury to consumers which outweighs its benefits." *Id*. (quoting *McKell v. Wash. Mut., Inc.*, 142 Cal. App. 4th 1457, 1473 (2006)). Courts evaluate the unfair prong under a "balancing test" that weighs the utility of the practice against the "gravity of harm to the alleged victim." *Id*. (quoting *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012)). To have standing, a plaintiff must have "lost money or property." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011).

With respect to standing, Plaintiffs allege that they would not have purchased their devices if they knew about the accidental Siri triggers. This represents a cognizable economy injury. *See Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 966 (9th Cir. 2018). Plaintiffs partially plead this theory because they allege that Apple's privacy representations "conveyed false information about the goods [they] purchased" and that they "would not have purchased the goods in question absent this misrepresentation." *Hinojos v. Kohl's Corp.*, 718 F.3d 1098, 1105 (9th Cir. 2013); (*see* AC ¶¶ 43, 191, 199.) However, Plaintiffs fail to allege the basic facts necessary for this theory,

including that they actually purchased the devices and that they saw Apple's representations prior to the purchase. Accordingly, Plaintiffs have not adequately alleged standing.

With respect to the unlawful prong, Plaintiffs have also not alleged a predicate violation for the reasons stated in this Order.[7] *Rojas-Lozano*, 159 F. Supp. 3d at 1117. Last, with respect to the unfair prong, the resolution of the utility of Apple's interception's weight against the privacy harm to consumers is plainly inappropriate at the motion to dismiss stage. Apple cites cases where claims under the unfair prong were patently unreasonable. *See, e.g.*, *Davis*, 691 F.3d at 1170-71 (dismissing claims where the plaintiff read terms and conditions disclosing a purportedly omitted fact); *Rojas-Lozano*, 159 F. Supp. 3d at 1118 (dismissing claim that typing words into CAPTCHA field constitutes unpaid labor). Here, by contrast, a reasonable consumer could plausibly conclude that the harm from interception of confidential communications outweighs the utility from having Siri in the first place. Accordingly, the unfair prong is sufficiently pled.

For these reasons, the Court dismisses the UCL claim for lack of standing and for lack of a predicate violation under the unlawful prong only.

I. Declaratory Judgment

Plaintiffs' declaratory judgment claim is "entirely commensurate" with the other claims. *Monreal v. GMAC Mortg., LLC*, 948 F. Supp. 2d 1069, 1081 (S.D. Cal. 2013). The Court therefore dismisses it for the same reasons stated above.

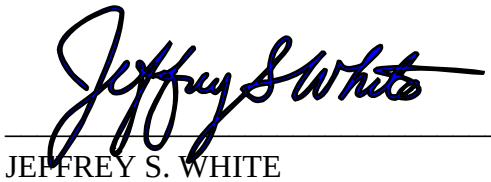
CONCLUSION

For the foregoing reasons, the Court GRANTS Apple's motion to dismiss with leave to amend. Plaintiff shall file and serve an amended complaint or a statement that no such amended complaint shall be filed within twenty days of the date of this Order, and Defendants shall file their response within twenty days thereafter.

[7] In the complaint, Plaintiffs also allege a violation of the California Online Privacy Protection Act, Cal. Bus. & Prof. Code. § 22576. However, Plaintiffs do not argue for violation of this statute in their brief, and the Court dismisses that claim accordingly. Similarly, the Court deems abandoned any argument under the "tethering" test of the unfair prong of the UCL.

IT IS SO ORDERED.

Dated: February 10, 2021



JEFFREY S. WHITE
United States District Judge

United States District Court
Northern District of California