

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

United States District Court  
Northern District of California

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION**

IN RE GOOGLE ASSISTANT PRIVACY  
LITIGATION

Case No. 19-cv-04286-BLF

**ORDER RE DEFENDANTS’ MOTION  
TO DISMISS**

[Re: ECF 56]

The instant litigation comprises two separately-filed cases that the Court has consolidated. See ECF 42 (consolidating Kumandan et al v. Google LLC et al, Case No. 19-cv-04286-BLF and Galvan et al v. Google LLC et al, Case No. 19-cv-04360-BLF). Both cases charge Defendants Google LLC and Alphabet, Inc. with unlawfully intercepting, recording, disclosing, and using the private conversations of thousands of users of the Google Assistant software. Presently before the Court is Defendants’ motion to dismiss the entire consolidated suit. ECF 56. Having considered the parties’ arguments and the applicable law, the Court GRANTS IN PART and DENIES IN PART the motion to dismiss; further, any dismissals are WITH LEAVE TO AMEND.

**I. BACKGROUND**

This is a putative consumer class action concerning the Google Assistant, a virtual assistant software developed by Defendants Google LLC and Alphabet, Inc. for use on various “Google Assistant Enabled Devices” (“GAEDs”) manufactured by Defendants and by third parties. Specifically, the operative Consolidated Amended Class Action Complaint (“Consolidated FAC”), which was filed on October 25, 2019, ECF 48, contains the following allegations:

The Google Assistant is a voice-activated software, which means that users can ask questions of and give instructions to the Google Assistant using their voices. ECF 48 (“Consol.

1 FAC”) ¶¶ 2, 22. This software comes preloaded onto certain devices, such as the Google Home,  
2 the Google Pixel smartphones, and third party-manufactured smartphones that use the Google  
3 Android operating system; it can also be installed on a range of devices. *Id.* ¶ 2. Because the  
4 Google Assistant is voice-activated, it is constantly listening for “hotwords”—i.e., “Okay Google”  
5 or “Hey Google.” *Id.* ¶ 22. It does this by recording and analyzing short snippets of audio, which  
6 are stored locally in the Google Assistant Enabled Device’s random-access memory (“RAM”);  
7 these snippets are continuously overwritten, however, if no hotwords are detected. *Id.* ¶ 23. When  
8 the hotwords are detected, the Google Assistant switches into “active listening” mode, meaning  
9 that it begins recording and analyzing audio in order to carry out the user’s command. *Id.* ¶ 24.  
10 The Google Assistant can also be manually activated by pressing a button on the device. *Id.*

11 Plaintiffs allege that Defendants also keep and use the audio recordings for two purposes  
12 other than carrying out the user’s command: (1) to target personalized advertising to users, and (2)  
13 to improve the voice recognition capabilities of the Google Assistant. *Id.* ¶ 25. The focus of this  
14 suit is the latter. Citing a 2019 news article by VRT NWS, Plaintiffs allege that the Google  
15 Assistant produces a script of each audio recording that it stores; Defendants then task human  
16 subcontractors with comparing the script to the audio recording to check the accuracy of the  
17 Google Assistant’s interpretation. *Id.* ¶ 35. In a blog post responding to this and similar reports,  
18 Google apparently confirmed that it uses human reviewers to analyze audio recordings, but stated  
19 that only “0.2 percent” of all audio recordings are subject to such analysis. *Id.* ¶ 39.

20 Sometimes, the Google Assistant may be triggered into active listening mode when the  
21 Google Assistant misperceives other words as the hotwords. This is known as a “false accept.”  
22 *Id.* ¶ 39. Plaintiffs believe that in such situations, Defendants do not destroy the audio recordings,  
23 but rather continue to use them for personalized advertising and to analyze the accuracy of the  
24 Google Assistant—just as Defendants would do with authorized recordings. *Id.* ¶¶ 38, 41. As  
25 evidence, Plaintiffs point to the investigation carried out by VRT NWS, in which VRT NWS  
26 reviewed “more than a thousand” audio recordings and “identified 153 conversations” that were  
27 recorded due to false accepts. *Id.* ¶ 36.

28 This suit is based on Defendants’ use of audio recordings in “false accept” situations. In

1 Plaintiffs’ view, such use is an invasion of privacy, especially because many of the recorded  
2 conversations take place in individuals’ homes. Id. ¶¶ 27-30. Plaintiffs also believe that this  
3 practice contravenes the privacy assurances that Defendants make to users in their Privacy Policy.  
4 Id. ¶ 31. Finally, Plaintiffs are particularly troubled by the fact that some of the recordings include  
5 the conversations of children because they do not believe that these children can consent to being  
6 recorded. Id. ¶ 42.

7 Based on the foregoing, Plaintiffs have sued Google LLC and its parent company Alphabet  
8 Inc. under various state and federal laws. There are 12 claims in the Consolidated FAC: (1)  
9 violation of the federal Wiretap Act, 18 U.S.C. §§ 2510 et seq.; (2) violation of the federal Stored  
10 Communications Act (“SCA”), 18 U.S.C. §§ 2701 et seq.; (3) violation of the California Invasion  
11 of Privacy Act (“CIPA”), Cal. Penal Code § 631(a); (4) violation of the CIPA, Cal. Penal Code §  
12 632; (5) intrusion upon seclusion under California common law; (6) invasion of privacy, in  
13 violation of Article I, Section 1 of the California Constitution; (7) breach of contract under  
14 California common law; (8) breach of express warranty under Cal. Comm. Code § 2313; (9)  
15 breach of the implied warranty of merchantability under Cal. Comm. Code § 2314; (10) violation  
16 of the Magnuson-Moss Warranty Act, 15 U.S.C. §§ 2301 et seq.; (11) violation of the California  
17 Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200 et seq.; (12) request for  
18 declaratory judgment under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 et seq. Consol.  
19 FAC ¶¶ 76-252.

20 These claims are brought by five Named Plaintiffs:

- 21 • Plaintiff Asif Kumandan is a resident of Kings County, New York. Consol. FAC ¶  
22 13. He alleges that he owned a Google Pixel smartphone during the Class Period  
23 (defined below) and that he “interacted with the Google Assistant on his Google  
24 Pixel repeatedly.” Id. ¶ 52.
- 25 • Plaintiff Melissa Spurr is a resident of Union County, New York. Id. ¶ 14. She  
26 alleges that she owned a Google Home device during the Class Period and that  
27 “she interacted with this Google Home device repeatedly.” Id. ¶ 51.
- 28 • Plaintiff B.S. is a minor member of Plaintiff Spurr’s household; as such, she has

1 allegedly interacted with Plaintiff Spurr’s Google Home device during the Class  
2 Period. Id. ¶¶ 15, 51. She brings suit by and through her legal guardian, Plaintiff  
3 Spurr. Id. ¶ 15.

- 4 • E.G., is a member of Plaintiff Galvan’s household; she was a minor during a  
5 portion of the Class Period but now brings suit on her own. Id. ¶¶ 17, 53. Plaintiff  
6 E.G. alleges that she owned a Samsung Galaxy Tab device on which she activated  
7 the Google Assistant. Id. ¶ 53. She further alleges that she interacted with the  
8 Samsung Galaxy Tab device repeatedly during the Class Period. Id.
- 9 • Lourdes Galvan is a resident of Los Angeles County, California. Id. ¶ 16. She  
10 alleges that she interacted with Plaintiff E.G.’s Samsung Galaxy Tab device during  
11 the Class Period. Id. ¶ 53.

12 To be precise, all five Named Plaintiffs assert Counts 1-7 and 11-12 on behalf of themselves and  
13 the following nationwide “Class”:

14 All individual purchasers of a Google Assistant Enabled Device, who  
15 reside in the United States and its territories and members of their  
16 households, whose conversations were obtained by Google without  
17 their consent or authorization and/or were shared with third parties  
without their consent from at least as early as May 18, 2016 to the  
present, or during the applicable statute of limitations period (the  
“Class Period”).

18 Consol. FAC ¶ 60. As for Counts 8, 9, and 10, Plaintiffs Kumadan and Spurr assert these claims  
19 on behalf of themselves and the “Google Manufactured Device Subclass,” which is defined as:

20 A Subclass of individual purchasers of a Google Manufactured  
21 Device, who reside in the United States and its territories, and  
22 members of their households, whose conversations were obtained by  
Google without their consent or authorization and/or were shared with  
third parties without their consent during the Class Period.

23 Id.

24 Defendants now move to dismiss the Consolidated FAC in full pursuant to Federal Rule of  
25 Civil Procedure 12(b)(6). ECF 56 (“Mot.”) at 1. The motion has been fully briefed and was heard  
26 on April 9, 2020. ECF 58 (“Opp.”); ECF 61 (“Reply”); ECF 75 (hearing).

## 27 **II. LEGAL STANDARD**

28 Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include “a

1 short and plain statement of the claim showing that the pleader is entitled to relief.” A complaint  
2 that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure  
3 12(b)(6). In other words, “[a] motion to dismiss under Federal Rule of Civil Procedure 12(b)(6)  
4 for failure to state a claim upon which relief can be granted ‘tests the legal sufficiency of a  
5 claim.’” *Conservation Force v. Salazar*, 646 F.3d 1240, 1241-42 (9th Cir. 2011) (quoting  
6 *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001)). To survive a Rule 12(b)(6) motion, a  
7 complaint must contain “enough facts to state a claim to relief that is plausible on its face.” *Bell*  
8 *Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the  
9 plaintiff pleads factual content that allows the court to draw the reasonable inference that the  
10 defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The  
11 plausibility standard is not akin to a probability requirement, but it asks for more than a sheer  
12 possibility that a defendant has acted unlawfully.” *Id.* (internal quotation marks omitted).

13 A court’s review on a 12(b)(6) motion to dismiss “is limited to the complaint, materials  
14 incorporated into the complaint by reference, and matters of which the court may take judicial  
15 notice.” *Cedar Point Nursery v. Shiroma*, 923 F.3d 524, 530 (9th Cir. 2019) (citing *Tellabs, Inc.*  
16 *v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007)). Moreover, in evaluating the  
17 complaint, the court must “accept factual allegations in the complaint as true and construe the  
18 pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire &*  
19 *Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). At the same time, a court need not accept  
20 as true “allegations that contradict matters properly subject to judicial notice” or “allegations that  
21 are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.” *In re Gilead*  
22 *Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (internal quotation marks and citations  
23 omitted).

### 24 **III. REQUEST FOR JUDICIAL NOTICE AND INCORPORATION BY REFERENCE**

25 Defendants have submitted six exhibits that they ask the Court to review in ruling on their  
26 motion to dismiss. See ECF 56-1 ¶¶ 2-7; *id.* at Ex. A-F. Defendants believe these exhibits are  
27 either incorporated by reference by the Consolidated FAC or subject to judicial notice.

28 There are two doctrines that permit district courts to consider material outside the

1 pleadings without converting a motion to dismiss into a motion for summary judgment: judicial  
2 notice under Federal Rule of Evidence 201 and incorporation by reference. *Khoja v. Orexigen*  
3 *Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018), cert. denied sub nom. *Hagan v. Khoja*, 139  
4 S. Ct. 2615 (2019). The judicial notice doctrine permits a court to take judicial notice of matters  
5 that are “not subject to reasonable dispute.” Fed. R. Evid. 201(b). A fact is “not subject to  
6 reasonable dispute” if it is “generally known,” or “can be accurately and readily determined from  
7 sources whose accuracy cannot reasonably be questioned.” Fed. R. Evid. 201(b)(1)–(2).  
8 However, “[j]ust because the document itself is susceptible to judicial notice does not mean that  
9 every assertion of fact within that document is judicially noticeable for its truth.” *Khoja*, 899 F.3d  
10 at 999. For instance, though public records are generally subject to judicial notice, a court may not  
11 take judicial notice of disputed facts within public records. *Id.*

12 “[I]ncorporation-by-reference is a judicially created doctrine that treats certain documents  
13 as though they are part of the complaint itself.” *Khoja*, 899 F.3d at 1002. This doctrine permits a  
14 court to consider a document “if the plaintiff refers extensively to the document or the document  
15 forms the basis of the plaintiff’s claim.” *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir.  
16 2003). A court generally “may assume an incorporated document’s contents are true for purposes  
17 of a motion to dismiss under Rule 12(b)(6).” *Khoja*, 899 F.3d at 1003 (internal quotations  
18 omitted). Because all inferences must still be drawn in the nonmoving party’s favor, however, “it  
19 is improper to assume the truth of an incorporated document if such assumptions only serve to  
20 dispute facts stated in a well-pleaded complaint.” *Id.*

21 Having reviewed the basic principles of judicial notice and incorporation by reference, the  
22 Court turns to each of the six documents Defendants have submitted. Plaintiffs have not opposed  
23 the Court’s consideration of any of the documents at issue.

24 Exhibit A is a copy of the 2019 news report by VRT NWS cited by Plaintiffs in  
25 Consolidated FAC. ECF 56-1, Ex. A; see Consol. FAC ¶¶ 34-38. Defendants ask the Court to  
26 treat the article as incorporated by reference; Defendants also argue that the article is subject to  
27 judicial notice, as it “appears on [a] publicly accessible website.” Mot. at 2-3. It is well-  
28 established that “[c]ourts may take judicial notice of publications introduced to indicate what was

1 in the public realm at the time, not whether the contents of those articles were in fact true.” Von  
2 Saher v. Norton Simon Museum of Art at Pasadena, 592 F.3d 954, 960 (9th Cir. 2010) (internal  
3 quotations omitted); see also Packsys, S.A. de C.V. v. Exportadora de Sal, S.A. de C.V., 899 F.3d  
4 1081, 1087 n.2 (9th Cir. 2018) (“We take notice of the fact of publication, but do not assume the  
5 truth of the article’s contents.”). The Court therefore takes judicial notice of the fact that VRT  
6 NWS published each of the allegations contained in the article, but not of the truth of those  
7 allegations. As Defendants do not ask the Court to treat the contents of the article as true—indeed,  
8 they dispute its truth—the Court need not reach the issue of incorporation by reference. The  
9 request for judicial notice is GRANTED, with the caveats just described.

10 Defendants similarly ask the Court to consider Exhibit B—the Google blog post referenced  
11 in the Consolidated FAC, see Consol. FAC ¶ 39—as incorporated by reference or as a judicially-  
12 noticeable website. Mot. at 2-3; ECF 56-1, Ex. B. Again, Defendants do not ask the Court to treat  
13 the contents of the blog post as true. Thus, as with the VRT NWS article, the Court takes judicial  
14 notice of the blog post for the fact that Google made the statements it contains, but not for the  
15 truth of those statements. The request for judicial notice is GRANTED as stated; the Court need  
16 not decide whether the blog post was incorporated by reference.

17 Exhibits C and D are copies of Defendants’ Terms of Service (“TOS”) and Privacy Policy,  
18 respectively. ECF 56-1, Ex. C (Google Terms of Service), Ex. D (Privacy Policy). These  
19 documents “form the basis” for Plaintiffs’ claims for breach of contract (Count 7) and breach of  
20 express warranty (Count 8), as they contain the contract terms and warranty terms that were  
21 allegedly breached. See Consol. FAC ¶¶ 189-199, 210. Defendants’ request to incorporate by  
22 reference the Terms of Service and Privacy Policy is therefore GRANTED. See Ritchie, 342 F.3d  
23 at 908; accord Bass v. Facebook, Inc., 394 F. Supp. 3d 1024, 1037 n.1 (N.D. Cal. 2019) (granting  
24 Facebook’s request to incorporate by reference the Terms of Service because the consolidated  
25 complaint relied upon them to allege the breach of contract claims and statutory claims).

26 Lastly, Exhibit E purports to be a copy of the “Google Home Warranty – United States”  
27 and Exhibit F purports to be a copy of the “Hardware limited warranty for Android Hardware  
28 devices, including the Pixel smartphone.” ECF 56-1 ¶¶ 6-7; see id. Ex. E-F. These documents are

1 not incorporated by reference by the Consolidated FAC; rather, Defendants ask the Court take  
2 judicial notice of them because “they appear on publicly accessible websites and their authenticity  
3 cannot be reasonably questioned.” Mot. at 3 (citing *Datel Holdings Ltd. v. Microsoft Corp.*, 712  
4 F. Supp. 2d 974, 983-84 (N.D. Cal. 2010)). The Court agrees that the existence of these  
5 documents is a judicially noticeable fact, and therefore GRANTS Defendants’ unopposed request.  
6 See, e.g., *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 976 (N.D. Cal. 2015) (collecting cases in  
7 which courts have taken judicial notice of publicly available policies and agreements). The Court  
8 notes, however, that its judicial notice does not establish that these documents are “valid or  
9 binding contracts.” *Datel Holdings*, 712 F. Supp. 2d at 984.

#### 10 **IV. DISCUSSION**

11 Defendants move to dismiss all the claims in the Consolidated FAC; Plaintiffs, of course,  
12 oppose the motion. Because the legal requirements for each claim differ substantially, the Court  
13 considers the sufficiency of Plaintiffs’ allegations as to each set of claims seriatim.

##### 14 **A. Count 1: Federal Wiretap Act**

15 The Federal Wiretap Act (“Wiretap Act”), 18 U.S.C. §§ 2510–2520, “is designed to  
16 prohibit ‘all wiretapping and electronic surveillance by persons other than duly authorized law  
17 enforcement officials engaged in investigation of specified types of major crimes.’” *Greenfield v.*  
18 *Kootenai County*, 752 F.2d 1387, 1388 (9th Cir. 1985) (quoting S. Rep. No. 1097, 90th Cong., 2d  
19 Sess.). In Count 1 of the Consolidated FAC, Plaintiffs allege that the Defendants violated 18  
20 U.S.C. § 2511(1)(a), which makes it unlawful for a person to “intentionally intercept[], endeavor[]  
21 to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or  
22 electronic communication.” *Id.* § 2511(1)(a); see *Consol. FAC* ¶¶ 88-91. The Wiretap Act also  
23 imposes liability on any person who “intentionally discloses” to “any other person the contents of  
24 any wire, oral, or electronic communication,” or “intentionally uses” the “contents of any wire,  
25 oral or electronic communication” while “knowing or having reason to know that the information  
26 was obtained through the [unlawful] interception,” *id.* § 2511(1)(c)-(d); Plaintiffs allege that  
27 Defendants also violate this provision. See *Consol. FAC* ¶¶ 92-95

28 Defendants contend that Plaintiffs have failed to adequately plead either of their theories



1 because (1) Plaintiffs have not shown that any interception was “intentional” rather than  
2 inadvertent, (2) Plaintiffs have not identified any specific “oral communications” that were  
3 allegedly intercepted, (3) Defendants’ conduct falls within the “ordinary course of business  
4 exception,” and (4) Plaintiffs have not shown that Defendants used or disclosed information they  
5 knew to be unlawfully obtained. Mot. at 4-8. The Court addresses each argument below.

6 **i. “Intentional” Interception**

7 As the text of the statute makes clear, the Wiretap Act prohibits only interception that is  
8 “intentional, as opposed to inadvertent.” *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026,  
9 1030 (N.D. Cal. 2014) (citing *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742–43 (4th Cir.  
10 1994)). Defendants emphasize that Plaintiffs’ claim is based only on “false accepts,” which  
11 Defendants maintain are definitionally inadvertent rather than intentional. Mot. at 4-5. That is,  
12 false accepts are a defect rather than an intended feature of the Google Assistant. *Id.* Plaintiffs  
13 respond that Defendants’ knowledge of the defect combined with its failure to remedy it or to  
14 destroy the recordings suffice to make its conduct “intentional” under the statute. ECF 58  
15 (“Opp.”).

16 The intent requirement under § 2511 requires the interception to have been “purposeful[]  
17 and deliberate[]” and not “a result of accident or mistake.” *United States v. Christensen*, 828 F.3d  
18 763, 774 (9th Cir. 2015); accord *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003) (“An act is  
19 not intentional if it is the product of inadvertence or mistake.”). Although inadvertent  
20 interceptions are plainly not actionable, several courts have rejected a defendant’s claim that the  
21 interception was inadvertent where the defendant was aware it was occurring. The case most  
22 similar to this one is *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033 (N.D. Cal. 2014), in which the  
23 court allowed a Wiretap Act claim to proceed despite Apple’s contention that it had “mistakenly”  
24 intercepted the messages at issue. *Id.* at 1044. The court held that Plaintiffs’ allegations that  
25 Apple knowingly allowed the defect to recur and “even charged consumers \$19 to ‘fix’ the  
26 problem” were sufficient to “foreclose[] the possibility that Apple’s actions were the product of  
27 inadvertence or mistake.” *Id.* This reasoning is consistent with that of courts outside this Circuit.  
28 See *Abraham v. Cty. of Greenville, S.C.*, 237 F.3d 386, 392 (4th Cir. 2001) (upholding a jury’s

1 finding of intent under § 2511 based on evidence that the County knew it “might be inadvertently  
2 eavesdropping” on judges’ conversations using a recording system intended only for  
3 “administrative personnel and the guards in the jail” yet never informed the judges); *Anderson v.*  
4 *City of Columbus, Georgia*, 374 F. Supp. 2d 1240, 1247 (M.D. Ga. 2005) (denying summary  
5 judgment on the issue of intent under § 2511 because “evidence exists that Turner was aware of  
6 the glitch in the recording system when the headsets were used. Therefore, a reasonable jury could  
7 conclude that Turner knew that the system would record Plaintiff, and she intentionally failed to  
8 tell Plaintiff how to prevent the recording”).

9 The Court agrees with Plaintiffs and these various courts that interceptions may be  
10 considered intentional where a defendant is aware of the defect causing interception and takes no  
11 remedial action. And indeed, the Consolidated FAC alleges that Defendants are aware of false  
12 accepts and the recordings they cause to be made, yet have not fixed the problem. See Consol.  
13 FAC ¶¶ 38-39. At the same time, the Court finds persuasive Defendants’ argument that some de  
14 minimis error rate in the Google Assistant may be tolerated without exposing them to liability;  
15 after all, even the human ear misinterprets words and sounds at times. For that reason, the degree  
16 of error will likely be material to the ultimate factual determination of whether Defendants’  
17 conduct was intentional. At the motion to dismiss stage, however—construing the allegations in  
18 Plaintiffs’ favor—the Court will not assume that the rate of false accepts is de minimus.

19 Besides, Plaintiffs’ objection is not only to Defendants’ failure to prevent recordings  
20 caused false accepts—which may be a tall order—but also to Defendants’ failure to destroy the  
21 audio recordings produced by false accepts. Plaintiffs allege that Defendants persist in using the  
22 recordings for personalized advertising or to improve the functionality of the Google Assistant,  
23 even after they become aware of their provenance. FAC ¶¶ 38-39. That Defendants allegedly do  
24 not destroy the audio recordings further supports an inference that the interception is “intentional.”

25 The Court therefore rejects Defendants’ argument that Plaintiffs have not adequately  
26 pleaded “intentional” interception. To be clear, the Court does not hold that inaction in the face of  
27 a known design defect necessarily makes an interception “intentional” under the Wiretap Act—  
28 only that the facts alleged here are sufficient to survive a motion to dismiss.

**ii. “Oral Communications”**

1 Defendants’ second argument for dismissal concerns the requirement that a plaintiff show  
2 interception of a “wire, oral, or electronic communication.” 18 U.S.C. § 2511(a)(1). Defendants  
3 argue that Plaintiffs’ claim, despite being premised on the alleged interception of “oral  
4 communications,” has failed “to identify a single oral communication that they contend was  
5 intercepted.” Mot. at 5-6. Moreover, the Wiretap Act defines “oral communication” as “any oral  
6 communication uttered by a person exhibiting an expectation that such communication is not  
7 subject to interception under circumstances justifying such expectation,” 18 U.S.C. § 2510(2); i.e.,  
8 an oral communication in which the speaker had a “reasonable expectation of privacy,” United  
9 States v. McIntyre, 582 F.2d 1221, 1223 (9th Cir. 1978). Defendants therefore assert that  
10 Plaintiffs must not only identify intercepted oral communications, they must also show that those  
11 communications were subject to a reasonable expectation of privacy. Mot. at 5-6.

12 In response, Plaintiffs point first to the 153 recordings due to false accepts that VRT NWS  
13 discovered in the course of reporting its 2019 news piece. Consol. FAC § 36. To show that these  
14 conversations were subject to a reasonable expectation of privacy, VRT NWS’s description of  
15 these conversations as including “bedroom conversations, conversations between parents and their  
16 children,” and “professional phone calls containing lots of private information.” Id. But Plaintiffs  
17 do not allege that any of these 153 recordings covered Plaintiffs’ communications rather than the  
18 communications of unnamed third parties. Hence, these allegations do not suffice to show that  
19 Plaintiffs’ own oral communications were intercepted, which they must do. See Lewis v. Casey,  
20 518 U.S. 343, 357 (1996) (“[N]amed plaintiffs who represent a class must allege and show that  
21 they personally have been injured, not that injury has been suffered by other, unidentified  
22 members of the class to which they belong and which they purport to represent.”) (internal  
23 quotations omitted).

24 As for the allegations regarding the Named Plaintiffs themselves, the Court finds these to  
25 be too vague. See Consol. FAC ¶¶ 51-53. At the outset, the Court rejects Defendants’ suggestion  
26 that Plaintiffs must identify specific communications that Plaintiffs reasonably believed to be  
27 private and that were wrongly recorded. The Court is not convinced that Plaintiffs are required to  
28

1 produce such details at the pleading stage, prior to discovery. At the motion hearing, Defendants  
2 represented that through their accounts, users can view all their past conversations with the Google  
3 Assistant, including false accepts. If that is the case, Plaintiffs are advised to avail themselves of  
4 that information. But the Court believes it would be enough for Plaintiffs to show that they  
5 frequently have oral communications near their respective Google Assistant Enabled Devices  
6 under circumstances giving rise to a reasonable expectation of privacy. That, coupled with the  
7 allegations that false accepts routinely occur, would support an inference that Plaintiffs had private  
8 conversations intercepted.

9 In their Opposition, Plaintiffs maintain that they have done this. Opp. at 6. Not so. The  
10 Consolidated FAC contains insufficient detail regarding the particular circumstances under which  
11 Plaintiffs used their Google Assistant Enabled Devices. The Consolidated FAC merely alleges  
12 that Plaintiffs' conversations were "confidential" without alleging any facts regarding the  
13 participants in the conversations, the locations of the conversations, or examples of content from  
14 the conversations. Cf. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (finding  
15 plaintiffs' allegations that their emails were "private" to be "fatally conclusory"). Nor does the  
16 bare allegation that each Named Plaintiff "interacted with" their device "repeatedly" establish that  
17 those devices necessarily picked up private conversations, or that any expectation of privacy was  
18 reasonable. Cf. *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, 1035 (N.D. Cal. 2014)  
19 ("[T]here is no legally protected privacy interest and reasonable expectation of privacy in  
20 electronic messages, in general. Rather, a privacy interest can exist, if at all, only with respect to  
21 the content of those communications.") (internal quotations omitted).

22 This problem is especially glaring for Plaintiffs Kumandan, Galvan, and E.G., who  
23 allegedly interacted with smartphones. After all, smartphones are by their nature mobile and are  
24 frequently used in public places. The allegations as to Plaintiffs Spurr and B.S. also fall short.  
25 Though they allegedly interacted with a Google Home device—which presumably is less  
26 mobile—Plaintiffs make no allegations as to where the Google Home device was located and how  
27 Plaintiffs used it. Consol. FAC ¶ 51. Under these circumstances, the Court cannot infer that the  
28 Plaintiffs themselves had "oral communications" intercepted, as necessary under the Wiretap Act.

1           Accordingly, the Court must GRANT Defendants’ motion to dismiss. That dismissal is  
2 with LEAVE TO AMEND, as leave ordinarily must be granted in this Circuit and Defendants  
3 have articulated no reason it should not be. See *Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d  
4 1048, 1052 (9th Cir. 2003) (citing *Foman v. Davis*, 371 U.S. 178, 182 (1962)).

5                           **iii. Ordinary Course of Business Exception**

6           Although the Court must dismiss the Wiretap Act claim for failure to adequately plead  
7 “oral communications,” the Court proceeds to address Defendants’ other proposed grounds for  
8 dismissal. The next of these is Defendants’ contention that the “ordinary course of business  
9 exception” inoculates its alleged interceptions here. The Wiretap Act defines “intercept” as “the  
10 aural or other acquisition of the contents of any wire, electronic, or oral communication through  
11 the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). In other words,  
12 there is no illegal interception without the use of a “device.” Accord *In re Yahoo Mail Litig.*, 7 F.  
13 Supp. 3d at 1026. The Wiretap Act then goes on to carve out from its definition of “device” “any  
14 telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used  
15 by a provider of wire or electronic communication service in the ordinary course of business.” *Id.*  
16 § 2510(5)(a)(ii); the “ordinary course of business” exception refers to this carve-out.

17           Defendants claim that their alleged conduct falls within the ordinary course of business  
18 exception because “the Assistant cannot operate unless it records and transmits audio to Google.”  
19 Mot. at 7. They further assert that any false accepts are “incidental to” the necessary  
20 transmissions. *Id.* (citing *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 WL  
21 5423918 (N.D. Cal. Sept. 26, 2013)).

22           In response, Plaintiffs contend that Defendants are not a provider of “electronic  
23 communication service” (“ECS”) as required for the exception to apply. Opp. at 7 (quoting 18  
24 U.S.C. § 2510(5)(a)(ii)). The Wiretap Act defines “electronic communication service” as “any  
25 service which provides to users thereof the ability to send or receive wire or electronic  
26 communications.” 18 U.S.C. § 2510(15). Of relevance here, “oral communications” are distinct  
27 from both “wire communications” and “electronic communications” under the Wiretap Act. See  
28 18 U.S.C. §§ 2510(1), (2), (12); *Siripongs v. Calderon*, 35 F.3d 1308, 1320 (9th Cir. 1994)

1 (treating the intercepted communication as an “oral communication” because police “acquired  
2 only what they recorded Siripongs saying into the mouthpiece, not what was transmitted over the  
3 wire”). Plaintiffs maintain that Defendants “cannot be considered” an ECS provider “in the  
4 instance when it is recording Plaintiffs’ private oral communication” because oral communications  
5 are not “wire or electronic communications.” Opp. at 7.

6 Plaintiffs misunderstand Defendants’ argument, however. The “wire or electronic  
7 communication service” that the Google Assistant purports to provide is the transmission of valid  
8 commands from the user to Defendants’ servers, which carry out the commands. These  
9 commands arguably constitute “electronic communications,” which “means any transfer of signs,  
10 signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part  
11 by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or  
12 foreign commerce.” 18 U.S.C. § 2510(12). In simple terms—and as described in the  
13 Consolidated FAC, see *id.* ¶ 24—the Google Assistant translates a user’s verbal command (e.g.,  
14 “Hey Google, what is the weather forecast?”) into electronic signals and then transmits those  
15 signals to the recipient, the relevant Google server. The Google Assistant could thus be seen as  
16 providing an electronic communication service.<sup>1</sup>

17 Nevertheless, the Court need not conclusively decide the merits of this issue, which has not  
18 been treated in any depth by the parties. Even assuming the Google Assistant is an electronic  
19 communication service provider, the ordinary course of business exception does not preclude  
20 Plaintiffs’ Wiretap Act claims.

21 As Defendants themselves acknowledge, “the ordinary course of business exception . . .  
22 offers protection from liability only where an electronic communication service provider’s  
23 interception facilitates the transmission of the communication at issue or is incidental to the  
24 transmission of such communication.” *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at \*8.

---

25  
26 <sup>1</sup> Defendants point out that Plaintiffs allege in the Consolidated FAC that the Google Assistant is  
27 an “electronic communication service” within the meaning of the SCA, 18 U.S.C. § 2702(a).  
28 Consol. FAC ¶ 112. Although true, this allegation is not dispositive. First of all, Plaintiffs are  
entitled to plead claims in the alternative: Plaintiffs may have pleaded that SCA claim in the event  
the Wiretap Act claim was found to be precluded by the ordinary course of business exception.  
Besides, the Court is not required to accept the purely legal conclusion offered by the allegation.

1 False accepts certainly do not “facilitate” the functioning of the Google Assistant; they are, in both  
2 parties’ views, produced by the malfunctioning of the Google Assistant. The question becomes,  
3 then, whether false accepts are so unavoidable that they could fairly be considered “incidental to”  
4 the Google Assistant’s ordinary functioning. But as noted earlier, the degree to which that false  
5 accepts are unavoidable is a factual issue, unsuited for resolution at the pleading stage. See *Khoja*,  
6 899 F.3d at 1003. Moreover, the Court is not aware of any cases applying the exception to  
7 interceptions that are allegedly the product of a defect. Hence, even if Defendants are providers of  
8 electronic communication services, there is a question of fact as to whether false accepts are  
9 “incidental to” the transmission of legitimate commands by the Google Assistant. Plaintiffs’  
10 Wiretap Act claim is not subject to dismissal on the basis of the ordinary course of business  
11 exception.

12 **iv. Use or Disclosure**

13 Plaintiffs’ Wiretap Act claim also asserts the theory that Defendants “used” and  
14 “disclosed” unlawfully intercepted information, which is itself unlawful under 18 U.S.C. §§  
15 2511(1)(c)-(d). See generally *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009). Of relevance to  
16 this claim, Plaintiffs allege that Defendants used the unlawfully created audio recordings to  
17 personalize advertising and to improve the voice recognition capabilities of the Google Assistant.  
18 See Consol. FAC ¶¶ 41, 95. Plaintiffs further allege that, in order to accomplish the latter,  
19 Defendants disclosed the audio recordings to third party subcontractors. *Id.* ¶¶ 35-39.

20 Defendants move to dismiss this theory on two grounds. First, they correctly point out that  
21 liability for disclosure or use is contingent on the original interception being unlawful. *Noel*, 568  
22 F.3d at 751; see *Mot.* at 8. Because the Court has just determined that Plaintiffs have not  
23 adequately pleaded the unlawfulness of the interceptions, their use or disclosure claim likewise  
24 fails.

25 Defendants’ second argument implicates the requirement under §§ 2511(1)(c)-(d) that a  
26 defendant “know[] or hav[e] reason to know that the information was obtained through” an  
27 interception that violates the Wiretap Act. 18 U.S.C. §§ 2511(1)(c)-(d). Defendants maintain that  
28 Plaintiffs “have not and cannot allege that Google knew that the information allegedly disclosed or

1 used came from an intercepted communication (rather than a communication intended for the  
2 Assistant) or that such interception was prohibited by the Wiretap Act.” Mot. at 8. The argument  
3 appears to be that Defendants reasonably believed each audio recording to be the result of a  
4 legitimate command at the time when it sent the recording to a third party for analysis or used it to  
5 customize advertising.

6 To be sure, Defendants may mount a defense based on this argument. But Plaintiffs have  
7 specifically pleaded that “even after Google discovers that it has wrongly recorded a conversation,  
8 it nonetheless keeps and analyzes the recording.” Consol. FAC ¶ 38. In other words, Plaintiffs  
9 allege that Defendants knew each recording was the product of an unauthorized interception at the  
10 time of their alleged use and disclosure. The Court must construe this allegation to be true at the  
11 motion to dismiss stage, despite Defendants’ assertion to the contrary. Accordingly, the Court will  
12 dismiss the “use” or “disclosure” theory, but not on the ground that Defendants lacked knowledge  
13 of the antecedent interception.

14 **B. Count 2: Stored Communications Act**

15 Count 2 alleges violations of the Stored Communications Act (“SCA”). As the Ninth  
16 Circuit has explained, the SCA is modeled off the common law of trespass. *Theofel v. Farey-*  
17 *Jones*, 359 F.3d 1066, 1072–73 (9th Cir. 2004). “Just as trespass protects those who rent space  
18 from a commercial storage facility to hold sensitive documents, the Act protects users whose  
19 electronic communications are in electronic storage with an ISP or other electronic  
20 communications facility.” *Id.* (internal quotations and citations omitted). Thus, the SCA forbids  
21 making unlawful access to a stored communication, imposing liability on any person or entity  
22 who:

23 (1) intentionally accesses without authorization a facility through  
24 which an electronic communication service is provided; or

25 (2) intentionally exceeds an authorization to access that facility;

26 and thereby obtains, alters, or prevents authorized access to a wire or  
27 electronic communication while it is in electronic storage in such  
28 system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2701(a).

Subsection (c) goes on to state that subsection (a) does not apply “to conduct authorized”



1 “(1) by the person or entity providing a wire or electronic communications service; [or] (2) by a  
2 user of that service with respect to a communication of or intended for that user.” 18 U.S.C.  
3 § 2701(c)(1); accord *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal.  
4 2001). However, an ECS provider still “shall not knowingly divulge to any person or entity the  
5 contents of a communication while in electronic storage by that service”; if it does so, it is liable  
6 for unlawful disclosure of customer communications under § 2702(a). 18 U.S.C. § 2702(a)(1).  
7 The Consolidated FAC asserts claims for unlawful access pursuant to § 2701(a) and unlawful  
8 disclosure pursuant to § 2702(a). Consol. FAC ¶¶ 117-124. In their motion to dismiss,  
9 Defendants argue that “Plaintiffs cannot state a claim under either provision.” The Court  
10 disagrees: Although Plaintiffs have not pleaded a claim for unlawful access, Count 2 may proceed  
11 based on a theory of unlawful disclosure.

12 **i. Unlawful Access under 18 U.S.C. § 2701(a)**

13 To make out a claim under either subsection of 18 U.S.C. § 2701(a), Plaintiffs must show  
14 that Defendants “(1) gained unauthorized access to a ‘facility’ where it (2) accessed an electronic  
15 communication in ‘electronic storage.’” *In re Facebook, Inc. Internet Tracking Litig.*, No. 17-  
16 17486, 2020 WL 1807978, at \*13 (9th Cir. Apr. 9, 2020). The SCA defines “electronic storage”  
17 as

18 (A) any temporary, intermediate storage of a wire or electronic  
communication incidental to the electronic transmission thereof; and

19 (B) any storage of such communication by an electronic  
20 communication service for purposes of backup protection of such  
communication;

21 18 U.S.C. §§ 2711(1), 2510(17). The SCA does not, however, provide a statutory definition of  
22 “facility,” which is a separate element of an SCA claim. See *In re Facebook*, 2020 WL 1807978,  
23 at \*13, \*14 n.10. Nor has the Ninth Circuit provided much guidance on interpreting the term.

24 In their motion to dismiss, Defendants argue that a facility must be “physical means or  
25 equipment,” such as a server. Mot. at 9 (quoting *Council on Am.-Islamic Relations Action*  
26 *Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 335 (D.D.C. 2011)). Defendants believe that  
27 Plaintiffs have failed to identify a qualifying “facility” providing “electronic storage” that has  
28 allegedly been accessed. See Mot at 9; Reply at 5. The Consolidated FAC indicates that the

1 Google Assistant “is the facility through which Google provides an electronic service.” Consol.  
2 FAC ¶ 115. In their Opposition brief, Plaintiffs reiterate that the Google Assistant is a “facility”  
3 within the meaning of the SCA, see Opp. at 9; Plaintiffs also offer another possible “facility”:  
4 Defendants’ “remote servers,” see *id.* (citing Consol. FAC ¶¶ 43, 93). Defendants maintain that  
5 neither qualifies. See Mot at 9; Reply at 5.

6 Turning first to whether the Google Assistant is a “facility,” the Court notes that Plaintiffs  
7 have not been consistent or precise as to what they mean by the “Google Assistant.” For clarity,  
8 the Court uses “Google Assistant” to refer to the virtual assistant software and not the Google  
9 Assistant Enabled Device onto which it may be pre-installed or downloaded. See Consol. FAC ¶¶  
10 21, 112. Without adopting Defendants’ definition of “facility” as “physical” equipment, the Court  
11 is skeptical that software could properly be considered a facility. Regardless whether a facility is  
12 necessarily “physical,” it indisputably must provide “electronic storage.” It is not alleged that the  
13 Google Assistant itself—which, as a “computer program,” is comprised of lines of code—  
14 provides electronic storage of any kind. See Consol. FAC ¶ 21. Rather, the Consolidated FAC  
15 states that a Google Assistant Enabled Device’s RAM stores the snippets of audio that are  
16 continuously being analyzed by the Google Assistant. See *id.* ¶ 23.

17 It is perhaps unsurprising, then, that Plaintiffs do not attempt to argue that the Google  
18 Assistant software is a “facility” in their Opposition brief; they assert instead that their devices’  
19 RAM constitutes the facility from which their communications were accessed “while they were  
20 temporarily stored” there. Opp. at 9. Defendants object that a user’s personal device cannot be a  
21 “facility” under the SCA. It is true that courts in this Circuit and others have interpreted “facility”  
22 to exclude users’ personal devices. See, e.g., *In re Google Inc. Cookie Placement Consumer*  
23 *Privacy Litig.*, 806 F.3d 125, 147-48 (3d Cir. 2015); *In re Facebook Internet Tracking Litig.*, 263  
24 F. Supp. 3d 836, 845 (N.D. Cal. 2017), *aff’d*, 956 F.3d 589 (9th Cir. 2020); *In re iPhone*  
25 *Application Litig.*, 844 F. Supp. 2d 1040, 1057-58 (N.D. Cal. 2012); *Freedom Banc Mortg. Servs.,*  
26 *Inc. v. O’Harra*, No. 2:11-cv-01073, 2012 WL 3862209, at \*9 (S.D. Ohio Sept. 5, 2012). Even  
27 the Ninth Circuit has alluded to the SCA as “cover[ing] access to electronic information stored in  
28 third party computers.” *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1104 (9th Cir. 2014); see also

1 Theofel, 359 F.3d at 1072–73 (“Just as trespass protects those who rent space from a commercial  
2 storage facility to hold sensitive documents, the Act protects users whose electronic  
3 communications are in electronic storage with an ISP or other electronic communications  
4 facility.”) (internal quotations and citation omitted).

5 These courts have focused on the requirement that the facility be one “through which an  
6 electronic communication service is provided.” 18 U.S.C. § 2701(a)(1). As the Fifth Circuit put  
7 it, “[t]he relevant ‘facilities’ that the SCA is designed to protect are not computers that enable the  
8 use of an electronic communication service, but instead are facilities that are operated by  
9 electronic communication service providers and used to store and maintain electronic storage.”  
10 *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 792 (5th Cir. 2012) (emphasis in original) (holding  
11 that plaintiff’s cell phone was not a “facility”). An individual’s personal device “does not provide  
12 an electronic communication service just because the device enables use of electronic  
13 communication services,” *id.* (emphasis in original); rather, that device is, in every practical sense,  
14 the “user.” Moreover, as another court in this district pointed out, a contrary reading would  
15 “render other parts of the statute illogical,” such as the provision at 18 U.S.C. § 2701(c)(1)  
16 permitting an ECS provider to authorize access to the facility. *In re iPhone Application Litig.*, 844  
17 F. Supp. 2d at 1058 (“It would certainly seem odd that the provider of a communication service  
18 could grant access to one’s home computer to third parties, but that would be the result of  
19 plaintiff’s argument.”); see also *In re Google*, 806 F.3d at 147 (“And this is consistent with the  
20 Act’s purpose: home computers are already protected by the Fourth Amendment, so statutory  
21 protections are not needed.”).

22 Thus, the weight of authority supports Defendants’ position. Plaintiffs, meanwhile, have  
23 failed even to respond, let alone show that the Google Assistant Enabled Devices at issue are  
24 factually distinct from the above situations. Under these circumstances, the Court does not believe  
25 Plaintiffs’ current allegations permit an inference that their personal Google Assistant Enabled  
26 Devices constitute “facilities.”

27 Plaintiffs also argue that “Google’s remote servers” constitute the requisite facilities. *Opp.*  
28 at 9. But of course, Defendants have authorization to access their own servers. See 18 U.S.C. §

1 2701(c)(1); accord *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1026–27 (“The SCA grants immunity  
2 to 18 U.S.C. § 2701(a) claims to electronic communication service providers . . . for accessing  
3 content on their own servers.”); *In re Google, Inc. Privacy Policy Litig.*, No. C–12–01382–PSG,  
4 2013 WL 6248499, at \*12 (N.D. Cal. Dec. 3, 2013) (“Whatever the propriety of Google’s actions,  
5 it plainly authorized actions that it took itself.”). Hence, though the servers are indisputably  
6 “facilities,” there cannot have been “unauthorized access” by Defendants. Any claim that  
7 Defendants improperly “process[ed]” or “disseminat[ed]” Plaintiffs’ communications, Mot. at 10,  
8 is properly brought under 18 U.S.C. § 2702(a), as assessed below.

9 Because Plaintiffs have not pleaded unauthorized access to a “facility” within the meaning  
10 of the SCA, their SCA claim under § 2701(a) is DISMISSED. Although the Court is skeptical that  
11 Plaintiffs will be able to articulate yet another theory of unlawful access to an electronic storage  
12 “facility”, the Court will nonetheless grant LEAVE TO AMEND.

13 **ii. Unlawful Disclosure under 18 U.S.C. § 2702(a)**

14 Next, turning to Plaintiffs’ claim for unlawful disclosure 18 U.S.C. § 2702(a), Plaintiffs  
15 allege that Defendants did not have authorization to disclose any audio recordings or transcripts  
16 resulting from false accepts, but nonetheless did so “for analysis or other purposes, including  
17 improving the functionality of Google Assistant for Google’s own financial benefit and targeting  
18 personalized advertising to users.” Consol. FAC ¶ 122.

19 First, to the extent Plaintiffs assert a claim based on Defendants’ use of audio or transcripts  
20 to “target[] personalized advertising to users,” the Court agrees with Defendants that this claim  
21 fails. There are no allegations in the Consolidated FAC suggesting that Defendants disclose any  
22 information to “third parties” to accomplish this purpose. Defendants’ own use of Plaintiffs’ data  
23 for advertising purposes does not constitute an unlawful “disclosure.” The Court therefore  
24 DISMISSES WITH LEAVE TO AMEND any claim based on targeted advertising.

25 On the other hand, the Consolidated FAC does contain allegations of disclosure to third  
26 parties for the purpose of improving the Google Assistant’s voice recognition functionality; these  
27 third parties are the “subcontractors” Defendants allegedly use to perform the relevant analysis.  
28 See Consol. FAC ¶¶ 35, 39. Defendants move to dismiss this claim on the ground that any

1 disclosure was consented to by Plaintiffs. Mot. at 10. As relevant here, § 2702(b)(3) permits an  
2 ECS provider to divulge the contents of a communication “with the lawful consent of the  
3 originator or an addressee or intended recipient of such communication, or the subscriber in the  
4 case of remote computer service.” Defendants say that Plaintiffs (the originator of the purported  
5 communications) explicitly consented to any disclosure to “subcontractors” that Defendants may  
6 have used by agreeing to Defendants’ Privacy Policy. Mot. at 10-11. Plaintiffs acknowledge that  
7 they are bound by the Privacy Policy, which forms the basis for their breach of contract and breach  
8 of express warranty claims. See Consol. FAC ¶¶ 2, 192, 210. The question then becomes whether  
9 the Privacy Policy adequately indicated to users that Defendants would engage in the disclosures  
10 at issue, such that users could fairly be said to have “agreed” to these disclosures. In re Facebook,  
11 Inc., Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019). The Court  
12 considers this question “objectively, from the perspective of a reasonable . . . user.” Id.

13 The Privacy Policy, of which the Court has taken judicial notice, see *infra* Part III, contains  
14 a section entitled “When Google shares your information.” ECF 56-1 at 30. That section states,  
15 “We do not share your personal information with companies, organizations, or individuals outside  
16 of Google except in the following cases.” ECF 56-1 at 30. It then goes on to state that one of  
17 these instances is “for external processing”:

18 We provide personal information to our affiliates and other trusted  
19 businesses or persons to process it for us, based on our instructions  
20 and in compliance with our Privacy Policy and other appropriate  
21 confidentiality and security measures. For example, we use service  
22 providers to help us with customer support.

23 Id. at 31.

24 Plaintiffs contend that this provision is too general to conclusively establish consent, and  
25 the Court agrees. See Opp. at 11. The Privacy Policy says nothing about the types of information  
26 that Defendants might send to “affiliates and other trusted business or persons” for “processing.”  
27 Critically, moreover, the Privacy Policy does not indicate that such “processing” might involve  
28 human reviewers listening to the audio. Under these circumstances, the Court cannot say that a  
reasonable user reading the Privacy Policy must have understood it to cover the disclosures  
alleged in the Consolidated FAC. As the party seeking the benefit of an exception, Defendants

1 have the burden to establish the existence of consent. See *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at  
2 1028. It also bears repeating that, at the motion to dismiss stage, the Court must give Plaintiffs the  
3 benefit of all reasonable inferences. Where, as here, “the contract language at issue is reasonably  
4 susceptible to more than one interpretation, with one of those interpretations suggesting consent  
5 and another belying it, the Court cannot decide the consent issue in [Defendants’] favor.” *In re*  
6 *Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d at 789.

7 Other courts in this district have come to the same conclusion when evaluating similarly  
8 vague language. In particular, the instant terms bear a close resemblance to those in *Campbell v.*  
9 *Facebook Inc.*, 77 F. Supp. 3d 836 (N.D. Cal. 2014). There, Facebook’s counsel argued that their  
10 disclosure “that Facebook ‘may use the information we received about you’ for ‘data analysis.’”  
11 *Id.* at 847. The court held, however, that “this disclosure is not specific enough to establish that  
12 users expressly consented to the scanning of the content of their messages . . . for alleged use in  
13 targeted advertising.” *Id.*; see also *id.* at 848 (“[A]ny consent with respect to the processing and  
14 sending of messages itself does not necessarily constitute consent to the specific practice alleged  
15 in this case—that is, the scanning of message content for use in targeted advertising.”). The court  
16 in *In re Facebook, Inc., Consumer Privacy User Profile Litigation* made a similar point:  
17 “Although Facebook points to a section in its Data Use Policy entitled ‘Service Providers’ which  
18 says ‘we give your information to the people and companies that help us provide, understand, and  
19 improve the services we offer,’ that statement does not come close to disclosing the massive  
20 information-sharing program with business partners that the plaintiffs allege in the complaint.”  
21 402 F. Supp. 3d at 792. So too here.

22 In an effort to supplement the Privacy Policy’s notice regarding information sharing,  
23 Defendants highlight another provision in the Privacy Policy:

24 We also use your information to ensure our services are working as  
25 intended, such as tracking outages or troubleshooting issues that you  
26 report to us. And we use your information to make improvements to  
27 our services—for example, understanding which search terms are  
28 most frequently misspelled helps us improve spell-check features  
used across our services.

ECF 56-1 at 24. However, this provision comes in a different section of the Privacy Policy,

1 entitled “Why Google collects data.” A reasonable user cannot be expected to connect the two  
2 sections and anticipate that Defendants may use “external processing” for any purpose for which  
3 Defendants collect data. Put another way, although users may have consented to Google’s  
4 collection of their data to “to improve the functionality of the Assistant,” Mot. at 11 (quoting  
5 Consol. FAC ¶ 122), that consent does not reasonably extend to disclosure of data. The Court  
6 DENIES Defendants’ motion to dismiss the § 2702(a) claim on the ground that Plaintiffs’  
7 consented to any disclosures.

8 Defendants assert an additional reason for dismissal in a footnote: They maintain that their  
9 subcontractors are “employees or agents” and not “third parties” under § 2702(a). See Mot. at 10-  
10 11 n.3. The Court rejects this argument, which is hardly even developed. That the putative third  
11 parties here are referred to as “subcontractors” does not, by itself, defeat Plaintiffs’ claim. After  
12 all, whether an entity is a “third party” within the meaning of the statute is a factual question,  
13 interrogating the relationship between the entity and the provider. Moreover, the relevant facts are  
14 likely unavailable to Plaintiffs prior to discovery. Construing the allegations in Plaintiffs’ favor,  
15 the Court finds that the “subcontractors” may be third parties, which suffices at the motion to  
16 dismiss stage. Defendants’ motion to dismiss for failure to plead that subcontractors are “third  
17 parties” is DENIED.

18 In sum, the Court finds that Plaintiffs have adequately pleaded a claim for unlawful  
19 disclosure under 18 U.S.C. § 2702(a) based on Defendants’ disclosure of audio and transcripts to  
20 subcontractors for analysis “to improve the functionality” of the Google Assistant.

### 21 **C. Counts 3 and 4: California Invasion of Privacy Act**

22 Counts 3 and 4 of the Consolidated FAC assert violations of the California Invasion of  
23 Privacy Act (“CIPA”), Cal. Penal Code §§ 630, et seq. Consol. FAC ¶¶ 127-146. The CIPA is the  
24 California state law analogue to the federal Wiretap Act, enacted in 1967 in response to “advances  
25 in science and technology [that] have led to the development of new devices and techniques for  
26 the purpose of eavesdropping upon private communications.” Cal. Penal Code § 630; see  
27 *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014). Two provisions of the  
28 CIPA are implicated in the instant case: Count 3 asserts a violation of California Penal Code §

1 631, which addresses “wiretapping,” and Count 4 asserts a violation of California Penal Code §  
2 632, which addresses “eavesdropping.”

3 Defendants move to dismiss both counts on several grounds, as set forth below.

4 **i. Section 631**

5 To briefly describe the statutory framework, California Penal Code § 631 addresses  
6 “wiretapping.” As relevant here, § 631(a) imposes liability upon

7 Any person who, by means of any machine, instrument, or  
8 contrivance, or in any other manner, intentionally taps, or makes any  
9 unauthorized connection, whether physically, electrically,  
10 acoustically, inductively, or otherwise, with any telegraph or  
11 telephone wire, line, cable, or instrument, including the wire, line,  
12 cable, or instrument of any internal telephonic communication  
13 system, or who willfully and without the consent of all parties to the  
14 communication, or in any unauthorized manner, reads, or attempts to  
15 read, or to learn the contents or meaning of any message, report, or  
16 communication while the same is in transit or passing over any wire,  
17 line, or cable, or is being sent from, or received at any place within  
18 this state; or who uses, or attempts to use, in any manner, or for any  
19 purpose, or to communicate in any way, any information so obtained  
20 . . . .

21 Cal. Penal Code § 631(a). The California Supreme Court has clarified that this lengthy provision  
22 contains three operative clauses protecting against “three distinct and mutually independent  
23 patterns of conduct”: (i) “intentional wiretapping,” (ii) “willfully attempting to learn the contents  
24 or meaning of a communication in transit over a wire,” and (iii) “attempting to use or  
25 communicate information obtained as a result of engaging in either of the two previous activities.”  
26 *Tavernetti v. Superior Court*, 22 Cal. 3d 187, 192 (1978); accord *In re Google Inc.*, No. 13-MD-  
27 02430-LHK, 2013 WL 5423918, at \*15 (N.D. Cal. Sept. 26, 2013). Count 3 purports to allege  
28 violations of all three clauses in that “(i) Google made an unauthorized connection with Class  
Members’ GAEDs; (ii) through the unauthorized interception, Google learned the contents of  
Plaintiffs’ and Class Members’ confidential communications; and (iii) Google transmitted the  
contents of the confidential communications to Google’s servers as well as to third-party  
vendors.” *Opp.* at 13 (citations omitted); see *Consol. FAC* ¶¶ 135-36.

In their motion to dismiss, Defendants argue that Plaintiffs cannot state a claim based on  
any of the three types of conduct prohibited by § 631(a) because the provision prohibits only



1 connections with a “wire, line, or cable” and hence “does not apply to in-person verbal  
2 communications” Mot. at 13. The Court considers this argument as to each clause.

3 Beginning the first clause of § 631(a), Defendants are correct that it protects only  
4 communications that are made over a “wire, line, or cable.” This is evident from the plain text of  
5 the statute: The first clause expressly requires that the unauthorized “connection” be made with  
6 “any telegraph or telephone wire, line, cable, or instrument.” Cal. Penal Code § 631(a); accord  
7 *Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 8200619, at \*18 (N.D. Cal. Aug. 12,  
8 2016) (explaining that “the first clause” of § 631(a) is “limited to communications passing over  
9 ‘telegraph or telephone’ wires, lines, or cables”). Plaintiffs do not dispute this; they also do not  
10 explain how their allegations satisfy the requirement of a “telegraph or telephone wire, line, cable,  
11 or instrument.” Nor does the Consolidated FAC suggest that the Google Assistant operates using  
12 telegraph or telephone wires. In light of the foregoing, the Court finds that Plaintiffs fail to state a  
13 claim for violation of § 631(a) based on intentional wiretapping.

14 The Court turns next to the second clause, which applies to any person who “willfully and  
15 without the consent of all parties to the communication, or in any unauthorized manner, reads, or  
16 attempts to read, or to learn the contents or meaning of any message, report, or communication  
17 while the same is in transit or passing over any wire, line, or cable, or is being sent from, or  
18 received at any place within this state.” 18 U.S.C. § 631(a). Defendants argue that this clause also  
19 requires a “wire, line, or cable.” Plaintiffs object, citing *In re Google Inc. Gmail Litigation*, 2013  
20 WL 5423918. But that case simply stands for the proposition that “the limitation of ‘telegraphic  
21 or telephone’ on ‘wire, line, cable, or instrument’ in the first clause of the statute” is not “imported  
22 to the second clause of the statute”; it did not find that the second clause lacked the requirement of  
23 a “wire, line, or cable.” *Id.* at \*20; accord *Matera*, 2016 WL 8200619, at \*18 (explaining that “the  
24 second clause prohibits the unauthorized interception of communications passing over ‘any wire,  
25 line, or cable’”).

26 However, Plaintiffs also point out that the second clause applies if a communication is “in  
27 transit or passing over any wire, line, or cable, or is being sent from, or received at any place  
28 within this state.” Because the clause is written in the disjunctive, the Court agrees that it could be

1 read to cover messages “being sent from, or received at any place within this State,” without  
2 regard to whether the sending and receiving makes use of a “wire, line, or cable.” See Opp. at 13.

3 At the same time, California courts have often distinguished the essential concepts of  
4 eavesdropping under § 632 and wiretapping under § 631 on the ground that eavesdropping “does  
5 not require an unauthorized connection to a transmission line, whereas wiretapping does.” People  
6 v. Guzman, 11 Cal. App. 5th 184, 192 n.7 (Ct. App. 2017), *aff’d*, (2019) (emphasis in original).  
7 And, as already noted, the California Supreme Court summarized the second clause as proscribing  
8 “wilfully attempting to learn the contents or meaning of a communication in transit over a wire.”  
9 Tavernetti, 22 Cal. 3d at 192. Yet, the question of whether a defendant may be liable under  
10 § 631(a) for reading or attempting to read communications not sent over a wire, line or cable does  
11 not appear to have been squarely considered by other courts.

12 This Court may also leave that question to another day. That is because Plaintiffs have not  
13 plausibly alleged that their communications were being “sent from, or received at any place within  
14 this State.” Although it may be possible for a communication to be “sent” or “received” without  
15 use of a wire, line or cable, it cannot fairly be said that a face-to-face conversation between two  
16 people in the same location involves “sending” or “receiving” communications within the meaning  
17 of the § 632. Per the Consolidated FAC, the “communications” of which the Defendants are  
18 alleged to have “learned the contents” are oral conversations that took place in the presence of  
19 Plaintiffs’ GAEDs. But as already discussed, Plaintiffs have not alleged any information about  
20 these conversations—they have not even plausibly alleged that they themselves were party to  
21 intercepted conversations. Of particular relevance here, there are no facts from which the Court  
22 could infer that any communications were being “sent from” and “received at” different locations;  
23 on the contrary, the Consolidated FAC suggests that the conversations were had in person. The  
24 Court therefore GRANTS Defendants’ motion to dismiss any claim based on the second clause of  
25 § 631(a).

26 Last, the third clause covers any “attempt[] to use or communicate information obtained as  
27 a result of engaging in either of the two previous activities.” Tavernetti, 22 Cal. 3d at 192. In  
28 other words, Plaintiffs must establish that the information at issue—here, the recordings and

1 transcripts that Defendants’ allegedly analyzed—was obtained through a violation of the first or  
 2 second clauses. Because Plaintiffs have not done so, they also have failed to plead a violation of  
 3 the third clause of § 631(a).

4 For these reasons, Count 3 is DISMISSED. Although Plaintiffs’ theories as currently  
 5 alleged do not appear to be compatible with § 631, the Court will nevertheless grant LEAVE TO  
 6 AMEND to clarify those theories.

7 **ii. Section 632**

8 Defendants next challenge Plaintiffs’ claim under California Penal Code § 632, which  
 9 addresses “eavesdropping on or recording confidential communications.” Specifically, § 632(a)  
 10 imposes liability upon

11 A person who, intentionally and without the consent of all parties to  
 12 a confidential communication, uses an electronic amplifying or  
 13 recording device to eavesdrop upon or record the confidential  
 14 communication, whether the communications is carried on among the  
 15 parties in the presence of one another or by means of a telegraph,  
 16 telephone, or other device, except a radio . . . .

17 “California courts interpret ‘eavesdrop,’ as used in section 632, to refer to a third party secretly  
 18 listening to a conversation between two other parties.” *Thomasson v. GC Services Ltd. P’ship*,  
 19 321 Fed. App’x. 557 (9th Cir. 2008) (citing *Ribas v. Clark*, 38 Cal.3d 355, 363 (1985)); see also  
 20 *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002) (§ 632 prohibits “unconsented-to  
 21 eavesdropping or recording of conversations”). Count 4 alleges that Defendants violate this  
 22 provision by “creat[ing] recordings . . . of Plaintiffs’ and Class Members’ confidential  
 23 communications not preceded by the utterance of a hot word or where the Google Assistant  
 24 Enabled Device was not manually activated.” Consol. FAC ¶ 152.

25 A claim under § 632 bears many similarities to a claim under the federal Wiretap Act. See,  
 26 e.g., *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 954 (N.D. Cal. 2014) (“Because  
 27 NovelPoster is unable to allege a violation of the Wiretap Act, it is also unable to allege a violation  
 28 of CIPA.”). In particular, it covers only (1) “confidential communications” and (2) “intentional”  
 conduct. Defendants therefore move to dismiss the § 632 claim for two of the reasons already  
 discussed as to Count 1: that Plaintiffs have not adequately pleaded that their conversations were

1 “confidential” or that Defendants’ alleged interceptions were “intentional” rather than inadvertent.

2 Taking the latter first, the Court considered the parties’ arguments regarding whether  
3 Defendants’ conduct could be considered “intentional” as to Plaintiffs’ Wiretap Act claim. As  
4 explained, the Court finds that Defendants’ failure to rectify the defect causing “false accepts” or  
5 destroy the recordings produced under such circumstances could plausibly be considered  
6 “intentional” rather than “a result of accident or mistake.” See supra Part IV.A.i. The result is the  
7 same under the CIPA, as the CIPA does not define “intentional” more restrictively than the  
8 Wiretap Act. See Mot. at 13; *Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 435 (2018)  
9 (“[T]he recording of a confidential conversation is intentional if the person using the recording  
10 equipment does so with the purpose or desire of recording a confidential conversation, or with the  
11 knowledge to a substantial certainty that his use of the equipment will result in the recordation of  
12 a confidential conversation.”) (quoting *People v. Superior Court of Los Angeles Cty.*, 70 Cal. 2d  
13 123, 134 (1969)) (emphasis in original). Defendants’ motion to dismiss for failure to plead  
14 “intentional” eavesdropping is therefore DENIED.

15 In the same vein, though, the Court agrees that Plaintiffs have not adequately pleaded  
16 “confidential communications.” The California Supreme Court has held that a conversation is  
17 “confidential” under § 632 “if a party to that conversation has an objectively reasonable  
18 expectation that the conversation is not being overheard or recorded.” *Kearney v. Salomon Smith*  
19 *Barney, Inc.*, 39 Cal. 4th 95, 117 n. 7 (2006); see also *Faulkner v. ADT Sec. Services, Inc.*, 706  
20 F.3d 1017, 1019 (9th Cir. 2013). Neither party disputes that this standard is the same as the  
21 “reasonable expectation of privacy” required under the Wiretap Act, 18 U.S.C. § 2510(2). See  
22 Mot. at 14; Opp. at 15. The Court already concluded that the Consolidated FAC does not  
23 adequately demonstrate Plaintiffs’ reasonable expectation of privacy in the conversations that the  
24 Google Assistant alleged intercepted and recorded. See supra Part IV.A.ii. That same defect  
25 afflicts Plaintiffs’ § 632 claim, wherefore the Court must GRANT Defendants’ motion to dismiss  
26 Count 4. As with the Wiretap Act claim, the Court gives LEAVE TO AMEND.

27 Having dismissed Count 4 for failure to allege “confidential communications,” the Court  
28 need not address Defendants’ additional argument that Plaintiffs “have not alleged facts showing

1 that the parties did not consent to the alleged recording.” Mot. at 14. The Court nonetheless  
2 advises Plaintiffs to further develop their contention that Defendants lacked consent to listen or  
3 record, as required to state a claim under § 632(a). Plaintiffs’ allegation that the recordings “were  
4 made without Plaintiffs’ consent” is conclusory. Consol. FAC ¶ 152. Meanwhile, Plaintiffs made  
5 little effort to respond to Defendants’ argument in their Opposition briefing, opting to reference  
6 their arguments regarding consent under the SCA, 18 U.S.C. § 2702(a). But the SCA claim  
7 concerned unlawful disclosure to third parties—not the initial recording of Plaintiffs’  
8 conversations. Moreover, whereas consent is a defense under the SCA, “[i]t appears that, under  
9 California law, the plaintiff bringing a CIPA claim has the burden to prove that the defendant  
10 lacked consent to record.” *Reyes v. Educ. Credit Mgmt. Corp.*, 773 Fed. App’x 989, 990 n.1 (9th  
11 Cir. 2019). Plaintiffs therefore cannot simply rest on their arguments regarding consent as to the  
12 SCA claim.

13 **D. Counts 5 and 6: Common Law Intrusion upon Seclusion and Invasion of**  
14 **Privacy**

15 Plaintiffs’ next two claims are also California state law claims: Count 5 is the common law  
16 tort of intrusion upon seclusion and Count 6 is invasion of privacy in violation of the California  
17 Constitution, Art. I, Sec. 1. Consol. FAC ¶¶ 162, 187. Defendants move to dismiss both claims.  
18 Because the common law and constitutional sources of privacy protection under California law are  
19 closely related, the Court treats them together. See *Hernandez v. Hillside, Inc.*, 47 Cal. 4th 272,  
20 286 (2009).

21 To state a claim for intrusion upon seclusion, a plaintiff must allege “(1) intrusion into a  
22 private place, conversation or matter (2) in a manner highly offensive to a reasonable person.”  
23 *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998)). As to the first element, the  
24 plaintiff must have had an “objectively reasonable expectation of seclusion or solitude in the  
25 place, conversation or data source.” *Id.* at 232. “The second common law element essentially  
26 involves a policy determination as to whether the alleged intrusion is “highly offensive” under the  
27 particular circumstances.” *Hernandez*, 47 Cal. 4th at 287. “Relevant factors include the degree  
28 and setting of the intrusion, and the intruder’s motives and objectives.” *Id.*

1 To allege a violation of California’s constitutional right to privacy, a plaintiff must allege  
2 “(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the  
3 circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the  
4 protected privacy interest.” *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1024 (N.D. Cal. 2012)  
5 (citing *Hill v. Nat’l Collegiate Athletic Ass’n*, 7 Cal. 4th 1, 35-37 (1994)). Regarding the first  
6 element, the California Supreme Court has explained that “[l]egally recognized privacy interests  
7 are generally of two classes: (1) interests in precluding the dissemination or misuse of sensitive  
8 and confidential information (‘informational privacy’); and (2) interests in making intimate  
9 personal decisions or conducting personal activities without observation, intrusion, or interference  
10 (‘autonomy privacy’).” *Hill*, 7 Cal. 4th at 35. The third element, meanwhile, requires the invasion  
11 to be “sufficiently serious in [its] nature, scope, and actual or potential impact to constitute an  
12 egregious breach of the social norms underlying the privacy right.” *Id.* at 37.

13 In this case, Plaintiffs allege that Defendants’ practice of “intercepting, recording,  
14 transmitting, and disclosing” Plaintiffs’ communications in false accept situations “constitute[s] an  
15 intentional intrusion” upon Plaintiffs’ seclusion “in that Google effectively placed itself in the  
16 middle of a conversation to which it was not invited.” *Consol. FAC* ¶ 164. Plaintiffs further  
17 allege that this same practice invades Plaintiffs’ informational privacy interest “in the confidential  
18 and sensitive information” contained in their communications as well as Plaintiffs’ autonomy  
19 privacy interest “in conducting their personal activities.” *Id.* ¶ 179.

20 As evident from the foregoing, the constitutional and common law causes of action overlap  
21 substantially. Accordingly, the California Supreme Court has recognized that “the largely parallel  
22 elements of these two causes of action” require a court to consider “(1) the nature of any intrusion  
23 upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion,  
24 including any justification and other relevant interests.” *Hernandez*, 47 Cal. 4th at 288. In their  
25 motion to dismiss, Defendants argue that (1) Plaintiffs have failed to allege a “reasonable  
26 expectation of privacy” in the communications at issue and (2) the alleged intrusion is not  
27 sufficiently “offensive” or “serious” to support a claim for invasion of privacy or intrusion upon  
28 seclusion. *Mot.* at 15.

1 First, Defendants contend that Plaintiffs have not shown that they had a “reasonable  
2 expectation of privacy” in the conversations upon which Defendants allegedly intruded. Mot. at  
3 15. They are correct. As the Court already explained with respect to Plaintiffs’ Wiretap Act  
4 claim, Plaintiffs have not alleged sufficient information about the conversations that were  
5 allegedly intercepted and recorded to establish that they were had under circumstances that would  
6 give rise to a reasonable expectation of privacy. See supra Part IV.A.ii. That deficiency is fatal to  
7 Plaintiffs’ claims for invasion of privacy and intrusion upon seclusion.

8 In addition, Defendant argue that Plaintiffs have not alleged sufficient facts to establish a  
9 “highly offensive” or “serious” invasion of privacy. Mot. at 15-16. It is true, as Defendants  
10 emphasize, that “[t]he California Constitution and the common law set a high bar” for an intrusion  
11 to be actionable. Low, 900 F. Supp. 2d at 1025 (collecting cases). Many courts have found that  
12 the collection—and even disclosure to certain third parties—of personal information about the  
13 users of a technology may not constitute a sufficiently “egregious breach of social norms” to make  
14 out a common law or constitutional privacy claim. See, e.g., *In re Google, Inc. Privacy Policy*  
15 *Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (no intrusion claim based on Google’s collection  
16 and disclosure of users’ data, including their browsing histories); Low, 900 F. Supp. 2d at 1025  
17 (finding that LinkedIn did not commit a “highly offensive” invasion of users’ privacy by  
18 disclosing users’ browsing histories to third parties); *In re iPhone Application Litig.*, 844 F. Supp.  
19 2d 1040, 1063 (N.D. Cal. 2012) (finding no invasion of privacy based on Defendants’ disclosure  
20 of each user’s addresses, geolocation, the unique device identifier assigned to the user’s device,  
21 gender, age, time zone, and information about app usage). These courts have characterized the  
22 collection and disclosure of such data as “routine commercial behavior.” Low, 900 F. Supp. 2d at  
23 1025 (quoting *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011)).

24 Nonetheless, the Court is not persuaded that the conduct Plaintiffs have described is not  
25 “highly offensive” or “serious” as a matter of law. Although it is a close call, the Court believes  
26 that a reasonable person could find Defendants’ alleged conduct to be “highly offensive.”

27 To begin with, the Court observes that courts have repeatedly found the surreptitious  
28 recording of a plaintiff’s conversations or activity to constitute an actionable intrusion. See, e.g.,

1 Shulman v. Grp. W Prods., Inc., 18 Cal. 4th 200, 237, 955 P.2d 469, 494 (1998), as modified on  
2 denial of reh'g (July 29, 1998); Safari Club Int'l v. Rudolph, No. SACV131989JVSANX, 2014  
3 WL 12577408, at \*8 (C.D. Cal. May 14, 2014). Plaintiffs' allegations that Defendants recorded  
4 their private conversations without authorization could be considered more analogous to these  
5 surreptitious recording cases than cases involving, for instance, browsing history. That human  
6 reviewers are alleged to listen to the recordings makes the analogy to surreptitious recording  
7 especially apt.

8 In any event, determining whether an intrusion is "highly offensive" requires a fact-  
9 intensive inquiry that "examine[s] all of the surrounding circumstances." Hernandez, 47 Cal. 4th  
10 at 295. Such an inquiry cannot be conducted at the motion to dismiss stage where, as here, there  
11 are open factual questions regarding "the likelihood of serious harm to the victim, the degree and  
12 setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests  
13 or social norms render the intrusion inoffensive." In re Facebook, Inc. Internet Tracking Litig.,  
14 2020 WL 1807978, at \*11 ("The ultimate question of whether Facebook's tracking and collection  
15 practices could highly offend a reasonable individual is an issue that cannot be resolved at the  
16 pleading stage."). In particular, false accepts are, by definition, situations in which the user is not  
17 attempting to use the relevant technology. A reasonable person could thus find that Defendants  
18 have no justifiable "motive" or "objective" for making the alleged interceptions, or that the  
19 "degree" of the intrusion is especially great. See id. ("Plaintiffs' allegations of surreptitious data  
20 collection when individuals were not using Facebook are sufficient to survive a dismissal motion  
21 on the issue.").

22 Many other factual circumstances remain to be ascertained. Take for instance the  
23 frequency with which false accepts occur and the amount of information that is subsequently  
24 recorded. As the California Supreme Court has recognized in the context of surreptitious  
25 surveillance, the scope or frequency of recording affects the offensiveness and seriousness of the  
26 privacy intrusion; "electronic surveillance that is persistent and pervasive may constitute a tortious  
27 intrusion on privacy even when conducted in a public or semi-public place." Hernandez, 47 Cal.  
28 4th at 297. Other relevant factors include the content of the recordings and the degree to which



1 the recordings are anonymized.

2 In sum, Plaintiffs have failed adequately to plead claims for intrusion upon seclusion or  
3 invasion of privacy because they have not established a reasonable expectation of privacy in the  
4 conversations or the recordings thereof. If they are able to do so, however, the Court believes that  
5 any dispute regarding the offensiveness of Defendants' alleged conduct is ill-suited for resolution  
6 on a motion to dismiss. Defendants' motion to dismiss Counts 5 and 6 is GRANTED WITH  
7 LEAVE TO AMEND.

8 **E. Count 7: Common Law Breach of Contract**

9 Count 7 is a claim for breach of contract based on Defendants' Terms of Service ("TOS")  
10 and the Privacy Policy contained therein. Consol. FAC ¶¶ 188-201. In order to plead a claim for  
11 breach of contract, Plaintiffs must allege: (1) the existence of a contract with Defendants, (2) their  
12 performance under that contract, (3) Defendants breached that contract, and (4) they suffered  
13 damages. In re Facebook, Inc. Internet Tracking Litig., 2020 WL 1807978, at \*14 (citing Oasis  
14 West Realty, LLC v. Goldman, 51 Cal. 4th 811, 821 (2011)). Defendants move to dismiss on the  
15 grounds that (1) Plaintiffs have failed to identify the specific provisions that have allegedly been  
16 breached; (2) there has been no breach, in any event; and (3) Plaintiffs have not alleged an  
17 adequate damages theory. See Mot. at 16-18.

18 **i. Specific Contractual Provisions**

19 The Court begins with Defendants' contention that Plaintiffs have not identified the  
20 specific contractual provisions creating the obligation Defendants are said to have breached, which  
21 the Court confirms Plaintiffs must do. See Miron v. Herbalife Int'l, Inc., 11 Fed. App'x. 927, 929  
22 (9th Cir. 2001); Young v. Facebook, Inc., 790 F. Supp. 2d 1110, 1117 (N.D. Cal. 2011).

23 Defendants do not dispute that the TOS and the Privacy Policy are binding agreements to  
24 which they are parties. See Mot. at 16. Hence, there is no dispute that any provisions contained  
25 therein would be actionable in Plaintiffs' breach of contract claim. The Consolidated FAC alleges  
26 that Defendants breached the provision of the Privacy Policy promising, "We do not share your  
27 personal information with companies, organizations, or individuals outside of Google except in  
28 the following cases": "with your consent," "with domain administrators," "for external

1 processing,” and “for legal reasons.” ECF 56-1 at 31-32; see Consol. FAC ¶¶ 192-93. Under the  
2 subheading entitled “with your consent,” the Privacy Policy elaborates:

3 We’ll share personal information outside of Google when we have  
4 your consent. For example, if you use Google Home to make a  
5 reservation through a booking service, we’ll get your permission  
6 before sharing your name or phone number with the restaurant. We’ll  
7 ask for your explicit consent to share any sensitive personal  
8 information.

9 See ECF 56-1 at 30. The Consolidated FAC specifically highlights the statement, “We’ll ask for  
10 your explicit consent to share any sensitive personal information.” See Consol. FAC ¶ 193. The  
11 Court finds these provisions to be alleged with particularity, as required to state a claim for breach  
12 of contract.

13 However, these are the only contractual provisions that may form the basis for Plaintiffs’  
14 breach of contract claim. As the Court will explain, the other provisions referenced in the  
15 Consolidated FAC are not actionable.

16 First, in their Opposition brief, Plaintiffs assert a violation of another provision of the  
17 Privacy Policy: one stating that Defendants “may” collect “voice and audio information when you  
18 use audio features.” Opp. at 18 (quoting ECF 56-1 at 22). The Consolidated FAC makes no  
19 reference to this provision, which means the Court cannot consider it to be alleged for purposes of  
20 the instant motion. *Broom v. Bogan*, 320 F.3d 1023, 1026 n.2 (9th Cir. 2003) (“In determining the  
21 propriety of a Rule 12(b)(6) dismissal, a court may not look beyond the complaint to a plaintiff’s  
22 moving papers, such as a memorandum in opposition to a defendant’s motion to dismiss.”).

23 Additionally, Plaintiffs attempt to base their contract claim upon various provisions from  
24 different websites, including the “Google Nest Help Center” and the “Google Safety Center.” See  
25 Consol. FAC ¶¶ 193-94. Plaintiffs assert that these websites are “incorporated into Google’s TOS  
26 or Privacy Policy” by virtue of the following provision in the TOS:

27 Our Services are very diverse, so sometimes additional terms or  
28 product requirements (including age requirements) may apply.  
Additional terms will be available with the relevant Services, and  
those additional terms become part of your agreement with us if you  
use those Services.

Consol. FAC ¶ 191; see ECF 56-1 at 13. But this vague statement is hardly sufficient to establish  
that the particular websites cited by Plaintiffs are part of the TOS or otherwise are binding upon

1 the parties. Although it certainly possible that statements on the cited websites constitute binding  
2 agreements between the parties, Plaintiffs have not plausibly alleged this to be so.

3 All told, the only specific contractual terms allegedly breached are Defendants' promises  
4 in the Privacy Policy (1) not to share users' "personal information" "outside of Google" except in  
5 the four stated circumstances (2) to "ask for [users'] explicit consent to share any sensitive  
6 personal information."

7 **ii. Breach**

8 The Court now turns to whether Plaintiffs have plausibly alleged that Defendants breached  
9 these terms of the Privacy Policy. In Plaintiffs' view, these provisions amount to a promise that  
10 Defendants will not share users' "personal information" with "companies organizations, or  
11 individuals outside of Google except . . . [with the express consent of the user]." Opp. at 19  
12 (alterations in original). Plaintiffs then assert that Defendants violate this promise by "shar[ing]  
13 the audio recording obtained from Plaintiffs and the Class with third-party vendors without  
14 Plaintiffs' consent in order to improve the functionality of the Google Assistant and not for  
15 external processing of users' request or queries." Id.

16 At the outset, the Court observes that in paraphrasing the relevant terms, Plaintiffs have  
17 altered them. Remember, the Privacy Policy listed four circumstances under which it would share  
18 users' personal information: "with your consent," "with domain administrators," "for external  
19 processing," and "for legal reasons." To establish a breach, then, Plaintiffs must not only plead  
20 that Defendants lacked consent, but also that their conduct does not fall within the other three  
21 circumstances. The Consolidated FAC has not done this. It all but ignores the existence of these  
22 three circumstances, focusing only on the alleged lack of consent. See Consol. FAC ¶¶ 197-99.

23 The Consolidated FAC falls short for another reason: It does not adequately plead that  
24 Plaintiffs' "personal information" has been shared. The vague and conclusory allegation that  
25 Plaintiffs "private conversations" were recorded and disclosed does not suffice. Consol. FAC ¶  
26 199. As already discussed multiple times, Plaintiffs have not plausibly alleged that Plaintiffs' own  
27 conversations were intercepted. See supra Part IV.A.ii. Relevant here, the Consolidated FAC  
28 contains no allegations describing the content of those conversations or the circumstances under

1 which they were had. See *id.* In the absence of such allegations, the Court has no basis upon  
2 which to infer that Plaintiffs’ “sensitive personal information” is implicated.

3 For these reasons, the Court finds that Plaintiffs have not stated a claim for breach of  
4 contract and DISMISSES Count 7. The Court will grant LEAVE TO AMEND.

5 **iii. Damages**

6 Although the Court need not do so, it now briefly considers the parties’ arguments  
7 regarding Plaintiffs’ damages theories. Plaintiffs proffer three damages theories: (1) benefit of the  
8 bargain, (2) “harm to [Plaintiffs]” “privacy interests,” and (3) “disgorgement of profits made by  
9 Google as a result of its breach of contract.” Consol. FAC ¶ 201; see Opp. at 19. Defendants  
10 believe all of these theories to be flawed. See Mot. at 18-19.

11 The first theory is benefit of the bargain damages: “Plaintiffs seek damages resulting from  
12 their overpayment for the GAEDs, which they allege are worth less due to Google’s breaches of  
13 contract.” Opp. at 19; see Consol. FAC ¶ 201. Also known as expectation damages, a benefit of  
14 the bargain measure of damages is intended “to give the injured party the benefit of his bargain  
15 and insofar as possible to place him in the same position he would have been in had the promisor  
16 performed the contract.” *Coughlin v. Blair*, 262 P.2d 305, 314 (Cal. 1953); see also *Twin City  
17 Fire Ins. Co. v. Philadelphia Life Ins. Co.*, 795 F.2d 1417, 1425 (9th Cir. 1986).

18 Courts have approved damages based on benefit of the bargain in several technology cases  
19 involving privacy. For instance, in *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, Plaintiff  
20 Mortensen alleged that he paid “\$19.95 each year since December 2007 for Yahoo’s premium  
21 email service” but did not acquire the full value of Yahoo’s service because it was not secure. 313  
22 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018). There, Plaintiff Mortensen plausibly lost the benefit of  
23 the bargain in that he received a less valuable email service than the one he paid for. See *id.*  
24 Similarly, in *In re Anthem, Inc. Data Breach Litig.*, plaintiffs paid premiums to defendants for  
25 health insurance plans. No. 15-MD-02617-LHK, 2016 WL 3029783, at \*7-\*8 (N.D. Cal. May 27,  
26 2016). When the defendants experienced various breaches of its database containing individuals’  
27 health record information, the plaintiffs alleged, *inter alia*, that the defendants had breached their  
28 privacy policies. *Id.* at \*9. The Court allowed the plaintiff to pursue a theory of benefit of the

1 bargain losses on the theory that some portion of their premiums went toward paying for robust  
2 security measures, which they allegedly did not receive. *Id.* at \*13.

3 In this case, however, Plaintiffs have not alleged that they paid anything to Defendants for  
4 the Google Assistant. Not only does the Consolidated FAC say nothing about any fee or premium  
5 paid, it appears that the Google Assistant is available free of charge for use on Google Assistant  
6 Enabled Devices. See Consol. FAC ¶ 21. As a result, it cannot be said that Plaintiffs received less  
7 than what they paid for—they appeared to have paid nothing. See *In re LinkedIn User Privacy*  
8 *Litig.*, 932 F. Supp. 2d 1089, 1093 (N.D. Cal. 2013) (rejecting plaintiffs’ benefit of the bargain  
9 theory because “the FAC fails to allege that Plaintiffs actually provided consideration for the  
10 security services which they claim were not provided”). The Court therefore does not believe that  
11 benefit of the bargain is a viable damages theory.

12 On the other hand, Plaintiffs’ second theory of damages—harm to their privacy interests—  
13 is more promising. Generally, a plaintiff may seek damages for “the detriment caused by the  
14 breach.” *Stephens v. City of Vista*, 994 F.2d 650, 657 (9th Cir. 1993) (citing Cal. Civ. Code §  
15 3300). In this case, the detriment Plaintiffs say they suffered was an invasion of their privacy.  
16 Plaintiffs are entitled to seek compensatory damages or perhaps nominal damages for such harm.  
17 See *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d at 802; Cal. Civ.  
18 Code § 3360. The problem is that Plaintiffs have not sufficiently alleged an invasion of their  
19 privacy in the Consolidated FAC. As the Court has explained, the Consolidated FAC does not  
20 plausibly allege that Plaintiffs’ own private conversations were intercepted. See Part IV.A.ii. If  
21 Plaintiffs are able to cure that deficiency, the Court believes they would be able to seek damages  
22 based on harm to their privacy interests.

23 Plaintiffs’ third theory of damages suffers from a similar problem, but may also be viable.  
24 That theory is that Plaintiffs are entitled to “disgorgement of profits made by Google as a result of  
25 its breach of contract.” Consol. FAC ¶ 201. The Ninth Circuit has said that “under California  
26 law, a defendant’s unjust enrichment can satisfy the ‘damages’ element of a breach of contract  
27 claim, such that disgorgement is a proper remedy.” *Foster Poultry Farms, Inc. v. SunTrust Bank*,  
28 377 Fed. App’x 665, 669 (9th Cir. 2010) (citing *Ajaxo Inc. v. E\*Trade Group, Inc.*, 135 Cal. App

1 4th 21, 56-57 (2005)). The Ninth Circuit has further held that “California law recognizes a right to  
2 disgorgement of profits resulting from unjust enrichment, even where an individual has not  
3 suffered a corresponding loss.” In re Facebook, Inc. Internet Tracking Litig., 2020 WL 1807978,  
4 at \*5-\*6.

5 To plead a theory of disgorgement, Plaintiffs must show “that they retain a stake in the  
6 profits garnered.” Id. at \*6. Plaintiffs attempt to plead that they are entitled to the “substantial  
7 profits” that Defendants’ have earned using their “personal information” because Defendants’ use  
8 was unauthorized. Consol. FAC ¶¶ 199-200. But Plaintiffs have not adequately alleged that their  
9 unspecified “personal information” has financial value or that Defendants have profited from the  
10 information. Although courts have found that individuals’ browsing history may plausibly carry  
11 financial value, In re Facebook, Inc. Internet Tracking Litig., 2020 WL 1807978, at \*6., Plaintiffs  
12 have not pleaded any description of the “personal information” that Defendants’ allegedly used.  
13 Without such facts, Plaintiffs’ assertion that Defendants garnered “substantial profits” from the  
14 information is purely conclusory. See, e.g., Varga v. Wells Fargo Bank, N.A., 796 Fed. App’x  
15 430, 431 (9th Cir. 2020) (“Varga’s conclusory assertion that she was ‘deprived of the contractual  
16 and consumer protections and benefits’ of the notice provision is insufficient to plausibly allege”  
17 damages.). Should Plaintiffs cure this deficiency, however, the Court believes they could  
18 plausibly demonstrate that any profits were unjustly earned by virtue of Defendants’ use being  
19 allegedly unauthorized. In re Facebook, Inc. Internet Tracking Litig., 2020 WL 1807978, at \*6.

20 **F. Counts 8, 9, 10: Breach of Warranty**

21 Counts 8, 9, and 10 are claims for breach of express and implied warranty; Counts 8 and 9  
22 are brought under California state law and Count 10 is brought under the federal Magnuson-Moss  
23 Warranty Act. Unlike the other counts, these are asserted only by Plaintiffs Kumandan and Spurr,  
24 based upon their purchases of GAEDs manufactured by Defendants. Specifically, Plaintiff  
25 Kumandan allegedly purchased a Google Pixel smartphone and Plaintiff Spurr allegedly  
26 purchased a Google Home. The three claims assert essentially the same factual basis for relief:  
27 Defendants made affirmations of fact or promises to consumers that they would not intercept,  
28 record, or use the consumers’ communications unless hotwords were uttered or the device was

1 manually activated; Defendants subsequently breached these promises.

2 Defendants move to dismiss Counts 8, 9, and 10 on various grounds. As set forth below,  
3 the motion GRANTED WITH LEAVE TO AMEND as to all three claims.

4 **i. Breach of Express Warranty**

5 Count 8 alleges a breach of express warranty. Consol. FAC ¶¶ 202-210. “Any affirmation  
6 of fact or promise made by the seller to the buyer which relates to the goods and becomes part of  
7 the basis of the bargain creates an express warranty that the goods shall conform to the affirmation  
8 or promise.” Cal. Comm. Code § 2313. To plead an action for breach of express warranty under  
9 California law, a plaintiff must allege: (1) the exact terms of the warranty; (2) reasonable reliance  
10 thereon; and (3) a breach of warranty which proximately caused plaintiff’s injury. *Williams v.*  
11 *Beechnut Nutrition Corp.*, 185 Cal. App. 3d 135, 142 (1986). To satisfy the first element, a  
12 plaintiff must identify a “specific and unequivocal written statement,” *Maneely v. Gen. Motors*  
13 *Corp.*, 108 F.3d 1176, 1181 (9th Cir. 1997), “relating to the title, character, quality, identity, or  
14 condition of the sold goods,” *In re Sony PS3 Other OS Litig.*, 551 Fed. App’x 916, 919 (9th Cir.  
15 2014). The statement need not be in a formal warranty document; for instance, “statements made  
16 in a manufacturer’s advertising that are ‘disseminated to the consuming public in order to induce  
17 sales’ can create express warranties.” *Birdsong v. Apple Inc.*, No. C 06-02280 JW, 2007 WL  
18 9723505, at \*5 (N.D. Cal. Dec. 14, 2007) (quoting *Keith v. Buchanan*, 173 Cal. App. 3d 13, 22  
19 (1985)).

20 Defendants move to dismiss this claim for two reasons. First, Defendants argue that  
21 Plaintiffs have not alleged the exact terms of the warranty, as they are required to do at this stage,  
22 see, e.g., *Blennis v. Hewlett-Packard Co.*, No. C 07-00333 JF, 2008 WL 818526, at \*2 (N.D. Cal.  
23 Mar. 25, 2008). Mot. at 19. In response, Plaintiffs simply refer to the Court to its arguments  
24 regarding breach of contract (Count 7). Opp. at 20; see Part IV.E.i. In so doing, Plaintiffs seem to  
25 imply that the same provisions of the Privacy Policy and Terms of Service that form the basis for  
26 their contract claim are also the relevant warranty terms for their warranty claim. But as  
27 Defendants emphasize, the “sold goods” here are the GAEDs that Plaintiffs purchased—not the  
28 Google Assistant software. Plaintiffs have not shown the cited provisions of the Privacy Policy

1 relate to the Google Home or Google Pixel—let alone that they amount to an “explicit guarantee”  
2 about the quality or character of either product. *Hadley v. Kellogg Sales Co.*, 273 F. Supp. 3d  
3 1052, 1092 (N.D. Cal. 2017). Indeed, the cited provisions—which are general assurances about  
4 Defendants’ use and disclosure of user information—do not allude to any particular product or  
5 products.

6 Most of the statements that Plaintiffs cite from the “Google Nest Help Center” and the  
7 “Google Safety Center” webpages fare no better. See Consol. FAC ¶¶ 193-195. There is one  
8 statement, however, that could plausibly be construed as an express warranty term for the Google  
9 Home. In the Frequently Asked Questions section of the Google Nest Help Center cite,  
10 Defendants provided the following response to the question, “Is Google Home recording all of my  
11 conversations?”:

12 No. Google Home listens in short (a few seconds) snippets for the  
13 hotword. Those snippets are deleted if the hotword is not detected,  
14 and none of that information leaves your device until the hotword is  
15 heard. When Google Home detects that you’ve said “Ok Google” or  
16 “Hey Google,” or that you’ve physically long pressed the top of your  
17 Google Home device, the LEDs on top of the device light up to tell  
18 you that recording is happening, Google Home records what you say,  
19 and sends that recording (including the few-second hotword  
20 recording) to Google in order to fulfill your request. You can delete  
21 these recordings through My Activity anytime.

22 *Id.* ¶ 195. This passage pertains to the Google Home device and describes the way that it  
23 functions. The Court finds that this statement about the Google Home is sufficiently specific and  
24 unequivocal, and could plausibly be considered a promise that the Google Home will delete any  
25 recordings “if the hotword is not detected.” However, Plaintiffs have not adequately alleged that  
26 the promise was breached. See Mot. at 17-18. As described in the Consolidated FAC, false  
27 accepts are situations in which a hotword is detected, albeit mistakenly. Plaintiffs must plausibly  
28 plead that retaining recordings when a hotword is mistakenly detected violates a promise to delete  
recording if a hotword is not detected. They have not yet done so.

Accordingly, because Plaintiffs have not identified any particular warranty term that has  
plausibly been breached, Count 8 is DISMISSED WITH LEAVE TO AMEND.

The Court also briefly addresses Defendants’ second ground for dismissal: They argue in a



1 footnote that the Google Home and Google Pixel “are subject to express limited warranties which  
2 state that they are the only express warranty that Google provides for these devices, and provide  
3 an exclusive remedy in the event a defect arises during the warranty period.” Mot. at 19 n.4. In  
4 other words, Defendants disclaim any express warranties beyond the ones they have submitted in  
5 their request for judicial notice. ECF 56-1 ¶¶ 6-7; see id. Ex. E-F. In Part III, the Court took  
6 judicial notice of the existence of the two documents—the “Google Home Warranty – United  
7 States” and the “Hardware limited warranty for Android Hardware devices, including the Pixel  
8 smartphone”—because they are available on public websites. However, the Court made clear that  
9 its judicial notice does not establish that these documents are “valid or binding contracts.” *Datel*  
10 *Holdings*, 712 F. Supp. 2d at 984. That is because the binding effect of the documents is not a  
11 matter that “cannot reasonably be questioned,” Fed. R. Evid. 201.

12 Consequently, the Court cannot yet determine whether the two documents asserted by  
13 Defendants operate to preclude any warranty claim based other statements Defendants have made.  
14 See *Ladore v. Sony Computer Entm’t Am., LLC*, 75 F. Supp. 3d 1065, 1074 (N.D. Cal. 2014)  
15 (“[T]he Court will not consider whether Sony may have effectively disclaimed any express  
16 warranties in its Terms of Service or Software License.”). Therefore, Count 8 is not subject to  
17 dismissal on that basis.

18 To summarize, then, Defendants’ motion to dismiss Count 8 is GRANTED WITH LEAVE  
19 TO AMEND for failure to plead a prima facie case of breach of express warranty, but not based  
20 on the disclaimer proffered by Defendants.

## 21 **ii. Breach of Implied Warranty**

22 Next, Defendants move to dismiss Count 9, Plaintiffs’ claim for breach of the implied  
23 warranty of merchantability. *Consol. FAC* ¶¶ 211-222; see Mot. at 20-21. Plaintiffs have asserted  
24 Count 9 under California Commercial Code § 2314, which is modeled on the Uniform  
25 Commercial Code. See *Consol. FAC* ¶ 217; *Opp.* at 20-21. Defendants move to dismiss this  
26 claim for three reasons, but the Court need only reach the first: that Plaintiffs’ claims are barred by  
27 an explicit disclaimer of the implied warranty of merchantability in its Terms of Service.

28 Defendants cite the following provision from their Terms of Service, of which the Court

1 has taken judicial notice, see supra Part III:

2 Other than as expressly set out in these terms or additional terms,  
3 neither Google nor its suppliers or distributors make any specific  
4 promises about the services. For example, we don't make any  
5 commitments about the content within the services, the specific  
6 functions of the services, or their reliability, availability, or ability to  
7 meet your needs. We provide the services "as is."

8 Some jurisdictions provide for certain warranties, like the implied  
9 warranty of merchantability, fitness for a particular purpose and non-  
10 infringement. To the extent permitted by law, we exclude all  
11 warranties.

12 ECF 56-1 at 16. Plaintiffs do not dispute that they are bound by the TOS or that the disclaimer  
13 contained therein covers the implied warranty of merchantability asserted in Count 9. Cal. Com.  
14 Code § 2316(2) (providing that a disclaimer of the implied warranty of merchantability "must  
15 mention merchantability and in case of a writing must be conspicuous").

16 Plaintiffs nonetheless challenges the validity of the disclaimer by arguing that it is  
17 "unconscionable in that it 'creates an overly harsh or one-sided result that shocks the conscience.'"  
18 Opp. at 22. But Plaintiffs have alleged no facts to support this argument, which is made in a scant  
19 few sentences in their Opposition brief. They simply assert that the TOS is "a non-negotiable  
20 contract of adhesion." Id. That is not enough, for not all contracts of adhesion are  
21 unconscionable. Under California law, a contract provision is unconscionable, and therefore  
22 unenforceable, only if it is both procedurally and substantively unconscionable. See *Armendariz*  
23 *v. Found. Health Psychcare Servs., Inc.*, 24 Cal. 4th 83, 113-14 (2000). Procedural  
24 unconscionability "focus[es] on 'oppression' or 'surprise' due to unequal bargaining power,";  
25 substantive unconscionability focuses on "'overly harsh' or 'one-sided' results." Id. Plaintiffs  
26 have made no non-conclusory allegations to establish either element.

27 Meanwhile, this Court and other courts in this district have dismissed implied warranty  
28 claims based on similar disclaimers. See *In re Nexus 6P Prod. Liab. Litig.*, 293 F. Supp. 3d 888,  
944 (N.D. Cal. 2018) (collecting cases). Under these circumstances, the Court is not persuaded by  
Plaintiffs' cursory argument that the instant disclaimer is unconscionable.

The Court will therefore enforce the disclaimer and GRANT Defendants' Motion to  
Dismiss the implied warranty claim. The Court will grant LEAVE TO AMEND to allege further

1 facts in support of Plaintiffs' unconscionability argument.

2 **iii. Magnuson-Moss Warranty Act**

3 Count 10 alleges a violation of the federal Magnuson-Moss Warranty Act based on breach  
4 of the implied warranty of merchantability. Consol. FAC ¶¶ 223-233. Although the Magnuson-  
5 Moss Warranty Act creates a separate federal cause of action for breach of an implied warranty, it  
6 directs courts to state law to determine the meaning and scope of the implied warranty. See 15  
7 U.S.C. § 2301(7); see *Birdsong v. Apple, Inc.*, 590 F.3d 955, 958 n.2 (9th Cir. 2009). In this case,  
8 Plaintiffs have predicated their Magnuson-Moss Warranty Act claim on a breach of California  
9 state warranty law. See Opp. at 22. The Court has found Plaintiffs' claim for breach of implied  
10 warranty under California law (Count 9) to be inadequately pleaded; consequently, Plaintiffs'  
11 claim under the Magnuson-Moss Warranty Act must also be dismissed. See *Birdsong*, 590 F.3d at  
12 958 n.2 (dismissing plaintiffs' claims under the Magnuson-Moss Act "because we conclude that  
13 the plaintiffs have failed to state a claim for breach of an express or implied warranty" under  
14 California law). Defendants' motion to dismiss is GRANTED WITH LEAVE TO AMEND.

15 **G. Count 11: California UCL**

16 Count 11 is brought under California's Unfair Competition Law ("UCL"), which prohibits  
17 any "unlawful, unfair or fraudulent business practice and unfair, deceptive, untrue or misleading  
18 advertising." Cal. Bus. & Prof. Code § 17200. The California Supreme Court has clarified that  
19 the UCL, because it is "written in the disjunctive," prohibits three separate types of unfair  
20 competition: (1) unlawful acts or practices, (2) unfair acts of practices, and (3) fraudulent acts or  
21 practices. *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999);  
22 accord *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1168 (9th Cir. 2012). To plead a UCL  
23 claim, a plaintiff's allegations must show that a defendant's conduct violates one of these three  
24 "prongs." *Id.* In addition, because a UCL claim may only be brought by "a person who has  
25 suffered injury in fact and has lost money or property as a result of the unfair competition," Cal.  
26 Bus. & Prof. Code § 17204, a plaintiff must "demonstrate some form of economic injury."  
27 *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011). This requirement is sometimes  
28 referred to as "UCL standing." *Id.* at 320-21.

1 In their motion to dismiss, Defendants contend that Plaintiffs have failed to allege  
2 economic injury, which would preclude any UCL claim. Defendants also challenge the  
3 sufficiency of Plaintiffs' allegations as to each of the three prongs ("unlawful," "unfair," and  
4 "fraudulent").

5 **i. Economic injury**

6 The Court begins by addressing Defendants' contention that Plaintiffs have not alleged  
7 economic injury, as necessary to bring a UCL claim. Under California law, a UCL plaintiff must  
8 "(1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e.,  
9 economic injury, and (2) show that that economic injury was the result of, i.e., caused by, the  
10 unfair business practice or false advertising that is the gravamen of the claim." *Kwikset Corp. v.*  
11 *Superior Court*, 51 Cal. 4th 310, 322 (2011). "There are innumerable ways in which economic  
12 injury" may be shown; for instance:

13 A plaintiff may (1) surrender in a transaction more, or acquire in a  
14 transaction less, than he or she otherwise would have; (2) have a  
15 present or future property interest diminished; (3) be deprived of  
16 money or property to which he or she has a cognizable claim; or (4)  
17 be required to enter into a transaction, costing money or property, that  
18 would otherwise have been unnecessary.

19 *Id.* at 323.

20 In the instant case, Plaintiffs advance two theories of economic injury. First, Plaintiffs  
21 allege overpayment for their Google Assistant Enabled Devices, i.e. "that they would not have  
22 purchased their GAEDs, or would have paid less for them, if they had known that Google was  
23 intercepting, recording, disclosing, and otherwise misusing their conversations without their  
24 authorization." *Opp.* at 22 (citing *Consol. FAC* ¶¶ 7, 54, 241). Certainly, overpayment is an  
25 economic injury under the UCL. See, e.g., *Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 966  
26 (9th Cir. 2018), cert. denied, 139 S. Ct. 640 (2018). The question becomes whether Plaintiffs have  
27 pleaded sufficient facts to establish overpayment here.

28 On that issue, Defendants maintain that the Consolidated FAC contains insufficient details  
regarding Plaintiffs' purchase of their Google Assistant Enabled Devices. *Mot.* at 22; *Reply* at 13.  
According to Defendants, the Consolidated FAC merely alleges that Plaintiffs "owned" and

1 “interacted” with GAEDs and not that they purchased their devices. *Id.* (citing Consol. FAC ¶¶  
2 51-53). That is true of Named Plaintiff B.S., who allegedly interacted with a GAED that he did  
3 not own. See Consol. FAC ¶ 51. It is also true of Named Plaintiffs Galvan and E.G., who  
4 allegedly interacted with a device that was not manufactured by Defendants, the Samsung Galaxy  
5 Tab. See *id.* ¶ 53. Because these Named Plaintiffs have failed to allege that they actually paid any  
6 money for a Google Assistant Enabled Device, they cannot have been injured by overpayment.

7 By contrast, the Consolidated FAC does allege that Plaintiffs Kumandan and Spurr  
8 “purchased their Google Manufactured Device either directly from Google or from actual or  
9 apparent agents of Google.” Consol. FAC ¶ 215. This allegation suffices to support an inference  
10 that Plaintiffs Kumandan and Spurr paid for their respective GAEDs. Defendants raise no other  
11 objection to the overpayment theory of damages. The Court therefore finds that Plaintiffs  
12 Kumandan and Spurr have plausibly alleged they would not have purchased their GAEDs, or  
13 would have paid less for them, if they had been aware of Defendants’ practices with regard to false  
14 accepts.

15 Plaintiffs’ second theory of economic injury is that Defendants “wrongfully monetized and  
16 profited from Plaintiffs’ personal content and information, which is of value, entitling Plaintiffs to  
17 restitution.” *Opp.* at 23. According to Plaintiffs, “[e]ntitlement to restitution is sufficient to  
18 demonstrate a loss of money or property under the UCL.” *Opp.* at 23.

19 The Court does not doubt that claims for restitution are often based on actual loss of  
20 money or property, as in the cases Plaintiffs cite. See *In re Anthem, Inc. Data Breach Litig.*, No.  
21 15-MD-02617-LHK, 2016 WL 3029783, at \*32 (N.D. Cal. May 27, 2016) (“All California  
22 Plaintiffs paid premiums, which were in turn used to pay for services by Defendants.”); *In re*  
23 *Google Android Consumer Privacy Litig.*, No. 11-MD-02264 JSW, 2014 WL 988889, at \*5 (N.D.  
24 Cal. Mar. 10, 2014) (“Plaintiffs have alleged sufficient facts to show standing based on the  
25 diminished battery life.”). But Plaintiffs are not absolved of their burden to plead economic injury  
26 by their conclusory assertion that they are entitled to restitution. Plaintiffs’ allegation that  
27 Defendants “wrongfully monetized and profited from Plaintiffs’ personal content and information”  
28 does not give rise to an inference that Plaintiffs “lost money or property,” Cal. Bus. & Prof. Code

1 § 17204. As another court in this district has explained, claiming that a defendant “may have  
2 gained money through its sharing or use of the plaintiffs’ information” is “different from saying  
3 the plaintiffs lost money.” *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F.  
4 Supp. 3d at 804.

5 Moreover, Plaintiffs have not shown that they are, in fact, entitled to restitution under the  
6 UCL. The California Supreme Court has “defined an order for ‘restitution’ as one ‘compelling a  
7 UCL defendant to return money obtained through an unfair business practice to those persons in  
8 interest from whom the property was taken.’” *Korea Supply Co. v. Lockheed Martin Corp.*, 29  
9 Cal. 4th 1134, 1144 (2003). Of relevance here, restitution is distinguished from disgorgement.  
10 “‘Disgorgement’ is a broader remedy than restitution” in that disgorgement “has been used to refer  
11 to surrender of all profits earned as a result of an unfair business practice regardless of whether  
12 those profits represent money taken directly from persons who were victims of the unfair  
13 practice.” *Id.* at 1145 (emphasis in original). By contrast, restitution under the UCL must “restore  
14 the status quo” by “returning to the plaintiff” funds taken from him or “benefits in which the  
15 plaintiff has an ownership interest.” *Id.* at 1148-49. Put another way, restitutionary disgorgement  
16 “focuses on the plaintiff’s loss, and nonrestitutionary disgorgement “focuses on the defendant’s  
17 unjust enrichment.” *Meister v. Mensinger*, 230 Cal. App. 4th 381, 398 (2014). Although the  
18 defendant’s benefit and the plaintiff’s loss are often the same, nonrestitutionary disgorgement may  
19 also be had “where a benefit has been received by the defendant but the plaintiff has not suffered a  
20 corresponding loss.” *Id.* (internal quotations and alterations omitted).

21 Plaintiffs say they are entitled to restitution because Defendants “wrongfully monetized  
22 and profited from Plaintiffs’ personal content and information.” *Opp.* at 23. But “plaintiff’s  
23 assertion that defendants received ill-gotten gain does not make a viable UCL claim unless the  
24 gain was money in which plaintiff had a vested interest.” *Madrid v. Perot Systems Corp.*, 130 Cal.  
25 App. 4th 440, 455 (2005). Here, as discussed in connection with Plaintiffs’ breach of contract  
26 claim, see *supra* Part IV.E.iii, Plaintiffs have not shown that they have a vested interest in any  
27 money earned from unspecified “personal content and information.”

28 To be clear, the Court is not requiring Plaintiffs to show they are entitled to restitution

1 under the UCL in order to establish their standing under the UCL. See *Kwikset Corp.*, 51 Cal. 4th  
 2 at 337 (holding that standing is not dependent on eligibility for restitution). But where, as here,  
 3 Plaintiffs themselves base their standing on eligibility for restitution, Plaintiffs' failure to plead  
 4 their entitlement to restitution under the UCL is fatal.

5 In sum, the Court GRANTS Defendants' motion to dismiss Plaintiff Galvan's, Plaintiff  
 6 B.S.'s, and Plaintiff E.G.'s UCL claims for failure to adequately plead economic injury; the Court  
 7 will GRANT LEAVE TO AMEND, however, because they may be able to remedy that defect.  
 8 Plaintiffs Kumandan and Spurr have adequately pleaded economic injury. Because their UCL  
 9 claims shall go forward, the Court proceeds to consider of the adequacy of Plaintiffs' pleadings  
 10 under each prong of the UCL.

11 **i. Unlawful Prong**

12 The "unlawful" prong of the UCL "borrows violations of other laws and treats them as  
 13 unlawful practices that the unfair competition law makes independently actionable." *Cel-Tech*, 20  
 14 Cal. 4th at 180. In other words, to be "unlawful" under the UCL, Defendants' conduct must  
 15 violate another "borrowed" law. *HSBC Bank Nevada*, 691 F.3d at 1168. "Virtually any state,  
 16 federal or local law can serve as the predicate for an action under section 17200." *Id.* (quoting  
 17 *People ex rel. Bill Lockyer v. Fremont Life Ins. Co.*, 104 Cal. App. 4th 508, 515 (2002))  
 18 (alterations omitted). Here, Plaintiffs predicate their "unlawful" claim on Defendants' alleged  
 19 violations of (1) the Wiretap Act, (2) the SCA, (3), the CIPA, (4) the Magnuson-Moss Warranty  
 20 Act, (5) Cal. Bus. & Prof. Code § 22576,<sup>2</sup> for having breached the Privacy Policy, (6) the

21 \_\_\_\_\_  
 22 <sup>2</sup> This provision states:

23 An operator of a commercial Web site or online service that collects  
 24 personally identifiable information through the Web site or online service  
 25 from individual consumers who use or visit the commercial Web site or  
 26 online service and who reside in California shall be in violation of this section  
 27 if the operator fails to comply with the provisions of Section 22575 or with  
 28 the provisions of its posted privacy policy in either of the following ways:

- (a) Knowingly and willfully.
- (b) Negligently and materially.

Cal. Bus. & Prof. Code § 22576. Plaintiffs allege that Defendants violate this provision by virtue  
 of its breach of contract, as alleged in Count 7. *Opp.* at 24; see *Consol. FAC* ¶ 235.

1 California Constitution’s right of privacy, and (7) the common law prohibition of intrusion upon  
2 seclusion. Opp. at 24; see Consol. FAC ¶ 235.

3 Because Plaintiffs assert each of these alleged violations as independent counts, the Court  
4 has already considered the adequacy of Plaintiffs’ allegations as to those counts. The Court’s  
5 findings in that regard are equally determinative of the validity of Plaintiffs’ UCL claim.

6 Accordingly, the Court must DISMISS WITH LEAVE TO AMEND any claims based on (1) the  
7 Wiretap Act, as alleged in Count 1; (2) Section 2701(a) of the Wiretap Act, as alleged in Count 2;  
8 (3) the CIPA, as alleged in Counts 3 and 4; (4) the Magnuson-Moss Warranty Act, as alleged in  
9 Count 10; (5) Cal. Bus. & Prof. Code § 22576, as alleged in Count 7; (6) the California  
10 Constitution’s right of privacy, and (7) the common law prohibition of intrusion upon seclusion.  
11 On the other hand, Plaintiffs have stated a UCL claim based on a violation of Section 2702(a) of  
12 the SCA, which the Court found to be sufficiently pleaded in Count 2. See supra Part IV.ii.

13 Although not addressed in Plaintiffs’ Opposition brief, the Consolidated FAC also alleges  
14 an “unlawful” claim based on California Family Code § 6701, see Consol. FAC ¶¶ 236-38, which  
15 provides:

16 Except as otherwise provided by statute, a contract of a minor may be  
17 disaffirmed by the minor before majority or within a reasonable time  
18 afterwards or, in case of the minor’s death within that period, by the  
19 minor’s heirs or personal representative.

20 The Consolidated FAC alleges that Defendants have run afoul of this provision by failing to obtain  
21 “minor Plaintiff B.S.’s or E.G.’s consent to intercept, record, disclose, or use their confidential  
22 communications.” Consol. FAC ¶ 238.

23 In their motion to dismiss, Defendants argue that Plaintiffs have not shown how the facts  
24 of this case implicate a minor’s right of disaffirmance. Mot. at 24. The Court agrees that it is not  
25 clear how Plaintiffs’ allegations pertain to the statute, and Plaintiffs have provided no explanation  
26 in their Opposition briefing. Based on Plaintiffs’ lack of response, the Court considers the claim  
27 based on California Family Code § 6701 abandoned and the argument conceded. *Montgomery v.*  
28 *Specialized Loan Servicing, LLC*, 772 Fed. App’x 476, 477 (9th Cir. 2019) (“The district court  
properly dismissed plaintiffs’ remaining claims because plaintiffs failed to respond to the



1 arguments raised in defendants’ motion to dismiss these claims.”) (citing *Walsh v. Nev. Dep’t of*  
 2 *Human Res.*, 471 F.3d 1033, 1037 (9th Cir. 2006)).

3 For these reasons, Plaintiffs may proceed with their UCL claim premised on Section  
 4 2702(a) of the SCA; Defendants’ motion to dismiss is otherwise GRANTED.

5 **ii. Fraudulent Prong**

6 The UCL also provides a cause of action against “fraudulent” business acts or practices. “A  
 7 business practice is fraudulent under the UCL if members of the public are likely to be deceived.”  
 8 *HSBC Bank Nevada*, 691 F.3d at 1169 (citing *Puentes v. Wells Fargo Home Mortg., Inc.*, 160 Cal.  
 9 *App. 4th* 638, 645 (2008)). In their Opposition brief, Plaintiffs argue that they “adequately allege  
 10 affirmative misrepresentations” and “omissions,” which are presumably meant to form the basis of  
 11 a claim that Plaintiffs have engaged in “fraudulent” business practices. *Opp.* at 23. But the  
 12 Consolidated FAC does not purport to assert a claim under the fraudulent prong of the UCL. See  
 13 *Consol. FAC* ¶¶ 234-242. Furthermore, the Consolidated FAC makes no mention of “affirmative  
 14 misrepresentations” or “omissions”; certainly, it has not identified any misrepresentations or  
 15 omissions with particularity.

16 The lack of specific allegations regarding the allegedly fraudulent business practices is  
 17 especially problematic here because claims under the fraudulent prong of the UCL are subject to  
 18 “the heightened pleading requirements of Rule 9(b).” *Davidson v. Kimberly-Clark Corp.*, 889  
 19 *F.3d* 956, 964 (9th Cir. 2018). To satisfy Rule 9(b), “a pleading must identify the who, what,  
 20 when, where, and how of the misconduct charged, as well as what is false or misleading about the  
 21 purportedly fraudulent statement.” *Cafasso, U.S. ex rel. v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d  
 22 1047, 1055 (9th Cir. 2011). Plaintiffs have not done any of the above. Defendants’ motion to  
 23 dismiss is therefore GRANTED WITH LEAVE TO AMEND.

24 **iii. Unfair Prong**

25 Last, Plaintiffs allege that Defendants have “engaged in business acts or practices deemed  
 26 ‘unfair’ under the UCL.” *Consol. FAC* ¶ 239.

27 “The UCL does not define the term ‘unfair.’ In fact, the proper definition of ‘unfair’  
 28 conduct against consumers is currently in flux among California courts.” *Hodsdon v. Mars, Inc.*,

1 891 F.3d 857, 866 (9th Cir. 2018) (internal quotations omitted). For some years, the California  
2 Courts of Appeal formulated different tests, such as whether the practice “offends an established  
3 public policy or when the practice is immoral, unethical, oppressive, unscrupulous or substantially  
4 injurious to consumers,” *Cel-Tech*, 20 Cal. 4th at 184 (quoting *S. Bay Chevrolet v. Gen. Motors*  
5 *Acceptance Corp.*, 72 Cal. App. 4th 861, 887 (1999)) (“South Bay test”), or whether “the gravity  
6 of the harm to the alleged victim” outweighs “the utility of the defendant’s conduct,” *id.* (quoting  
7 *State Farm Fire & Casualty Co. v. Superior Court*, 45 Cal. App. 4th 1093, 1104 (1996)) (“State  
8 Farm Fire test”). Then, in *Cel-Tech*, the California Supreme Court appeared to confine “unfair”  
9 to “conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit  
10 of one of those laws because its effects are comparable to or the same as a violation of the law, or  
11 otherwise significantly threatens or harms competition.” 20 Cal. 4th at 187. “It further required  
12 that ‘any finding of unfairness to competitors under section 17200 be tethered to some  
13 legislatively declared policy or proof of some actual or threatened impact on competition.’”  
14 *HSBC Bank Nevada*, 691 F.3d at 1170 (quoting *Cel-Tech*, 20 Cal. 4th at 185). The *Cel-Tech*  
15 Court explained that the prior definitions were “too amorphous” and “provide[d] too little  
16 guidance to courts and businesses.” *HSBC Bank Nevada*, 691 F.3d at 1169 (quoting *Cel-Tech*, 20  
17 Cal. 4th at 185).

18 However, the *Cel-Tech* court expressly limited its decision, stating, “Nothing we say  
19 relates to actions by consumers or by competitors alleging other kinds of violations of the unfair  
20 competition law such as ‘fraudulent’ or ‘unlawful’ business practices or ‘unfair, deceptive, untrue  
21 or misleading advertising.’” *Cel-Tech*, 20 Cal. 4th at 187 n.12. Consequently, California courts  
22 remain divided on whether the *Cel-Tech* definition applies to “consumer actions” or whether the  
23 *State Farm Fire* and *South Bay* tests remain valid. See *HSBC Bank Nevada*, 691 F.3d at 1170.  
24 The Ninth Circuit has noted this continued controversy but awaits the California Supreme Court’s  
25 resolution of it. See *id.*; *Hodsdon*, 891 F.3d at 866.

26 In this case, the parties follow the Ninth Circuit’s lead and argue under both *Cel-Tech* and  
27 the prior balancing tests from *State Farm Fire* and *South Bay*. See *Consol. FAC* ¶ 239.

28 First, as to Plaintiffs’ claim that Defendants’ conduct is unfair under the *Cel-Tech* test, the

1 Court agrees with Defendants that Plaintiffs have not alleged any harm to competition or violation  
2 of the “letter, policy, or spirit of the antitrust laws,” *HSBC Bank Nevada*, 691 F.3d at 1170. See  
3 *Mot.* at 24. Indeed, the Court cannot discern a single allegation in the Consolidated FAC  
4 pertaining to competitive harm. Plaintiffs’ brief in Opposition makes no attempt to explain or  
5 defend their omissions, wherefore the Court considers the claim abandoned. See *Montgomery*,  
6 772 Fed. App’x at 477.

7 Second, as to the pre-Cel-Tech definitions of “unfair,” some courts have treated the State  
8 Farm Fire and South Bay tests as distinct tests; others, including the Ninth Circuit, have referred  
9 to them together as the “balancing test,” see *HSBC Bank Nevada*, 691 F.3d at 1169; Accord  
10 *Herskowitz v. Apple Inc.*, 940 F. Supp. 2d 1131, 1146 (N.D. Cal. 2013). In any event, the parties  
11 agree that both tests require the Court to “weigh the utility of the defendant’s conduct against the  
12 gravity of the harm to the alleged victim.” *Mot.* at 25; *Opp.* at 25 (quoting *HSBC Bank Nevada*,  
13 691 F.3d at 1169). Plaintiffs say that Defendants’ actions have harmed Plaintiffs by “illegally  
14 wiretapping and wrongfully transmitting to third parties Plaintiffs’ confidential communications.”  
15 *Opp.* at 25. Defendants object that, considering the substantial benefit the Google Assistant  
16 provides to consumers, Plaintiffs “cannot reasonably allege” that the utility of their Google  
17 Assistant Enabled Devices is outweighed by the “occasional error” of false accepts. *Mot.* at 25.

18 Just how “occasional” the error is, however, is a question of fact that remains unanswered  
19 at this stage. Moreover, the harm that is asserted here is the invasion of privacy, which is difficult  
20 to quantify. The Court cannot say, as a matter of law, that the utility of the Google Assistant  
21 necessarily outweighs the harm from false accepts. Accord *In re Carrier IQ, Inc.*, 78 F. Supp. 3d  
22 1051, 1117 (N.D. Cal. 2015) (“The cost-benefit analysis this test calls for is not properly suited for  
23 resolution at the pleading stage.”); *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040  
24 (N.D. Cal. 2012) (“While the benefits of Apple’s conduct may ultimately outweigh the harm to  
25 consumers, this is a factual determination that cannot be made at this stage of proceedings.”).

26 The Court nevertheless finds that Plaintiffs’ “unfair” claim is deficient because, as  
27 discussed in Part IV.A.ii., the Named Plaintiffs failed to adequately plead that their own  
28 conversations were intercepted and that those conversations were subject to a reasonable

1 expectation of privacy. That failure means that Plaintiffs have not adequately pleaded “harm to  
2 the alleged victim” for purposes of their UCL claim. The Court therefore must DISMISS  
3 Plaintiffs’ claims under the “unfair” prong of the UCL but will GRANT LEAVE TO AMEND.

4 **H. Count 12: Declaratory Judgment**

5 Defendants do not move to dismiss Count 12, Plaintiffs’ request for declaratory judgment  
6 under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 et seq. Count 12 may proceed.

7 **V. ORDER**

8 For the foregoing reasons, the Court rules on Defendants’ motion to dismiss the 12 Counts  
9 in the Consolidated FAC as follows:

- 10 • Count 1: GRANTED WITH LEAVE TO AMEND.
- 11 • Count 2: GRANTED WITH LEAVE TO AMEND as to the claim under 18 U.S.C.  
12 § 2701(a); DENIED as to the claim under 18 U.S.C. § 2702(a).
- 13 • Count 3: GRANTED WITH LEAVE TO AMEND.
- 14 • Count 4: GRANTED WITH LEAVE TO AMEND.
- 15 • Count 5: GRANTED WITH LEAVE TO AMEND.
- 16 • Count 6: GRANTED WITH LEAVE TO AMEND.
- 17 • Count 7: GRANTED WITH LEAVE TO AMEND.
- 18 • Count 8: GRANTED WITH LEAVE TO AMEND.
- 19 • Count 9: GRANTED WITH LEAVE TO AMEND.
- 20 • Count 10: GRANTED WITH LEAVE TO AMEND.
- 21 • Count 11: GRANTED WITH LEAVE TO AMEND as to the fraudulent and unfair  
22 prongs; DENIED as to the unlawful prong.

23 Any amended complaint is **due by June 5, 2020**. Plaintiffs are directed to file a redlined  
24 complaint as an attachment to any amended complaint. Leave to amend is restricted to the defects  
25 discussed in this Order and in Defendants’ motion; Plaintiff may not add new parties or claims  
26 without obtaining prior express leave of the Court. However, to the extent Plaintiffs fail to cure  
27 the defects identified by this Order, their claims will be subject to dismissal with prejudice.

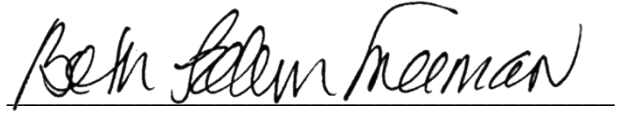
28

United States District Court  
Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**IT IS SO ORDERED.**

Dated: May 6, 2020



BETH LABSON FREEMAN  
United States District Judge