UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE, INC. PRIVACY POLICY LITIGATION

Case No. 5:12-cv-01382-PSG

ORDER GRANTING-IN-PART MOTION TO DISMISS AND GRANTING MOTION TO STRIKE

(Re: Docket Nos. 71, 77)

Over two years ago, Plaintiffs[1] filed this lawsuit against Defendant Google, Inc. for commingling user data across different Google products and disclosing such data to third parties.[2] Since then, the court has twice dismissed Plaintiffs' claims. Google now moves for a third dismissal.

[1] Originally, the complaint named only two Plaintiffs: Robert DeMars and Lorena Barrios. *See* Docket No. 1 at ¶ 27-28. The second amended complaint names five more: Pedro Marti, David Nisenbaum, Nicholas Anderson, Matthew Villani, and Scott McCullough. *See* Docket No. 68 at ¶¶ 25-31.

[2] *See* Docket No. 1.

Like Rocky rising from Apollo's uppercut in the 14th round, Plaintiffs' complaint has sustained much damage but just manages to stand. The court GRANTS the motion, but only IN-PART.

I. BACKGROUND[3]

This is a nationwide, putative class action against Google on behalf of all persons and entities in the United States that acquired a Google account between August 19, 2004 and February 29, 2012, and continued to maintain that Google account on or after March 1, 2012, when a new Google privacy policy went into effect. Plaintiffs also bring nationwide class claims against Google on behalf of (a) all persons and entities in the United States that acquired an Android-powered device between May 1, 2010 and February 29, 2012 and switched to a non-Android device on or after March 1, 2012 (the "Android Device Switch Subclass"); and (b) all persons and entities in the United States that acquired an Android-powered device between August 19, 2004 and the present, and downloaded at least one Android application through the Android Market and/or Google Play (the "Android App Disclosure Subclass").[4]

Google is a technology and advertising company that provides free web-based products to billions of consumers around the world. Google can offer its products free of charge due to its primary business model – advertising. In 2011, Google's revenues were $37.91 billion,

[3] Unless otherwise noted, all facts are drawn from the operative complaint and the docket records in this case. Plaintiffs' motion to strike the declaration of Silva Reyes is GRANTED, as a court is to decide a motion to dismiss based only on the complaint, and documents properly subject to judicial notice. *See Lee v. Cty. Of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001). Plaintiffs dispute the authenticity of the 2009 Mobile Privacy Policy, *see* Docket No. 77 at 2, rendering judicial notice of the document unsuitable. *See* Fed. R. Evid. 203. Because Plaintiffs do not contest the authenticity of the 2008 Mobile Privacy Policy submitted as Exhibit A to the Request for Judicial Notice, *see* Docket No. 76 at 2, the court will consider that document.

[4] *See* Docket No. 68 at ¶ 1.

approximately 95% of which ($36.53 billion) came from advertising. In 2012, Google's revenues increased to $46.04 billion, approximately 95% of which ($43.69 billion) came from advertising.[5]

In order to accomplish this, Google logs personal identifying information, browsing habits, search queries, responsiveness to ads, demographic information, declared preferences and other information about each consumer that uses its products. Google's Gmail service also scans and discloses to other Google services the contents of Gmail communications. Google uses this information, including the contents of Gmail communications, to place advertisements that are tailored to each consumer while the consumer is using any Google product or browsing third-party sites that have partnered with Google to serve targeted ads.[6]

Before March 1, 2012, information collected in one Google product was not automatically commingled with information collected during the consumer's use of other Google products. Google did not, for instance, ordinarily and automatically associate a consumer's Gmail account (and therefore his or her name and identity, his or her private contact list, or the contents of his or her communications) with the consumer's Google search queries or the consumer's use of other Google products like Android, YouTube, Picasa, Voice, Google+, Maps, Docs, and Reader.[7]

Google has always maintained a general or default privacy policy purporting to permit Google to "combine the information you submit under your account with information from other services."[8] However, before the introduction of the new privacy policy on March 1, 2012, this statement was qualified, limited, and contradicted in privacy policies associated with specific Google products, including both Gmail and Android-powered devices. The privacy policies

[5] *See id.* at ¶ 4.

[6] *See id.* at ¶ 5.

[7] *See id.* at ¶ 6

[8] *Id.* at ¶ 7.

associated with Android-powered devices, for example, specified that, although the default terms would generally apply, "[c]ertain applications or features of your Android-powered phone may cause other information [that is, other than certain delimited "usage statistics"] to be sent to Google but in a fashion that cannot be identified with you personally" and that "[y]our device may send us location information (for example, Cell ID or GPS information) that is not associated with your [Google] Account." These categories of information, and certain other discrete categories of Android user information, identified by the terms of the Android-powered device policy in effect prior to March 1, 2012, could affirmatively not be "combine[d] … with information from other services."[9]

On March 1, 2012, however, Google replaced those policies with a single, unified policy that allows Google to comingle user data across accounts and disclose it to third-parties for advertising purposes.[10] Plaintiffs, who each either acquired a Google account or purchased an Android-powered device before or on February 29, 2012, were not pleased and filed this suit.

Plaintiffs brought their original complaint on March 20, 2012 and consolidated it with related actions on June 8, 2012.[11] The complaint presented a bare-bones theory that, by switching to the less-restrictive privacy policy without user consent, Google violated both its prior policies and consumers' privacy rights.[12] However, Plaintiffs did not plead facts sufficient to show concrete economic harm or prima facie statutory or common law violations, so the court dismissed the complaint for lack of standing.[13] Because the court was without jurisdiction to consider

---

[9] *See id.* at ¶ 7.

[10] *See id.* at ¶¶ 5-14.

[11] *See* Docket No. 1; Docket No. 14.

[12] *See* Docket No. 14 at ¶¶ 9-10.

[13] *See* Docket No. 45 at 8-12.

Plaintiffs' substantive allegations, the dismissal provided Plaintiffs leave to amend their complaint.[14]

Plaintiffs' first amended complaint, filed on March 7, 2013, expanded the bounds of the alleged classes, as well as the explanations of Plaintiffs' injuries.[15] After Google again moved to dismiss, the court held that Plaintiffs have sufficiently plead standing,[16] but nonetheless granted the motion because Plaintiffs did not plead sufficient facts to support any of their claims.[17] Although Plaintiffs were granted leave to amend, the court warned "that any further dismissal [would] likely be with prejudice."[18] The most significant allegations added concern Google's plan entitled "Emerald Sea."[19] Unveiled within Google as early as May, 2010,[20] Emerald Sea's apparent objective was "to reinvent [Google] as a social-media advertising company."[21] The plan's execution involves creating cross-platform dossiers of user data that would allow third-parties to better tailor advertisements to specific consumers.[22] Plaintiffs allege that despite this objective, Google left in place the prior policies in order to avoid tipping-off consumers.[23] They cast Emerald

[14] *See id.* at 12.

[15] *See* Docket No. 50 at ¶¶ 19-22, 35-7, 128-91.

[16] In finding standing, the court relied on Plaintiffs' allegations of (a) economic harm in the forms of involuntary battery and bandwidth consumption, expenditures on replacement devices in order to avoid Google's privacy policy, and overpayment for devices in reliance on fraudulent privacy statements; and (b) violations of statutory rights. *See* Docket No. 67 at 11-17.

[17] *See id.* at 18-30.

[18] *Id.* at 30.

[19] Docket No. 68 at ¶ 9.

[20] *See id.* at ¶¶ 9-10.

[21] *Id.* at ¶ 9.

[22] *See id.* at ¶¶ 10, 12-13, 16, 49, 51, 57, 75.

[23] *See id*. at ¶¶ 11, 126-27, 146.

Sea as evidence of Google's intent to deceive consumers by disregarding existing privacy policies in pursuit of ad revenue.[24]

With these new allegations in place, Plaintiffs allege effectively the same harms as before. The class as a whole complains that commingling and disseminating user data violates Google's prior privacy policies and constitutes an unreasonable invasion of consumer privacy.[25] The Android Device Switch Subclass further complains that in order to avoid such an invasive policy, the class members replaced their Android devices and incurred costs in doing so.[26] Additionally, the Android Application Disclosure Subclass claims Google's disclosures to third parties caused increased battery and bandwidth consumption as well as invasions of Plaintiffs' statutory and common law privacy rights.[27] Plaintiffs frame these complaints within six legal theories: violations of the California Consumers Legal Remedies Act ("CLRA"), Federal Wiretap Act, Stored Electronic Communications Act, California's Unfair Competition Law ("UCL"), and common law theories of breach of contract and intrusion upon seclusion.[28]

Google now moves to dismiss this case once and for all, again arguing that Plaintiffs' lack standing and have failed to plead facts sufficient to substantiate their claims.

---

[24] *See id.* at ¶¶ 7, 15, 39, 76, 114, 124-27, 156, 159, 271, 292-93, 300.

[25] *See id.* at ¶¶ 149, 150, 151.

[26] *See id*. at ¶¶ 17, 146, 160.

[27] *See id.* at ¶¶ 18, 19, 147-48, 161-193.

[28] *See id.* at ¶¶ 250-343. Because the court previously dismissed them, Plaintiffs bring their claims for breach of contract and those under the Federal Wiretap Act and Stored Electronic Communications Act for appellate preservation purposes only. *See id.* at 75, 77, 80 nn.1-3. These claims would have been preserved for appeal, regardless of whether they were re-plead. *See Lacey v. Maricopa Cnty*., 693 F.3d 896, 928 (9th Cir.2012) (overruling prior rule that claims not re-alleged are waived and holding that "[f]or claims dismissed with prejudice and without leave to amend, we will not require that they be repled in a subsequent amended complaint to preserve them for appeal").

II. LEGAL STANDARDS

A. Article III Standing

To satisfy Article III, a plaintiff "must show that (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[29] A suit brought by a plaintiff without Article III standing is not a "case or controversy," and an Article III court lacks subject matter jurisdiction over the suit.[30] In that event, the suit should be dismissed under Fed. R. Civ. Pro. 12(b)(1).[31]

The injury required by Article III may exist by virtue of "statutes creating legal rights, the invasion of which creates standing."[32] In such cases, the "standing question . . . is whether the constitutional or standing provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief."[33] At all times the threshold question of standing "is distinct from the merits of [a] claim" and does not require "analysis of the merits."[34] The Supreme Court also has instructed that the "standing inquiry requires careful

---

[29] *See Friends of the Earth, Inc. v. Laidlaw Envtl. Sys. (TOC), Inc.*, 528 U.S. 167, 180-181 (2000).

[30] *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 101 (1998).

[31] *See Steel Co.*, 523 U.S. at 109-110; *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000).

[32] *See Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010) (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975)).

[33] *See id.* (quoting *Warth*, 422 U.S. at 500).

[34] *Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011).

judicial examination of a complaint's allegations to ascertain whether the particular plaintiff is entitled to an adjudication of the particular claims asserted."[35]

B. Rule 12(b)(6)

A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief."[36] If a plaintiff fails to proffer "enough facts to state a claim to relief that is plausible on its face," the complaint may be dismissed for failure to state a claim upon which relief may be granted.[37] A claim is facially plausible "when the pleaded factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged."[38] Accordingly, under Fed. R. Civ. P. 12(b)(6), which tests the legal sufficiency of the claims alleged in the complaint, "[d]ismissal can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory."[39] "A formulaic recitation of the elements of a cause of action will not do."[40]

On a motion to dismiss, the court must accept all material allegations in the complaint as true and construe them in the light most favorable to the non-moving party.[41] The court's review is limited to the face of the complaint, materials incorporated into the complaint by reference, and matters of which the court may take judicial notice.[42] However, the court need not accept as true

---

[35] *DaimlerChrysler*, 547 U.S. at 352 (quoting *Allen v. Wright*, 468 U.S. 737, 752 (1984)); *see also Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1121-22 (9th Cir. 2010).

[36] Fed. R. Civ. P. 8(a)(2).

[37] *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

[38] *Ashcroft v. Iqbal*, 556 U.S. 662, 663 (2009).

[39] *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990).

[40] *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

[41] *See Metzler Inv. GMBH v. Corinthian Colls., Inc.*, 540 F.3d 1049, 1061 (9th Cir. 2008).

[42] *See id.* at 1061.

allegations that are conclusory, unwarranted deductions of fact, or unreasonable inferences.[43]

"Dismissal with prejudice and without leave to amend is not appropriate unless it is clear . . . that the complaint could not be saved by amendment."[44]

III. DISCUSSION

As in prior motions, Google attacks Plaintiffs' operative complaint on two fronts. First, it argues that Plaintiffs lack standing to bring their claims at all. Second, it argues that even if they have standing, Plaintiffs have once again failed to plead their claims in more than a conclusory manner, such that they must be dismissed under *Iqbal* and *Twombly*.

A. Standing

In its earlier order, the court explained that Plaintiffs had standing to raise their claims based on: (1) the greater discharge of battery power and system resources due to unauthorized activity; (2) the costs incurred by each named plaintiff when he bought a new phone after the policy change, since his initial phone choice was substantially driven by privacy concerns; (3) the injury incurred overpaying for Android devices based on Google's misrepresentation about certain features; (4) violation of statutory rights bestowed by the Wiretap Act; (5) violations of statutory rights bestowed by the Stored Communications Act and (6) violations of statutory rights bestowed by Cal. Civ. Code § 3344.[45] In light of the claims Plaintiffs now pursue, only the first two reasons remain pertinent. Google argues that those two do not give rise to Article III standing and that all of Plaintiffs' other injury theories "fail anew for the same reasons they failed last time."[46] Google

[43] *See Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001); *see also Twombly*, 550 U.S. at 561 ("a wholly conclusory statement of [a] claim" will not survive a motion to dismiss).

[44] *Eminence Capital, LLC v. Asopeon, Inc.*, 316 F.3d 1048, 1052 (9th Cir. 2003).

[45] *See* Docket No. 67 at 13-17.

[46] Docket No. 71 at 6.

separately argues Plaintiffs' standing based on an alleged risk of future harm from data commingling and disclosure to third parties is insufficient. As explained below, while the latter argument is persuasive, the former arguments are not.

1. Alleged Heightened Risks of Future Harms Do Not Confer Standing

Google initially challenges the Application Disclosure subclass' standing to bring its claims for unfair competition and intrusion upon seclusion.[47] Google argues that the heightened security risk Plaintiffs allege as a result of their data being disclosed to app developers does not amount to Article III injury-in-fact.[48] Indeed, this court's prior order held that unauthorized disclosure in and of itself did not confer standing.[49] In response to that order, however, Plaintiffs have expanded their allegations to explain that the relevant injury is not the mere unauthorized disclosure of user data, but rather the fact that such disclosure exposes users "to a substantially increased, unexpected, and unreasonable risk of further interception or dissemination of their personal information as well as of other adverse consequences, including harassment, receipt of unwelcome communications, and identity theft."[50]

The Ninth Circuit has recognized that the improper disclosure of personal information can give rise to standing based on the threat of future harm so long as that harm is credible, real, and immediate, and not merely conjectural or hypothetical.[51] But establishing such a credible, real, and

---

[47] *See* Docket No. 68 at ¶¶ 287, 302.

[48] *See* Docket No. 71 at 8-9.

[49] *See id.* at 9 (citing Docket No. 45 at 10).

[50] Docket No. 68 at 42.

[51] *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (finding standing where plaintiffs alleged that employer's negligence and breach of implied contract under state law resulted in theft of a laptop containing sensitive employee data and thus an increased risk of identity theft although such theft had not yet occurred); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) ("injury in fact [must be] concrete and particularized, and actual or imminent, not conjectural or hypothetical.") (internal citations and quotations omitted).

immediate harm is no small feat. For example, in *Low v. LinkedIn*, the court found no such harm, even where a digital service provider was alleged to have disclosed information to (un)authorized third-parties.[52] Similarly, in *Yunker v. Pandora*, the court found insufficient harm to confer standing where the defendant, a music service provider, shared personal information without anonymizing it.[53] Each of these courts concluded that the alleged risk of future harm posed by the defendant's conduct was too conjectural and hypothetical to fall within the scope of the Ninth Circuit's standard. [54]

The alleged threat of future harm in this case is similarly conjectural. The information disclosure is markedly distinguishable from that in *Krottner*: there, disclosure was a result of laptop theft containing sensitive personal information of almost 100,000 Starbucks employees.[55] Here, no

[52] *See Low v. LinkedIn Corp.*, Case No. 5:11-cv-01468-LHK, 2011 WL 5509848, at *3-4 (N.D. Cal. Nov. 11, 2011) (holding that plaintiff did not have standing based on defendant's practice of transmitting user ID's to third parties to track and aggregate browser history); *see also Opperman v. Path, Inc*., Case No. 4:13-cv-00453-JST, 2014 WL 1973378, at *24 ("Plaintiffs assert a common law claim for invasion of privacy. Regardless of the merits of that claim, the Court finds Plaintiffs' allegations sufficient on [the] point [of standing]. The essence of the standing inquiry is to determine whether the plaintiff has 'alleged such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends.' It is beyond meaningful dispute that a plaintiff alleging invasion of privacy as Plaintiffs do here presents a dispute the Court is permitted to adjudicate." (quoting *Baker v. Carr*, 369 U.S. 186, 204 (1962)); *cf. In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1054 (N.D. Cal. 2012) (finding standing where Plaintiffs specifically alleged devices used, defendants and apps that accessed or tracked personal information and resulting harm).

[53] *See Yunker v. Pandora Media, Inc.*, Case No. 4:11 cv-03113-JSW, 2013 WL 1282980, at *5 (N.D. Cal. Mar. 26, 2013) (finding risk of future harm insufficient to establish standing where plaintiff alleged that online music provider failed to anonymize his personal information).

[54] *See also Frezza v. Google Inc.*, Case No. 5:12-cv-00237-RMW, 2013 WL 1736788, at *6 (N.D. Cal. Apr. 22, 2013) (dismissing claim for failure to plead injury-in-fact where plaintiff alleged that defendant retained, but did not disclose, credit card information); *Whitaker v. Health Net of California, Inc.*, Case No. 11-0910-KJM, 2012 WL 174961, at *4 (E.D. Cal. Jan. 20, 2012) (dismissing claims for lack of injury-in-fact where Plaintiff alleged loss, but not theft or publication, of plaintiff's information).

[55] *See Krottner*, 628 F.3d at 1140.

criminal activity is alleged to have been involved.[56] Google's authorized third-party disclosure not only differentiates this case from *Krottner*, but also brings it in line with *Low* and *Yunker*.[57]

2. Plaintiff Nisenbaum's Phone Replacement Still Confers Standing

Google's second argument against standing targets the injury that Nisenbaum asserts in bringing the Device Switch Subclass' UCL and CLRA claims. Google argues that Nisenbaum has not suffered an actual harm that would confer standing because (a) based on his purchase date, he was a party to a 2009 privacy policy—not the 2008 privacy policy upon which his claim is based—that expressly allows data commingling, and (b) the court's prior holding that phone replacement conferred standing no longer applies because he now alleges that Google's failure to disclose its intention to disregard its policy, rather than fear of data commingling, was the cause of replacement.[58] The court previously found standing based on Nisenbaum's allegation that he would not have replaced his Android but for Google's change in policy.[59]

Google's arguments are not persuasive. First, the court's granting Plaintiffs' motion to strike Google's submission of the 2009 privacy policy renders the first half of Google's argument moot. Accepting Plaintiffs' allegations as true, Nisenbaum was a party to the 2008 privacy policy giving rise to his claim. Second, and of more substantive import, the court's prior ruling that the

[56] *See Krottner*, 628 F.3d at 1143 ("Were Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible.").

[57] *See Low*, 2011 WL 5509848 at *6 (Plaintiff "has not yet articulated . . . a particularized and concrete harm as the plaintiffs did in *Krottner* . . . . [Plaintiff] has not alleged that his credit card number, address, and social security number have been stolen or published or that he is a likely target of identity theft as a result of [defendant]'s practices. Nor has [Plaintiff] alleged that his sensitive personal information has been exposed to the public.").

[58] *See* Docket No. 71 at 6-7; Docket No. 78 at 3-4.

[59] *See* Docket No. 67 at 13-14.

economic injury resulting from Nisenbaum's phone replacement still applies.[60] Nisenbaum still alleges that but for the policy switch he would not have otherwise bought a new phone[61] and this injury is still fairly traceable to Google's (now allegedly fraudulent) prior policies.[62] In sum, although Nisenbaum's ostensible motivation for switching phones has changed from the first to the second amended complaint, his injury remains the same and Google's privacy policy is alleged to be the source of that injury. Nisenbaum's phone replacement therefore continues to bestow standing allowing him to bring UCL and CLRA claims on behalf of the Android Device Switch Subclass.

3. Battery Depletion Confers Standing

Google's third substantive argument against standing attacks the alleged injury to Plaintiffs' battery life caused by Google Play's unauthorized transmission of their information when they download an app.[63] As in previous complaints, the App Disclosure subclass has asserted breach of contract and unfair competition, based on the injury caused by decreased battery life.[64] Google argues that the claims giving rise to that injury are "now gone," and that there is now "no nexus between the claimed violation (Google Play disclosing account information to developers) and the claimed injury (battery use)."[65] Google's reasoning is that app developers access user data from

[60] *See* Docket No. 67 at 14 ("Nisenbaum specifically alleges that but for the policy switch he would not have otherwise have bought a new phone. The alleged injury is fairly traceable to Google based on Mr. Nisenbaum's allegation that he relied on Google's previous policies in purchasing the Android phone in the first place.").

[61] *See* Docket No. 68 at ¶ 262.

[62] *See id.* at ¶ 259-62.

[63] *See* Docket No. 71 at 8.

[64] *See id.* at 69-73.

[65] *Id*.

Google Play's servers, not the user's individual phones, and therefore such optional access does not implicate phone battery consumption.[66]

Google's argument here—challenging the causal nexus between its alleged conduct and the Plaintiffs' alleged injury—requires a heavily and inherently fact-bound inquiry that the court may not reach at this stage in the litigation.[67] Google also concedes that its disclosure of user data causes the phones to send at least "a few bytes of name, email address, and zip code information."[68] Moreover, the court has already ruled that allegations of resource depletion, including battery power, gives rise to standing,[69] and the App Disclosure subclass has alleged resource depletion stemming from Google's breach of contract and the UCL.[70] Whatever their ultimate merits, the subclass plainly has standing to raise those claims.

B. Sufficiency of the Pleadings

With the standing question resolved, the court next turns to the legal sufficiency of the claims alleged. At the outset, it is worth noting that this court's prior order found that Google is immune from the claims alleged under the Wiretap Act because of its status as a provider of electronic communication services,[71] and Plaintiffs have not amended or altered their claim to avoid that immunity in this iteration. Similarly, the court's prior order determined that Google is

---

[66] *See* Docket No. 78 at 5.

[67] *See Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011) (quoting *Warth v. Seldin*, 422 U.S. 490, 501 (1975)) ("For purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing court must accept as true all material allegations of the complaint and must construe the complaint in favor of the complaining party.").

[68] Docket No. 78 at 5.

[69] *See* Docket No. 67 at 12-13.

[70] *See* Docket No. 71 at 70- 74.

[71] *See* Docket No. 67 at 18.

not subject to liability under the Stored Communications Act based on the conduct alleged,[72] and again, Plaintiffs have not amended their claim to suggest a different result. The breach of contract claim on behalf of the entire class falls for the same reason.[73] While Plaintiffs have successfully preserved these issues for appellate review, they are once again dismissed for failure to state a claim in the current proceeding.

1. CLRA Claim on Behalf of Device Switch Subclass

Plaintiffs' first cause of action seeks recovery under Sections (a)(5),(7), (9), (14) and (16) of the CLRA on behalf of the Device Switch Subclass. It is based on the theory that Google drafted its 2008 Android Policy with the intent of deceiving potential purchasers of Android devices into buying them based on the promise that Google would not associated device-related information (such as the device's IMEI) with a user's account, that Google had a secret plan to change that policy, and that "[h]ad Google disclosed in June 2010 that it did not intend to honor the terms of the 'Android-powered device privacy policy' at that time, Plaintiff Nisenbaum would not have purchased his Android device."[74] The CLRA proscribes representations that goods or services have characteristics that they do not have, representations that goods or services are of a particular standard when they are not, advertisement of goods with the intent not to sell them in the manner advertised, representations that a transaction conveys rights that it does not, and representations that the subject of a transaction has been conveyed in accordance with terms of a previous transaction, when it has not. In order to recover, Plaintiffs also must allege facts to

[72] *See id.* at 23.

[73] *See id.* at 25.

[74] *See* Docket No. 68 at ¶ 66.

establish that they relied on the misrepresentations in question, and that in so relying, they suffered damage.[75] These allegations are subject to Rule 9(b)'s heightened pleading standards.[76]

Google first argues that Plaintiffs' CLRA claim should fail because software is neither a good nor a service as required for liability under Cal. Civ. Code § 1770. However, Plaintiffs' allegations are not premised on the sale of the apps, but the sale of the Android device itself.[77] Plaintiffs allege that the same hardware that was the subject of the relevant sale was also subject to the privacy policy at issue.[78] The Android-powered device is the "tangible chattel" that makes Google the proper target of a CLRA claim.[79] Additionally, under the CLRA, the stream of commerce does not vitiate liability for alleged affirmative misrepresentations made by manufacturers that do not sell directly to customers.[80] Plaintiff's CLRA claim is not based upon an

---

[75] *See Marolda v. Symantec Corp.*, 672 F. Supp. 2d 992, 1003 (N.D. Cal. 2009).

[76] *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009) (citing *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1102 (9th Cir. 2003)).

[77] *Cf. In re iPhone Application Litig.* Case No. 5:11-md-02250-LHK, 2011 WL 4403963, at *10 (N.D. Cal. Sept. 20, 2011) ("Thus, to the extent Plaintiffs' allegations are based solely on software, Plaintiffs do not have a claim under the CLRA.").

[78] *See* Docket No. 68 at ¶ 255.

> The Android-powered device policy provided that Google "would not associate the following discrete categories of Android user information with that user's Google profile or account: (i) the hardware model of a user's Android-powered phone or device; (ii) the version of Android software used by a user; (iii) information about crashes or other phone-level events experienced by an Android-user; (iv) information generated by the use of third-party applications or features, such as mobile browsers, social networking software, address books, and reference applications, used by an Android user; and (v) an Android user's location information, including Cell ID and GPS information."

[79] *See Perrine v. Sega of America, Inc.*, Case No. 3:13-cv-01962-JSW, 2013 WL 6328489, at *3 (N.D. Cal Oct. 3, 2013) ("The CLRA defines 'goods to mean 'tangible chattels bought or leased for use primarily for personal, family, or household purposes'") (quoting Cal. Civ. Code § 1761(a)).

[80] *See Oestreicher v. Alienware Corp.*, 322 Fed. Appx. 489, 493 (9th Cir. 2009) (Unpub. Disp.) ("A manufacturer's duty to consumers is limited to its warranty obhligations absent either an affirmative misrepresentation or a safety issue.") (citation omitted); *Tietsworth v. Sears*, 720 F. Supp. 2d 1123, 1138 (N.D. Cal. 2010) (holding that, despite the lack of an alleged agreement or transaction between plaintiff and defendant manufacturer, "when a plaintiff can

omission, rather, Plaintiffs allege that through its privacy policy, Google "intentionally misrepresented the ability of Nisenbaum and other members of the Android Device Switch Subclass to prevent the association and commingling of their personal information."[81] Therefore, Plaintiffs need not allege a direct sale between Google and themselves to establish their CLRA claim.[82]

In its prior order, the court dismissed all of Plaintiffs' theories of recovery under the CLRA because Plaintiffs did not allege that Google intended to use their information in a manner other than was advertised at the time that Plaintiffs purchased devices and registered for accounts.[83] That omission has been remedied in the current version of the complaint.[84] However, the CSAC suffers from another, equally fatal omission: it never alleges that Nisenbaum or any other member of the subclass read, heard, saw or were in any way aware of Google's operative privacy policy.[85] If Nisenbaum and the other members of his subclass did not see, read, hear or consider the terms of Google's then-active privacy policy before creating their account, they could not have relied on any representation it contained in making their decisions to purchase Android phones, and without affirmatively alleging reliance on Google's misrepresentations, the CLRA claim cannot survive.

---

demonstrate that the manufacturer had exclusive knowledge of a defect and the consumer relied upon that defect, the CLRA's protection extends to the manufacturer as well, regardless of whether the consumer dealt directly with the manufacturer.") (citing *Chamberlan v. Ford*, 369 F. Supp. 2d 1138, 1144 (N.D. Cal. 2005)); *see also McAdams v. Monier, Inc.* 182 Cal. App. 4th 174, 184 (2010) ("We also pause here to note that a cause of action under the CLRA may be established independent of any contractual relationship between the parties.") (citation omitted).

[81] Docket No. 68 at ¶ 260.

[82] *See Oestreicher*, 322 Fed. Appx. at 493.

[83] *See* Docket No. 67 at 29.

[84] *See* Docket No. 68 at ¶ 257 ("Google's assurances in its Android-powered device privacy policy . . . were false when made because Google already decided, no later than May 2010, not to honor these terms.").

[85] *See* Docket No. 71 at 9.

Plaintiffs try to dodge this flaw in their claim with three arguments. First, they argue that "CLRA jurisprudence is abundantly clear that the reliance element is satisfied with allegations that 'the plaintiff 'in all reasonable probability' would not have engaged in the injury-producing conduct' absent the misrepresentation or omission."[86] This argument is problematic for several reasons, but the most glaring is that every case Plaintiffs cite in its support concerns the UCL, not the CLRA.[87] Furthermore, in two of those three cases, the plaintiff had clearly alleged that he or she was exposed to the misrepresentation,[88] and the parties were simply fighting about whether the complaint spelled out that the plaintiff had relied on it in deciding to pursue the injury-inducing conduct.[89] This complaint lacks the predicate allegation (exposure), which precludes the court from considering reliance. Second, Plaintiffs argue that reliance may be presumed from a material omission.[90] That is certainly true in a case based on a theory of non-disclosure, but here, Plaintiffs theory is that they made their purchasing decision based on affirmative, fraudulent

---

[86] *See* Docket No. 74 at 18.

[87] *See In re Tobacco II Cases*, 46 Cal. 4th 298, 324-25 (2009) ("The second question before us is the meaning of the phrase 'as a result of' in section 17204's requirement that a private enforcement action under the UCL can only be brought by "'a person who has suffered injury in fact and has lost money or property as a result of the unfair competition.'"); *Lanovaz v. Twinings N. Am., Inc.* Case No. 5:12-cv-02646-RMW, 2014 WL 46822, at *3 (N.D. Cal. Jan. 6, 2014) ("Lanovaz's claims under all three prongs of the UCL are based on fraud or misrepresentation. [] Therefore, Lanovaz must prove reliance to be successful on those claims."); *In re Google AdWords Litig.*, Case No. 5:08-cv-03369-EJD, Docket No. 166 (only UCL and FAL claims present in the Third Amended Complaint).

[88] *See In re Tobacco II*, 46 Cal. 4th at 324 ("[W]here, as here, a plaintiff alleges exposure to a long-term advertising campaign . . ."); *Lanovaz v. Twinings N. Am., Inc.* Case No. 5:12-cv-02646-RMW, Docket No. 67 at ¶ 14 ("Plaintiff reviewed the website at various times during the Class Period and read the health claims and antioxidant related nutrient content claims appearing on Defendant's website as specified above prior to purchasing said products and relied on this information in making her decisions to purchase Defendant's tea products.");

[89] There was no allegation of misrepresentation in the *In re Google AdWords* case; the case was based entirely on Google's omission of a material fact. *See* Docket No. 166.

[90] *See* Docket No. 74 at 18.

representations.[91] Third, Plaintiffs argues that the court can and should reasonably infer that "Nisenbaum was exposed to the 2008 Android Policy or 2009 Mobile Policy terms during the registration process" for his Android account.[92] However, that exposure would not have occurred until "after [Nisenbaum purchased] his Android device,"[93] at which point, it would not be reasonable to infer that Nisenbaum relied on the policy in deciding to purchase the device.

In short, although it was properly directed at Google, the Device Switch Subclass' CLRA claim must be dismissed once again based on deficient pleadings.[94]

2. UCL Claim on Behalf of Device Switch Subclass

California's UCL provides a private cause of action for users who are harmed by unfair, unlawful, or fraudulent business practices.[95] Plaintiffs plead their UCL claim under all three prongs. To sustain a claim under the unlawful prong, Plaintiffs must allege facts that, if proven, would demonstrate that Defendant's conduct violated another, underlying law.[96] If the unlawful conduct is part of a uniform course of fraudulent conduct, it must meet Rule 9(b)'s heightened

[91] *Cf. Collins v. eMachines, Inc.*, 202 Cal. App. 4th 249, 256 (2011) (addressing allegations of active concealment of a material defect in a product).

[92] Docket No. 74 at 19. With respect to the 2009 Mobile Policy, it is mentioned nowhere in the CSAC and thus is irrelevant.

[93] *See id.*

[94] Google also argues that the CLRA claim is also deficient under Fed. R. Civ. P. Rule 9(b), providing yet another ground for dismissal. *See* Docket No. 71 at 9. However, most of the particular deficiencies raised (where Nisenbaum's phone was purchased, from whom it was purchased, etc.) would do little to provide Google with the necessary notice to defend itself on these claims. In addition, under Nisenbaum's theory, he would not have purchased his phone if he had known that Google simply had the authority to associate device numbers with Google accounts, regardless of whether or not it ever actually did so.

[95] *See Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007).

[96] *See Trazo v. Nestle USA, Inc.*, Case No. 5:12-cv-2272-PSG, 2013 WL 4083218, at *9 (N.D. Cal. Aug. 9, 2013).

pleading standards.[97] Under the fraudulent prong, Plaintiffs must allege specific facts to show that the members of the public are likely to be deceived by the actions of the defendant.[98] The Ninth Circuit has established that this prong always is subject to Fed. Rule Civ. P. 9(b)'s heightened pleading requirements.[99] With respect to Plaintiffs' claim under the UCL's unfair prong, "[t]he standard for determining what business acts or practices are 'unfair' in user actions under the UCL is currently unsettled."[100] Generally speaking, "[a]n unfair business practice under the UCL is "one that either offends an established public policy or is immoral, unethical, oppressive, unscrupulous, or substantially injurious to users."[101] To determine whether a business practice is unfair, a court should consider "the impact of the practice or act on its victim, balanced against the reasons, justifications and motives of the alleged wrongdoer;" this prong of the UCL should be used to "enjoin deceptive or sharp practices."[102]

---

[97] *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009); *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003).

[98] *See Finuliar v. BAC Home Loans Servicing, L.P.*, Case No. 3:11-cv-02629-JCS, 2011 WL 4405659, at *9 (N.D. Cal. Sept. 21, 2011) ("'Fraudulent,' as used in the statute, does not refer to the common law tort of fraud but only requires a showing members of the public 'are likely to be deceived.'").

[99] *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009).

[100] *Yanting Zhang v. Superior Court*, 57 Cal. 4th 364, 380 n.9 (2013). One test holds that "an 'unfair' business practice occurs when it offends an established public policy or when the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to users." *People v. Casa Blanca Convalescent Homes, Inc.*, 159 Cal. App. 3d 509, 530 (1984). Another test requires that a plaintiff prove "that the defendant's "conduct is tethered to an . . . underlying constitutional, statutory or regulatory provision, or that it threatens an incipient violation of an antitrust law, or violates the policy or spirit of an antitrust law." *Byars v. SCME Mortgage Bankers, Inc.*, 109 Cal. App. 4th 1134, 1147 (2003). A third test requires that "(1) the user injury must be substantial; (2) the injury must not be outweighed by any countervailing benefits to users or competition; and (3) it must be an injury that users themselves could not reasonably have avoided." *Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 257 (2010).

[101] *McDonald v. Coldwell Banker*, 543 F.3d 498, 506 (9th Cir. 2008).

[102] *Wilson v. Hynek*, 207 Cal. App. 4th 999, 1008 (2012).

Plaintiffs' claim under the unlawful prong of the UCL is based entirely on their CLRA claim.[103] As the CLRA claim fails, so does the derivative UCL claim. Plaintiffs' claim under the fraudulent prong of the UCL also fails for the same reason that the CLRA claim failed: the complaint does not allege reliance.[104]

Plaintiffs' claim under the unfair prong of the UCL fails as well, but for a different reason. Their unfairness theory is best understood in a three-step syllogism: (1) Plaintiffs have a right to privacy under the California Constitution; (2) Google's conduct "resulted in a violation of" that right to privacy, therefore (3) Google's conduct ran afoul of the UCL.[105] Contrary to Google's suggestion that the harms alleged in this claim are the same as they were in the previous iterations, this framework offers a new and different theory of recovery.[106] Unfortunately for Plaintiffs, it is no more successful. A necessary piece of the theory is that Google's conduct violated Plaintiffs' right to privacy under the California Constitution, yet they have not alleged facts to support that assertion. To prove a claim under the California Constitutional right to privacy, a plaintiff must plead three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious, egregious invasion of the protected privacy interest.[107] Even if Plaintiffs have sufficiently alleged the first two elements, they have not met the third. Courts in this district have consistently refused

[103] *See* Docket No. 68 at ¶ 268.

[104] *See In re Tobacco II Cases*, 46 Cal. 4th 298, 328 (2009) (holding that plaintiff must allege reliance on defendant's misrepresentation in order to seek recovery under the fraudulent prong of the UCL).

[105] *See id.* at ¶ 269-70.

[106] *Compare* Docket No. 50 at ¶¶ 270-72, 314 (claiming violation of the unfair prong of the UCL based on luring Plaintiffs into becoming accustomed to "indispensable" services with promises of privacy protection then making it incredibly difficult to "opt out" of undesirable policies in the future), *with* Docket No. 68 at ¶ 268.

[107] *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35-37 (1994).

to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms.[108] The conduct at issue in this case is neither sufficiently different from prior cases nor sufficiently beyond the pale of social norms to justify such a characterization here.

As the theories of harm fail under all three prongs of the UCL, the Device Switch Subclass' claim under the UCL is dismissed.

3. Breach of Contract Claim on Behalf of App Disclosure Subclass

Plaintiffs' third through fifth causes of action are brought on behalf of the App Disclosure subclass. The first is the breach of contract claim, which underlies this subclass' other claims.

"Under California law, the elements of a breach of contract claim are: (1) the existence of a contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) resulting damage to plaintiff."[109] The court's prior order dismissed Plaintiffs' breach of contract claim because an express provision in the contract at issue allowed data commingling.[110] The complaint now adequately states a claim for breach of contract solely on behalf of the Android App Disclosure Subclass.[111] The complaint alleges: (1) that the subclass "entered into a contract with Google by registering for an Android Market/Google Play account, the key terms of which

---

[108] *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (declining to find that defendant violated constitutional right to privacy in releasing unique device identifier number, personal data, and geolocation information from cell phones to third parties); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (declining to find that defendant violated constitutional right to privacy in releasing digital identification information to third parties).

[109] *EPIS, Inc. v. Fid. & Guar. Life Ins. Co.*, 156 F. Supp. 2d 1116, 1124 (N.D. Cal.2001) (modifying punctuation) (citing *Reichert v. General Ins. Co.*, 68 Cal. 2d 822, 830 (1968)).

[110] *See* Docket No. 67 at 25.

[111] *See* Docket No. 68 at ¶¶ 273-280. Plaintiff includes a breach of contract claim on behalf of the entire class only for purposes of appellate preservation. *Id.* at 75 n.1.

were provided in the relevant terms of service and privacy policies,"[112] (2) the specific terms at issue;[113] (3) that Google breached those terms by disclosing user data to third parties following every download or purchase of an app[114] and (4) resulting damages in the form of resource consumption.[115]

Google argues that the complaint fails to state a breach of contract claim for three reasons.[116] First, it argues that the claim fails because the complaint fails to identify when the class members made their App purchases via Google Play, making it impossible to determine what privacy policy governed those transactions. [117] This argument misstates the complaint and is thus unpersuasive. The complaint alleges that Google used an ever-changing array of privacy policies that varied by device, platform and service, including "the Google Wallet privacy policy, the Google Play terms of service, the Android-powered device privacy policy, and the general or default Google privacy policy," that one of these policies was in place at the time of each transaction [118] and what provisions of the policies were allegedly violated.[119] Although these allegations may not be sufficient to sustain a fraud claim subject to Rule 9(b), this is a simple breach of contract claim subject to Rule 8. Under these laxer standards, the allegations will suffice.

---

[112] Docket No. 68 at ¶ 278.

[113] *See id.* at ¶¶ 130 (quoting Android-powered device policy), 131 ("The Google Play terms of service simply refer to the Google Wallet privacy policy"), 132-34 (discussing and quoting Google Wallet Privacy Policy), 135 (discussing and quoting Google's general privacy policy).

[114] *See id.* at ¶ 278.

[115] *See id.* at ¶ 279.

[116] *See* Docket No. 71 at 15-16.

[117] *Id.* at 15.

[118] Docket No. 68 at ¶ 277.

[119] *See id.* at ¶¶ 130-35.

Google's second and third arguments also are unpersuasive. The second—that Plaintiffs are not parties to the general privacy policy on which they base their claims[120]—fails for the same reason that it did when posed against Nisenbaum's standing: Google's 2009 policy is not properly before the court. The third—that Plaintiffs fail to point to any explicit terms in the contracts they allegedly breached[121] — is simply false. Paragraph 130 points to a term in the Android device policy that assures consumers that although Google "may share non-personal, aggregated information with certain third parties . . . such information will not identify you personally."[122] Paragraph 132 spells out that "[t]he November 16, 2011 Google Wallet Privacy Policy states that Google may share personal information outside Google only in certain defined circumstances. For example, that policy states that Google may share personal information with third parties '[a]s necessary to process your transaction and maintain your account. As with any credit card payment, if you process a credit card transaction through the Processing Service, we need to share some information (for example, your name and credit card number) with the banks and other entities in the financial system that process credit card transactions.'"[123] However, that same provision allegedly assures consumers that when additional information, such as a telephone number, is required, "you will be notified before you complete your transaction."[124] Finally, the complaint alleges that Google's general privacy policy specifically provides that it "restrict[s] access to personal information to Google employees, contractors and agents who need to know that information in order to process it on our behalf. These individuals are bound by confidentiality

[120] Docket No.71 at 15.

[121] *See* Docket No. 71 at 15.

[122] Docket No. 68 at ¶ 130.

[123] *Id* at ¶ 132.

[124] *Id.*

obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations."[125]

4. Intrusion Upon Seclusion Claim on Behalf of App Disclosure Subclass

As the court previously admonished Plaintiffs, to assert an intrusion upon seclusion claim, a plaintiff must plead facts in support of two elements: "1) intrusion into a private place, conversation or matter, and 2) in a manner highly offensive to a reasonable person. . . . To show intrusion, a plaintiff must have 'an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source,' and the defendant must have 'penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff.'"[126] In this context, "the concept of 'seclusion' is relative. The mere fact that a person [or their information] can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."[127] Courts have recognized facts sufficient to support these elements in the context of repeated phone calls,[128] eavesdropping on workplace conversations,[129] and unauthorized email review.[130]

Google argues that the court should simply stick with its prior holding that commingling of user data is an inadequate allegation for an intrusion claim.[131] But to so rule would fail to

---

[125] *Id.* at ¶ 135.

[126] *Thompson v. Chase Bank N.A.*, Case No. 4:09-cv-2153-DMS, 2010 WL 1329061, at *4 (S.D. Cal. Mar. 30, 2010) (citing *Shulman v. Group W Productions*, 18 Cal.4th 200, 232 (1998)).

[127] *Joseph v. J.J. Mac Intyre Companies, L.L.C.*, 281 F. Supp. 2d 1156, 1165 (N.D. Cal. 2003).

[128] *See Panahiasl v. Gurney*, Case No. 5:04-cv-04479-JF, 2007 WL 738642, at *3 (N.D. Cal. Mar. 8, 2007).

[129] *See Sanders v. Am. Broad. Companies, Inc.*, 20 Cal. 4th 907, 916 (1999).

[130] *See Yee v. Lin*, Case No. 5:12-cv-02474-WHA, 2012 WL 4343778, at*4 (N.D. Cal. Sept. 20, 2012).

[131] *See* Docket No. 71 at 16 (citing Docket No. 67 at 29).

recognize Plaintiffs' new theory: that the intrusion at issue is disclosure to third-party developers contrary to Google's own policies.[132] The court nonetheless cannot find that Plaintiffs have stated a claim under their revised theory either. This district "set[s] a high bar" for the requisite "intrusion [that is] highly offensive to a reasonable person."[133] Just as *In re iPhone Application Litig.*'s analogous facts were informative on the issue of standing, they also teach here that Plaintiffs' allegations do not plausibly rise to the level of intrusion necessary to establish an intrusion claim.[134] Plaintiffs' intrusion claims are therefore dismissed.

5. UCL Claim on Behalf of App Disclosure Subclass

Plaintiffs' fifth cause of action is another UCL claim, this time on behalf of the App Disclosure subclass. The App Disclosure subclass seeks recovery under two of the three prongs of the UCL, one of which is easily disposed of by this court's prior order. Their theory under the unfair prong of the UCL is that members of the App Disclosure subclass were lured into believing that their personal information would be closely guarded while Google encouraged them to "make Android devices and applications indispensable to their lives;" they were therefore trapped when Google implemented policies "from which they cannot effectively opt out."[135] In its last order, the court found that the "benefit to users in receiving free, 'indispensable services' offsets much of the harm they may suffer" as a result of being subjected to the changed policies. Plaintiff presents no

[132] *See* Docket No. 68 at ¶¶ 281-88 (alleging intrusion on behalf of App Disclosure subclass), 303-09 (alleging intrusion on behalf of entire class).

[133] *Belluomini v. Citigroup Inc*, Case No. 3:13-cv-01743, 2013 WL 5645168, at *3 (N.D. Cal. Oct. 16, 2013); *see also Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008) (dismissing invasion of privacy claim where Plaintiff's stolen laptop contained personal information including social security number).

[134] *See* 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (dismissing invasion of privacy claim where "information allegedly disclosed to third parties included the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices").

[135] *See* Docket No. 68 at ¶ 299.

persuasive reason to alter that holding here. As such the unfair prong of the App Disclosure subclass' UCL claim fails.

The App Disclosure subclass' claim under the fraudulent prong of the UCL, however, carries weight. As described above, under the fraudulent prong of the UCL, Plaintiffs must plead specific facts to show that the members of the public are likely to be deceived by the actions of the defendant and that Plaintiffs both relied on and were harmed by those actions.[136] Here, they allege that Google left a privacy policy in place which led consumers to believe that access to their data would be limited to certain groups,[137] even though it knew that it planned to distribute the data outside of those groups.[138] These allegations fill ten pages with extensive detail about the plan and its concealment, such that they clear the bar of Rule 9(b). Plaintiffs also successfully plead that they relied on these policies in making the decision to use Google Play and download Android applications.[139] Finally, Plaintiffs plead that they have suffered the loss of battery power and other system resources as a result of Google's fraudulent and surreptitious conduct. Once again, whatever the ultimate merits of this claim, the App Disclosure Subclass has stated a claim for relief that may go forward.

IV. CONCLUSION

After running each claim (and subclaim) of each class (and subclass) through the gauntlet of constitutional and procedural hurdles, two claims remain: the App Disclosure Subclass' breach of contract claim, and the fraudulent prong of the App Disclosure Subclass' UCL claim. Plaintiffs

[136] *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009); s*ee also Finuliar v. BAC Home Loans Servicing, L.P.*, Case No. 3:11-cv-02629-JCS, 2011 WL 4405659, at *10 (N.D. Cal. Sept. 21, 2011) ("'Fraudulent,' as used in the statute, does not refer to the common law tort of fraud but only requires a showing members of the public 'are likely to be deceived.'").

[137] *See* Docket No. 68 at ¶¶ 128-44, 295.

[138] *See id*. at ¶110-27.

[139] *See id.* at ¶ 296.

may proceed on these two causes of action alone. Because the court warned Plaintiffs in its last order that any future dismissal would likely be with prejudice,[140] and because the thorough nature of the allegations presented persuades the court that any and all omissions were intentional, all other causes of action dismissed in this order are dismissed with prejudice and without leave to amend. It is time for this case to move forward.

IT IS SO ORDERED.

Dated: July 21, 2014

PAUL S. GREWAL
United States Magistrate Judge

[140] *See* Docket No. 67 at 30.