

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  
SAN JOSE DIVISION**

ALICE SVENSON, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE INC., a Delaware Corporation,  
and GOOGLE PAYMENT  
CORPORATION, a Delaware Corporation,

Defendants.

Case No. 13-cv-04080-BLF

**ORDER DENYING MOTION TO  
DISMISS FOR LACK OF ARTICLE III  
STANDING; AND GRANTING  
MOTION TO DISMISS FOR FAILURE  
TO STATE A CLAIM WITH LEAVE TO  
AMEND IN PART**

[Re: ECF 20]

In this putative class action, Plaintiff Alice Svenson alleges that Defendants Google Inc. and Google Payment Corporation make unauthorized disclosures of user information to third-party developers of mobile applications (“Apps”) when users purchase Apps in the Google Play store using Google Wallet. Defendants move to dismiss under Federal Rule of Civil Procedure 12(b)(1) for lack of Article III standing and under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. The Court has considered the briefing and the oral argument presented at the hearing on June 26, 2014. For the reasons discussed below, the motion to dismiss for lack of Article III standing is DENIED and the motion to dismiss for failure to state a claim is GRANTED with leave to amend in part.

**I. BACKGROUND**

Plaintiff alleges that “Google provides internet search functionality, email services, virtual filing cabinet ‘cloud’ storage services, multimedia electronic distribution platforms, social media services, advertising services, and payment processing services, among many others.” (Corrected Complaint (“Compl.”) ¶ 10, ECF 5-1) Google Wallet is “Google’s electronic and mobile payment

1 processing service.” (*Id.* ¶ 17) Google Wallet allows users to store debit card and credit card  
2 information and to utilize those payment methods to purchase Apps and other products. (*Id.* ¶¶  
3 17-18) Apps may be purchased in the Google Play store, “Google’s digital multimedia content  
4 distribution platform that is accessible via mobile devices and other internet-capable computing  
5 equipment.” (*Id.* ¶¶ 26, 28)

6 When a user purchases an App in the Google Play store using Google Wallet, “Defendants  
7 process the payment.” (Compl. ¶ 49) “After Defendants process the user’s payment, Defendants  
8 automatically remit funds to the third-party vendor in addition to the user’s name, email address,  
9 Google account name, home city and state, zip code, and in some instances telephone number”  
10 (hereinafter, “Contact Information”).<sup>1</sup> (*Id.*) Google transmits the App to the user electronically  
11 via the Google Play store. (*Id.* ¶ 47)

12 The Contact Information is collected by Defendants when users register for a Google  
13 account, Gmail, the Google Play store, or Google Wallet. (Compl. ¶ 55) Plaintiff asserts that  
14 disclosure of Contact Information to third-party vendors is unnecessary and unauthorized by the  
15 user (*id.* ¶¶ 50-51, 54); breaches the terms of the agreements between the users and Defendants  
16 (*id.* ¶¶ 65-66); diminishes the economic value of the Contact Information (*id.* ¶¶ 83-84); and  
17 exposes the user to a greater risk of identity theft (*id.* ¶ 89).

18 Plaintiff alleges that on May 6, 2013, she bought an App in the Google Play store using  
19 Google Wallet. (Compl. ¶ 74). Specifically, Plaintiff paid \$1.77 for the “SMS MMS to Email”  
20 App published by third-party vendor YCDroid; upon purchase, the App was instantly downloaded  
21 for use on Plaintiff’s mobile device. (*Id.*) Following the purchase, Defendants “transmitted and/or  
22 made available” Plaintiff’s Contact Information to YCDroid. (*Id.* ¶ 77) Based upon this  
23 transaction, Plaintiff asserts claims against Defendants for: (1) breach of contract; (2) breach of  
24 the implied covenant of good faith and fair dealing; (3) violation of the Stored Communications  
25

---

26 <sup>1</sup> Plaintiff’s complaint and briefs use the term “Sensitive Identifiable Data,” abbreviated to “SID”  
27 to describe this information, while Defendants’ briefs use the term “Contact Information.”  
28 Because the term “Contact Information” is less unwieldy than the term “Sensitive Identifiable  
Data” and accurately describes the information, the Court uses the term “Contact Information” in  
this order.

1 Act, 18 U.S.C. § 2701; (4) violation of the Stored Communications Act, 18 U.S.C. § 2702; and (5)  
2 violation of California’s Unfair Competition Law, Cal. Bus. & Prof. Code § 17200.

3 Defendants contend that Plaintiff has failed to allege facts demonstrating that she has  
4 Article III standing and thus has failed to establish subject matter jurisdiction. Alternatively,  
5 Defendants contend that Plaintiff has failed to allege facts sufficient to state a claim upon which  
6 relief may be granted.

7 **II. LEGAL STANDARDS**

8 **A. Rule 12(b)(1)**

9 A motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(1) raises a  
10 challenge to the Court’s subject matter jurisdiction. *See* Fed. R. Civ. P. 12(b)(1). “Article III . . .  
11 gives the federal courts jurisdiction over only cases and controversies.” *Public Lands for the*  
12 *People, Inc. v. United States Dep’t of Agric.*, 697 F.3d 1192, 1195 (9th Cir. 2012) (internal  
13 quotation marks and citation omitted). “The oft-cited *Lujan v. Defenders of Wildlife* case states  
14 the three requirements for Article III standing: (1) an injury in fact that (2) is fairly traceable to  
15 the challenged conduct and (3) has some likelihood of redressability.” *Id.* at 1195-96 (citing *Lujan*  
16 *v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). If these requirements are not satisfied, the  
17 action should be dismissed for lack of subject matter jurisdiction. *See Steel Co. v. Citizens for a*  
18 *Better Env’t*, 523 U.S. 83, 109-10 (1998).

19 **B. Rule 12(b)(6)**

20 “A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) for failure to state a  
21 claim upon which relief can be granted ‘tests the legal sufficiency of a claim.’” *Conservation*  
22 *Force v. Salazar*, 646 F.3d 1240, 1241-42 (9th Cir. 2011) (quoting *Navarro v. Block*, 250 F.3d  
23 729, 732 (9th Cir. 2001)). When determining whether a claim has been stated, the Court accepts  
24 as true all well-pled factual allegations and construes them in the light most favorable to the  
25 plaintiff. *Reese v. BP Exploration (Alaska) Inc.*, 643 F.3d 681, 690 (9th Cir. 2011). However, the  
26 Court need not “accept as true allegations that contradict matters properly subject to judicial  
27 notice” or “allegations that are merely conclusory, unwarranted deductions of fact, or  
28 unreasonable inferences.” *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008)

1 (internal quotation marks and citations omitted). While a complaint need not contain detailed  
2 factual allegations, it “must contain sufficient factual matter, accepted as true, to ‘state a claim to  
3 relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl.*  
4 *Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible when it “allows the  
5 court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.*

6 **III. DISCUSSION**

7 **A. Subject Matter Jurisdiction**

8 In their motion, Defendants argue that Plaintiff has not alleged facts sufficient to establish  
9 Article III standing and thus that the Court lacks subject matter jurisdiction. After Defendants  
10 filed the motion, the Ninth Circuit clarified that a plaintiff suing under the Stored Communications  
11 Act (“SCA”) has Article III standing. *See In re Zynga Privacy Litig.*, 750 F.3d 1098, 1105 n.5  
12 (9th Cir. 2014). In that case, Defendants Zynga and Facebook argued that the plaintiffs lacked  
13 standing to assert claims under the Wiretap Act and the SCA because they had “not suffered any  
14 concrete or particularized injury arising from the alleged disclosure of users’ Facebook IDs and  
15 URL information to third parties.” *Id.* The court rejected that argument, holding that “a plaintiff  
16 demonstrates an injury sufficient to satisfy Article III when bringing a claim under a statute that  
17 prohibits the defendant’s conduct and grants persons in the plaintiff’s position a right to judicial  
18 relief.” *Id.* (internal quotation marks and citation omitted). The Court held that because the  
19 plaintiffs alleged that Zynga and Facebook were violating the Wiretap Act and the SCA – statutes  
20 granting persons in the plaintiffs’ position the right to judicial relief – they had standing to  
21 proceed. *Id.* Defendants in the present case concede that *Zynga* resolves the Article III standing  
22 issue for purposes of this motion. (Defs.’ Supp. Br. at 1, ECF 74)

23 Accordingly, the motion to dismiss for lack of Article III standing is DENIED.

24 **B. Failure to State a Claim**

25 **1. Claim 1 – Breach of Contract**

26 Claim 1 alleges breach of contract. To succeed on a breach of contract claim under  
27 California law, a plaintiff must establish a contract, the plaintiff’s performance or excuse for  
28 nonperformance, the defendant’s breach, and resulting damages to the plaintiff. *Pyramid Tech.*,

1 *Inc. v. Hartford Cas. Ins. Co.*, 752 F.3d 807, 818 (9th Cir. 2014).

2 **a. Relevant Contracts**

3 Plaintiff alleges the existence of a number of agreements that governed her App purchase:  
4 the Google Terms of Service (“GToS”) (Compl. ¶ 20); the Google Privacy Policy (“GPP”) (*id.*);  
5 the Google Wallet Terms of Service (“GWToS”) (*id.* ¶ 21); the Google Wallet Privacy Policy  
6 (“GWPP”) (*id.*); and the Google Play Terms of Service (“GPToS”) (*id.* ¶ 27). Plaintiff does not  
7 attach any of these agreements to her complaint.

8 As is discussed below, Plaintiff’s failure to attach the agreements as exhibits to the  
9 complaint, and her decision instead to include hyperlinks in the text of the complaint (some of  
10 which were inaccurate), needlessly multiplied and confused the proceedings. While Plaintiff is  
11 not required to do so, the Court strongly urges Plaintiff to attach the relevant contracts to any  
12 amended complaints she may file in this case.

13 Defendants request judicial notice of the GWToS and the GWPP. (Defs.’ RJN, ECF 21)  
14 Plaintiff objects to Defendants’ request, arguing that Defendants have submitted the September  
15 10, 2013 GWToS when Plaintiffs’ claims are governed by the October 23, 2012 GWToS.  
16 Plaintiff submits the October 23, 2012 GWToS in connection with her own request for judicial  
17 notice. (Pl.’s RJN, ECF 31, 36) Defendants do not object to the Court’s consideration of the  
18 October 23, 2012 GWToS, as Defendants state that there is no material difference between the two  
19 versions of the GWToS; Defendants explain that they submitted the later GWToS only because  
20 the complaint referenced a link to that version. (Defs’ Resp. to Pl.’s Objs., ECF 52) Defendants  
21 likewise do not object to Plaintiff’s request for judicial notice of Proposition 64, the relevant  
22 GPToS, and the relevant GToS. Judicial notice is appropriate with respect to Proposition 64. *See*  
23 *Kamen v. Kemper Fin. Svcs., Inc.*, 500 U.S. 90, 99 (1991) (courts may take judicial notice of the  
24 law of any state). The GWPP submitted by Defendants and the GPToS, GWToS, and GToS  
25 submitted by Plaintiff may be considered under the incorporation by reference doctrine. *See*  
26 *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005) (the incorporation by reference doctrine  
27 permits a court to consider documents referenced in but not physically attached to the complaint).  
28

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

**b. Allegations of Breach**

Plaintiff claims that “the GWPP and GPP, as incorporated into the GWToS, constitute a valid and enforceable contract between Plaintiff and the Class and Defendants.” (Compl. ¶ 102). Plaintiff alleges generally that under this contract, “Plaintiff and the Class agreed to register with the Google Play store and Google Wallet to allow Defendants to process their purchase and payment transactions in connection with provision and sale of Apps.” (*Id.* ¶ 100) According to Plaintiff, “[t]hese transactions thereby allow Google Payment Corp to earn a fee for processing the payment.” (*Id.*) In exchange, Defendants acted as “a middle-man” in the App transactions, and they agreed to share users’ Contact Information with third parties only in specific, limited circumstances. (*Id.* ¶¶ 103-06) Plaintiff alleges that she “and the Class did all or substantially all of the significant things required of them by the Relevant Terms.” (*Id.* ¶ 107) She alleges that Defendants breached the contract by sharing her Contact Information under circumstances not contemplated by the agreements. (*Id.* ¶¶ 103-06) Finally, she alleges that “Plaintiff and the Class are damaged and are alternatively entitled to restitution for Defendant’s unjust enrichment due to Defendants’ aforesaid breaches.” (*Id.* ¶ 108)

These allegations are insufficient to state a claim for breach of contract. Initially, Plaintiffs’ identification of the “contract” is inadequate. While Plaintiff alleges that the “contract” is a combination of the GWPP, GPP, and GWToS (Compl. ¶ 102), Plaintiff has admittedly identified the wrong contracts in her complaint.

More significantly, Plaintiff’s conclusory allegation that she and the Class “are damaged” is insufficient to plead this element of her contract claim. *See Iqbal*, 556 U.S. at 678 (“Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.”). Additionally, Plaintiff’s alternative allegation that she and the Class are entitled to restitution as a result of Defendants’ breach of contract is simply incorrect as a matter of law. Generally, if two parties have a valid and enforceable written contract, the plaintiff may not proceed on a claim in quasi-contract, *i.e.*, a claim of restitution or unjust enrichment. *See Klein v. Chevron U.S.C., Inc.*, 202 Cal. App. 4th 1342, 1388 (2012). “[A] plaintiff may not plead the existence of an enforceable contract and maintain a quasi-contract claim at the same time, unless

1 the plaintiff has pled facts suggesting that the contract may be unenforceable or invalid.” *Schulz v.*  
2 *Cisco Webex, LLC*, No. 13-cv-04987-BLF, 2014 WL 2115168, at \*5 (N.D. Cal. May 20, 2014).

3 Plaintiff’s allegations of breach of contract and resulting damages are set forth in  
4 paragraphs 74-89 and 98-108 of the complaint. In essence, Plaintiff alleges that upon purchase of  
5 the App, Google disclosed her Contact Information to the third-party App vendor but that  
6 disclosure was not “necessary” for the transaction with the third-party vendor and thus violated the  
7 privacy provisions of the various contracts at issue. (Compl. ¶ 106) Plaintiff alleges three theories  
8 of contract damages: benefit of the bargain, diminution in the economic and proprietary value of  
9 her Contact Information, and increased risk of identity theft.

10 With respect to her benefit of the bargain theory of damages, Plaintiff alleges that the  
11 \$1.77 she paid for the App included “built-in monies and transaction fees pocketed by Defendant  
12 Google Payment Corp.”; that those monies compensated Google for the “service” of facilitating  
13 the App purchase *without* disclosing Plaintiff’s Contact Information; and that Plaintiff was denied  
14 the benefit of her bargain when Defendants “pocketed monies” from the App purchase but  
15 nonetheless transmitted Plaintiff’s Contact Information to the third-party vendor when there was  
16 no necessity to do so. (Compl. ¶¶ 79-81)

17 Those allegations are insufficient because they do not show that Plaintiff paid anything for  
18 the asserted privacy protections. Plaintiff entered into the Google, Google Wallet and Google Play  
19 agreements separately from her actual purchase of the App. (Compl. ¶¶ 68-70, 74) She does not  
20 allege that she made any payment for those services. In fact, a review of the contracts makes it  
21 clear that those were all free services. (*See e.g.*, Pl.’s RJN Ex. 3 (GWToS) (“GPC does not charge  
22 a fee to use the Processing Service as a Buyer.”) Plaintiff does not allege facts showing that she  
23 entered into a new or different agreement upon purchase of the App that could have given rise to  
24 new or additional privacy protections. It appears clear from the face of the complaint that the only  
25 payment made was the \$1.77 to the third- party vendor for the App, and Plaintiff does not allege  
26 that any portion of that \$1.77 was retained by Defendants rather than being transmitted in full to  
27 the vendor. Finally, even if Plaintiff’s benefit of the bargain theory were not defective for the  
28 foregoing reasons, Plaintiff does not allege that what she received – the App and unauthorized

1 disclosure of her Contact Information – was worth less than what she allegedly bargained for – the  
2 App and non-disclosure of her Contact Information.

3 As to her second damages theory, Plaintiff alleges that the disclosure of her Contact  
4 Information to the third-party vendor diminished the economic and proprietary value of the  
5 Contact Information to her. (Compl. ¶ 82) A recent unpublished decision of the Ninth Circuit  
6 Court of Appeals suggests that this type of allegation may be sufficient to establish the element of  
7 damages for a breach of contract claim. *See In re Facebook Privacy Litigation*, --- Fed.Appx. ----,  
8 No. 12–15619, 2014 WL 1815489, at \*1 (9th Cir. May 8, 2014). At the hearing, Defendants’  
9 counsel asserted that the plaintiffs in that case had alleged a market for the information in  
10 question. That fact is not apparent from the decision, although as a matter of common sense a  
11 theory of diminished economic value would depend on the existence of a market for the  
12 information. Plaintiff has not alleged a market for her Contact Information.

13 Finally, Plaintiff alleges that Defendants’ disclosure of her Contact Information has  
14 increased her risk of identity theft. That allegation is too speculative to satisfy the pleading  
15 requirement of contract damages. *See Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917-18 (N.D. Cal.  
16 2009).

17 In summary, it appears that a Gmail account and a Google Wallet account are free; all of  
18 the contractual privacy provisions upon which Plaintiff relies are contained in agreements that  
19 were entered into in connection with creation of those free accounts; and Plaintiff did not agree to  
20 any additional terms or pay any additional consideration when she purchased the \$1.77 App that  
21 forms the basis of this lawsuit. Under these circumstances, it is not clear how Plaintiff could  
22 amend her complaint to allege contract damages. However, because this motion is the first  
23 challenge to the complaint, Plaintiff will be afforded an opportunity to cure the defects noted  
24 herein.

25 Accordingly, Defendants’ motion is GRANTED with leave to amend as to Claim 1.

26 **2. Claim 2 – Breach of the Implied Covenant**

27 Claim 2 alleges breach of the implied covenant of good faith and fair dealing. “The  
28 implied promise [of good faith and fair dealing] requires each contracting party to refrain from



1 doing anything to injure the right of the other to receive the benefits of the agreement.” *Avidity*  
2 *Partners, LLC v. State of Cal.*, 221 Cal. App. 4th 1180, 1204 (2013) (quoting *Egan v. Mutual of*  
3 *Omaha Ins. Co.*, 24 Cal. 3d 809, 818 (1979)). “The implied covenant of good faith and fair  
4 dealing does not impose substantive terms and conditions beyond those to which the parties  
5 actually agreed.” *Id.*

6 Plaintiff alleges that Defendants’ disclosure of her Contact Information ran contrary to her  
7 reasonable expectations and interfered with her right to receive the full benefit of the contract.  
8 (Compl. ¶ 114) This allegation is duplicative of Plaintiff’s claim for breach of contract. When the  
9 allegations of a claim for breach of the implied covenant “do not go beyond the statement of a  
10 mere contract breach and, relying on the same alleged acts, simply seek the same damages or other  
11 relief already claimed in a companion contract cause of action, they may be disregarded as  
12 superfluous as no additional claim is actually stated.” *Careau & Co. v. Security Pacific Business*  
13 *Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990).

14 Plaintiff contends that there is no duplication of the contract claim in this case because the  
15 implied covenant claim includes additional allegations that “the Relevant Terms are standardized  
16 and non-negotiable terms, which Defendants, at their own discretion, interpreted to carry out the  
17 above-described privacy promises as they saw fit, in a way that resulted in transmission of  
18 Plaintiff and other Class members’ [Contact Information] to third-party App vendors.” (Compl. ¶  
19 112) While a claim for breach of the implied covenant may be made out by allegations that a  
20 defendant acted in bad faith to frustrate the agreed common purpose of the contract, *see Careau*,  
21 222 Cal. App. 3d at 1395, the bad faith alleged on the part of Defendants here is simply breaching  
22 the contract by disclosing Plaintiff’s Contact Information (*see* Compl. ¶ 114). Thus while Plaintiff  
23 may be able to flesh out this claim, as presently framed it is duplicative of her claim for breach of  
24 contract.

25 Defendants’ motion is GRANTED with leave to amend as to Claim 2.

26 **3. Claim 3 – Violation of SCA § 2701**

27 Claims 3 and 4 assert that Defendants’ disclosure of Plaintiff’s Contact Information  
28 violated §§ 2701 and 2702 of the SCA, respectively. *See* 18 U.S.C. §§ 2701-02. “Enacted in

1 1986 as Section II of the Electronic Communications Protection Act (“ECPA”), the SCA creates  
2 criminal and civil liability for certain unauthorized access to stored communications and records.”  
3 *In re iPhone Applic. Litig.*, 844 F. Supp. 2d 1040, 1056-57 (N.D. Cal. 2012); *see also Konop v.*  
4 *Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) (discussing enactment of SCA).

5 Section 2701 of the SCA creates a private right of action against anyone who “(1)  
6 intentionally *accesses without authorization a facility* through which an electronic communication  
7 service is provided; or (2) intentionally *exceeds an authorization to access that facility*; and  
8 thereby obtains, alters, or prevents authorized access to a wire or electronic communication while  
9 it is in electronic storage in such system.” 18 U.S.C. § 2701(a) (emphasis added); *see id.* § 2707(a)  
10 (creating a private right of action). The prohibitions set forth in § 2701(a) do not apply “to  
11 conduct authorized – (1) by the person or entity providing a wire or electronic communications  
12 service; [or] (2) by a user of that service with respect to a communication of or intended for that  
13 user.” 18 U.S.C. § 2701(c).

14 Plaintiff alleges that Defendants utilize “server facilities,” and that “[i]n the course of  
15 processing Plaintiff and the Class’s Google Wallet App online purchases, Defendants exceeded  
16 their authorized access to the facilities through which Defendants provide the electronic  
17 communications services at issue and within which their [Contact Information] was stored on  
18 Defendants’ servers, by unnecessarily transmitting or making available their [Contact Information]  
19 to third-party App vendors.” (Compl. 119, 124) These allegations are insufficient to state a claim  
20 under section 2701(a). It appears from the face of the complaint that the “facility” in question was  
21 *Defendants’ own servers*. (See Compl. ¶ 124, alleging that the Contact Information “was stored  
22 on Defendants’ servers”) Plaintiff does not allege any facts suggesting that Defendants were not  
23 authorized to access their own servers as required under § 2701(a). Likewise, it appears from the  
24 face of the complaint that *Defendants provide the electronic communications service at issue*.  
25 (See *id.* (alleging that “Defendants provide the electronic communications services at issue”))  
26 Plaintiff does not allege facts showing why Defendants thus would not be exempt from liability  
27 under § 2701(c). See 18 U.S.C. § 2701(c)(1) (exempting conduct authorized “by the person or  
28 entity providing a wire or electronic communications service”).

1 Another court in this district confronted with a similar claim that Google had violated §  
2 2701(a) held that:

3 This claim borders on frivolous, considering the plain language of subsection (c) of  
4 Section 2701[] that exempts conduct authorized “by the person or entity providing  
5 a wire or electronic communications service.” Whatever the propriety of Google’s  
6 actions, it plainly authorized actions that it took itself.

6 *In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382-PSG, 2013 WL 6248499, at \*12 (N.D.  
7 Cal. Dec. 3, 2013) (footnote omitted). This Court agrees with the above analysis, and with other  
8 district courts that have dismissed § 2701(a) claims based upon the plaintiff’s failure to allege  
9 unauthorized access to a “facility.” *See, e.g., In re iPhone Applic. Litig.*, 844 F. Supp. 2d at 1057-  
10 58 (dismissing § 2701(a) claim after concluding that the iPhones allegedly accessed by the  
11 defendants were not “facilities” within the meaning of the statute).

12 At the hearing, Plaintiff’s counsel argued that by sending Plaintiff’s Contact Information to  
13 the third-party vendor, Defendants in essence granted the third-party vendor access to its servers  
14 (the “facility”). While Plaintiff raises an interesting question with respect to the meaning of  
15 “access” in the digital age, in order to make out a § 2701 claim against *Defendants*, Plaintiff must  
16 allege that *Defendants* engaged in unauthorized access of the facility. This they plainly cannot do  
17 here, as the facility in question belongs to Defendants.

18 Plaintiff argues that the line of cases discussed above applies §§ 2701(a) and (c) by rote,  
19 without giving sufficient consideration to whether a service provider should have blanket authority  
20 to access information on its servers. (*See Opp.* at 24, ECF 38) Regardless of the merits of  
21 Plaintiff’s policy arguments, this Court is without authority to alter the plain language of the  
22 statute, which clearly does not apply to the facts alleged in the complaint. The cases relied upon  
23 by Plaintiff address different statutes or otherwise fail to support the statutory construction she  
24 urges here.

25 Accordingly, Defendants’ motion is GRANTED without leave to amend as to Claim 3.

26 **4. Claim 4 – Violation of SCA § 2702**

27 Section 2702 of the SCA creates a private right of action for violation of the following  
28 provisions:

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

(a) Prohibitions. – Except as provided in subsection (b) or (c) –

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the *contents of a communication* while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the *contents of any communication* which is carried or maintained on that service –

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

18 U.S.C. § 2702(a) (emphasis added); *see id.* § 2707(a) (creating a private right of action).

While a provider described in subsection (a) may not disclose the “contents of a communication,” such provider may divulge “*a record* or other information” regarding a subscriber or customer to “any person other than a governmental entity” and to governmental entities under certain circumstances. 18 U.S.C. § 2702(c) (emphasis added).

For purposes of this motion, Defendants do not dispute that Google is an entity “providing an electronic communication service” and/or “providing remote computing service” within the meaning of § 2702(a). (*See Mot. at 17 n.10*) The question presented by this motion is whether the Contact Information that Defendants sent to the third-party vendor was “contents of a communication” or “a record or other information”; if the former, Plaintiff has made out a claim under § 2702(a), but if the latter she has not. For the reasons discussed below, the Court concludes that the facts alleged in the complaint establish the disclosure of record information rather than contents of a communication.

“The ‘contents’ of a communication are ‘any information concerning the substance, purport, or meaning of that communication.’ *Zynga*, 750 F.3d at 1105 (citing 18 U.S.C. §

1 2510(8)); *see also id.* at 1104 (noting that the SCA incorporates the Wiretap Act’s definition of  
2 “contents”). The Ninth Circuit has explained that “the term ‘contents’ refers to the intended  
3 message conveyed by the communication, and does not include record information regarding the  
4 characteristics of the message that is generated in the course of the communication.” *Id.* at 1106.  
5 The Ninth Circuit has recognized that record information generally includes “the name, address, or  
6 client ID number of the entity’s customers.” *Id.* at 1104.

7 In *Zynga*, the plaintiffs claimed that when users clicked on certain ads or icons on a  
8 Facebook webpage, the web browser sent a request to access the resource identified by the link  
9 and *also* sent a “referrer header” comprising the user’s Facebook ID and the address of the  
10 Facebook webpage the user was viewing when the user clicked the link. *Zynga*, 750 F.3d at 1101-  
11 02. The plaintiffs alleged that the referrer header constituted contents of a communication such  
12 that its transmission to third parties violated § 2702(a). The Court held that the referrer header did  
13 not meet the definition of “contents.” *Id.* at 1107. Equating the Facebook ID with a user’s  
14 “name” or “subscriber number or identity,” and equating the webpage address with a user’s  
15 “address,” the Court held that “these pieces of information are not the ‘substance, purport, or  
16 meaning’ of a communication.” *Id.*

17 The Court distinguished *In re Pharmatrak*, 329 F.3d 9 (1st Cir. 2003), a Wiretap Act case  
18 in which the defendants allegedly intercepted the contents of electronic communications,  
19 specifically, information that individuals provided to online pharmaceutical websites. That  
20 information included the individuals’ “names, addresses, telephone numbers, email addresses,  
21 dates of birth, genders, insurance statuses, education levels, occupations, medical conditions,  
22 medications, and reasons for visiting the particular website.” *Id.* at 15. It was undisputed that the  
23 information constituted “contents” of a communication under the circumstances of the case; the  
24 arguments focused on whether the “interception” element of the Wiretap Act claim was satisfied  
25 and whether the consent exception applied. *Id.* at 18. The Ninth Circuit opined in *Zynga* that the  
26 information in *Pharmatrak* properly was characterized as contents of a communication “[b]ecause  
27 the users had communicated with the website by *entering their personal medical information into*  
28 *a form provided by a website.*” *Zynga*, 750 F.3d at 1107 (emphasis added). The Ninth Circuit

1 distinguished the case before it by noting that the *Zynga* defendants did not divulge a user’s  
2 communications to a website but allegedly “divulged identification and address information  
3 contained in a referrer header automatically generated by the web browser.” *Id.*

4 Although *Zynga* distinguished *Pharmatrak* in part on the basis that the referrer header at  
5 issue in *Zynga* was automatically generated, this Court does not read *Zynga* so narrowly to mean  
6 that *only* automatically generated data may constitute record information. The Contact  
7 Information at issue in the present case – the user’s name, email address, Google account name,  
8 home city and state, zip code, and in some instances telephone number – is the type of information  
9 that the Ninth Circuit recognized as record information in *Zynga*. *See Zynga* at 1104 (recognizing  
10 that record information generally includes “the name, address, or client ID number of the entity’s  
11 customers”). Numerous courts in this district likewise have characterized such information as  
12 record information in the context of civil discovery. *See, e.g. Chevron Corp. v. Donziger*, No. 12-  
13 mc-80237 CRB (NC), 2013 WL 4536808, at \*6 (N.D. Cal. Aug. 22, 2013) (characterizing  
14 information associated with the creation of an email address, including names, mailing addresses,  
15 phone numbers, billing information, and date of account creation, as “record or other information”  
16 and not “contents” of a communication); *Obodai v. Indeed, Inc.*, No. 13-80027-MISC EMC  
17 (KAW), 2013 WL 1191267, at \*3 (N.D. Cal. Mar. 21, 2013) (holding that no “content” of  
18 communications was implicated by a subpoena seeking “subscriber information” provided when a  
19 user creates a Gmail account, such as phone numbers and alternative email addresses). To hold  
20 that such information constitutes contents of a communication unless it was automatically  
21 generated would read § 2702(c) out of the statute.

22 Plaintiff relies heavily upon her assertion that the Contact Information was entered  
23 by means of a form interface such as that used in *Pharmatrak*, although that fact is not clear from  
24 the complaint. Even assuming Plaintiff’s assertion to be true, the Court is not persuaded that the  
25 form interface was critical to the *Pharmatrak* decision. As noted above, it was undisputed in  
26 *Pharmatrak* that the information in question constituted contents of a communication. Indeed, any  
27 court would be hard-pressed to find that the highly personal disclosures in that case, which  
28 included insurance statuses, medical conditions, and medications, constituted mere record

1 information. The fact that the Ninth Circuit distinguished *Pharmatrak* on the additional ground  
2 that the information therein was input by means of a form interface does not mandate a conclusion  
3 that *all* information input by means of a form interface constitutes contents of a communication  
4 under § 2702(a). Such a conclusion would have broad implications in the civil discovery context,  
5 as information routinely obtained by subpoena no longer would be available by that means. This  
6 Court is unwilling to construe the term “contents” so broadly absent clearer direction from the  
7 Ninth Circuit or the Supreme Court.

8 Plaintiff further urges this Court to consider the holding in *Yunker v. Pandora Media, Inc.*,  
9 No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013). The Court does not find  
10 *Yunker* to be persuasive. First, in *Yunker* the § 2702 claim was dismissed on the ground that the  
11 plaintiff had failed to allege disclosure of contents of a communication “while in electronic  
12 storage.” *Id.* at \*8. That aspect of the statute is not at issue here. Second, in *Yunker* the scope of  
13 the disclosed information was broader than in the present case, including not only a universally  
14 unique device identifier and zip code, but also the user’s gender and birthday. *Id.* at \*6. The  
15 *Yunker* court declined to conclude that such information “cannot comprise the ‘substance, purport,  
16 or meaning’ of a communication.” *Id.* However, the court was careful to limit its ruling to the  
17 facts before it. *Id.*

18 After review of the complaint and the relevant authorities, the Court concludes that the  
19 facts alleged establish that “a record or other information” about Plaintiff was disclosed to the  
20 third-party vendor rather than “contents of a communication.” Given the analysis set forth herein,  
21 Plaintiff must consider whether she can allege additional facts that would demonstrate that the  
22 alleged disclosure was more than record information. Because the complaint has not previously  
23 been challenged by motion or addressed by the Court, Plaintiff is afforded the opportunity to do  
24 so. Accordingly, Defendants’ motion is GRANTED with leave to amend as to Claim 4.

25 **5. Claim 5 – Violation of California’s UCL**

26 Claim 5 asserts a violation of California Business & Professions Code § 17200 *et seq.* In  
27 order to state a claim for relief under that provision, Plaintiff must allege facts showing that  
28 Defendants engaged in an “unlawful, unfair or fraudulent business act or practice.” Cal. Bus. &

1 Prof. Code § 17200. “Because the statute is written in the disjunctive, it is violated where a  
2 defendant’s act or practice violates any of the foregoing prongs.” *Davis v. HSBC Bank Nevada,*  
3 *N.A.*, 691 F.3d 1152, 1168 (9th Cir. 2012). Plaintiff asserts claims under both the unlawful and  
4 unfair prongs.<sup>2</sup>

5 While Defendants identify numerous pleading defects with respect to both prongs – for  
6 example, Plaintiff asserts a claim under the unlawful prong based upon Defendants’ alleged  
7 violation of the SCA but has failed to make out a claim under the SCA – the Court concludes that  
8 the claim suffers from a more fundamental defect that obviates the need for further analysis. In  
9 order to maintain a claim under the UCL, Plaintiff must allege that she has suffered (1) economic  
10 injury (2) as a result of the alleged unfair business practice. *See Kwikset Corp. v. Sup. Ct.*, 51 Cal.  
11 4th 310, 323 (2011). Plaintiff has not alleged any facts showing that Defendants’ business  
12 practice – disclosing users’ Contact Information to third-party App vendors – changed her  
13 economic position at all. Plaintiff alleges that she purchased an App for \$1.77 and received that  
14 App. (Compl. ¶ 74, ECF 5-1) As is discussed in connection with the contract claim, Plaintiff has  
15 not alleged facts showing that she suffered any damages resulting from that transaction. Unless  
16 and until Plaintiff can allege economic injury resulting from Defendants’ practice of disclosing  
17 Contact Information, she cannot proceed with a UCL claim.

18 Based upon the foregoing, the motion to dismiss is GRANTED as to Claim 5 with leave to  
19 amend.

20 //  
21 //  
22 //  
23 //  
24 //

25 \_\_\_\_\_  
26 <sup>2</sup> At the hearing, Defendants’ counsel asserted that Plaintiff’s UCL claim most properly should be  
27 analyzed under the fraud prong, because in essence it is a promissory fraud claim. Because  
28 Plaintiff does not expressly allege a claim under the fraud prong, the Court limits its analysis to  
whether Plaintiff has stated a claim under the unlawful and unfair prongs. As a practical matter,  
analysis under the fraud prong would not change the outcome of the motion given the Court’s  
disposition of the claim based upon failure to allege economic injury.



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

**IV. ORDER**

- (1) Defendants’ Motion to Dismiss for lack of Article III standing is DENIED;
- (2) Defendants’ Motion to Dismiss for failure to state a claim is GRANTED as to Claims 1, 2, 4, and 5 with leave to amend and as to Claim 3 without leave to amend;
- (3) Leave to amend is limited to the claims addressed in this order; Plaintiff may not add additional claims without express leave of the Court;
- (3) Any amended complaint shall be filed on or before September 2, 2014; and
- (4) Any amended complaint shall be electronically filed in a searchable PDF format in compliance with Civil Local Rule 5-1(e)(2).<sup>3</sup>

Dated: August 12, 2014

  
BETH LABSON FREEMAN  
United States District Judge

---

<sup>3</sup> Because Plaintiff’s original complaint was converted to PDF from a scanned document, the Court was unable to conduct text searches of the complaint.