

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**  
For the Northern District of California

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

In re Facebook Privacy Litigation

NO. C 10-02389 JW

**ORDER GRANTING IN PART AND  
DENYING IN PART DEFENDANT’S  
MOTION TO DISMISS**

**I. INTRODUCTION**

Plaintiffs<sup>1</sup> bring this putative class action against Facebook, Inc. (“Defendant”) alleging violations of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*, California’s Unfair Competition Law, California Business & Professions Code §§ 17200, *et seq.*, and breach of contract. Plaintiffs allege that Defendant intentionally and knowingly transmitted personal information about Plaintiffs to third-party advertisers without Plaintiffs’ consent.

Presently before the Court is Defendant’s Motion to Dismiss.<sup>2</sup> The Court conducted a hearing on March 28, 2011. Based on the papers submitted to date and oral argument, the Court GRANTS in part and DENIES in part Defendant’s Motion to Dismiss.

---

<sup>1</sup> Named Plaintiffs are David Gould and Mike Robertson, both of whom are residents of California who have been registered users of Defendant’s services since at least 2008.

<sup>2</sup> (See Defendant’s Motion to Dismiss Consolidated Class Action Complaint, hereafter, “Motion,” Docket Item No. 75.)

1 **II. BACKGROUND**

2 In a Consolidated Class Action Complaint<sup>3</sup> filed on October 11, 2010, Plaintiffs allege as  
3 follows:

4 Defendant is a Delaware corporation that maintains its headquarters in Santa Clara  
5 County, California. (Complaint ¶ 6.) Defendant operates the world’s largest social  
6 networking website. (Id. ¶ 11.) Defendant allows anyone with access to a computer and  
7 Internet connection to register for its services free of charge. (Id. ¶ 12.) One of the few  
8 requirements Defendant places on its registrants is that they provide their actual names. (Id.  
9 ¶ 13.) Once registered, a user of Defendant’s website may also post personal information to  
10 a “profile” webpage. (Id. ¶ 14.)

11 Each user of Defendant’s website has a user ID number which uniquely identifies that  
12 user. (Complaint ¶ 15.) If a person knows the user ID number or “username” of an  
13 individual who is a user of Defendant’s website, that person can see the user’s profile  
14 webpage and see the user’s real name, gender, picture, and other information. (Id.)

15 Defendant now “serves more ad[vertisement] impressions than any other online  
16 entity.” (Complaint ¶ 18.) Because it possesses personal information about its users,  
17 Defendant’s advertisers are able to target advertising to users of Defendant’s website. (Id.  
18 ¶ 19.) Defendant’s own policies prohibit Defendant from revealing any user’s “true identity”  
19 or specific personal information to advertisers. (Id. ¶¶ 20-25.)

20 When a user of Defendant’s website clicks on an advertisement posted on the  
21 website, Defendant sends a “Referrer Header” to the corresponding advertiser. (Complaint  
22 ¶ 28.) This Referrer Header reveals the specific webpage address that the user was looking  
23 at prior to clicking on the advertisement. (Id.) Thus, Defendant has caused users’ Internet  
24 browsers to send Referrer Header transmissions which report the user ID or username of the  
25 user who clicked on an advertisement, as well as information identifying the webpage the  
26

---

27 <sup>3</sup> (Consolidated Class Action Complaint, hereafter, “Complaint,” Docket Item No. 36.)

1 user was viewing just prior to clicking on that advertisement. (Id.) Because of this, when an  
2 advertiser receives a Referrer Header transmission from Defendant, the advertiser can obtain  
3 substantial additional information about a user of Defendant’s website, such as the user’s  
4 name, gender and picture. (Id. ¶ 29.) Through these transmissions, Defendant shares users’  
5 personal information with third-party advertisers without users’ knowledge or consent, in  
6 violation of Defendant’s own policies. (Id. ¶ 27.)

7 Defendant began these transmissions no later than February, 2010, and they  
8 continued until May 21, 2010. (Complaint ¶¶ 31-33.) Software engineers employed by  
9 Defendant knew or should have known that these transmissions would divulge private user  
10 information to third-party advertisers. (Id. ¶ 36.) As a result of Defendant’s misconduct,  
11 Plaintiffs “suffered injury.” (Id. ¶ 109.)

12 On the basis of the allegations outlined above, Plaintiffs assert eight causes of action: (1)  
13 Violation of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2510, *et seq.*; (2)  
14 Violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*; (3) Violation of  
15 California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200, *et seq.*; (4)  
16 Violation of California’s Computer Crime Law, Cal. Penal Code § 502; (5) Violation of the  
17 Consumers Legal Remedies Act (“CLRA”), Cal. Civ. Code §§ 1750, *et seq.*; (6) Breach of Contract;  
18 (7) Violation of Cal. Civ. Code §§ 1572, 1573; and (8) Unjust Enrichment.

19 Presently before the Court is Defendant’s Motion to Dismiss pursuant to Rule 12(b)(1) and  
20 Rule 12(b)(6).

21 **III. STANDARDS**

22 **A. Lack of Subject Matter Jurisdiction**

23 Rule 12(b)(1) of the Federal Rules of Civil Procedure provides for a motion to dismiss for  
24 lack of subject-matter jurisdiction. A Rule 12(b)(1) motion may be either facial, where the inquiry  
25 is confined to the allegations in the complaint, or factual, where the court is permitted to look  
26 beyond the complaint to extrinsic evidence. Wolfe v. Strankman, 392 F.3d 358, 362 (9th Cir. 2004).  
27 On a facial challenge, all material allegations in the complaint are assumed true, and the question for  
28

1 the court is whether the lack of federal jurisdiction appears from the face of the pleading itself. See  
2 Wolfe, 392 F.3d at 362; Thornhill Publishing Co. v. General Telephone Electronics, 594 F.2d 730,  
3 733 (9th Cir. 1979). When a defendant makes a factual challenge “by presenting affidavits or other  
4 evidence properly brought before the court, the party opposing the motion must furnish affidavits or  
5 other evidence necessary to satisfy its burden of establishing subject-matter jurisdiction.” Safe Air  
6 For Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). The court need not presume the  
7 truthfulness of the plaintiff’s allegations under a factual attack. White v. Lee, 227 F.3d 1214, 1242  
8 (9th Cir. 2000); Augustine v. United States, 704 F.2d 1074, 1077 (9th Cir. 1983). However, in the  
9 absence of a full-fledged evidentiary hearing, disputes in the facts pertinent to subject-matter are  
10 viewed in the light most favorable to the opposing party. Dreier v. United States, 106 F.3d 844, 847  
11 (9th Cir. 1996). The disputed facts related to subject-matter jurisdiction should be treated in the  
12 same way as one would adjudicate a motion for summary judgment. Id.

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

14 Pursuant to Federal Rule of Civil Procedure 12(b)(6), a complaint may be dismissed against  
15 a defendant for failure to state a claim upon which relief may be granted against that defendant.  
16 Dismissal may be based on either the lack of a cognizable legal theory or the absence of sufficient  
17 facts alleged under a cognizable legal theory. Balistreri v. Pacifica Police Dep’t, 901 F.2d 696, 699  
18 (9th Cir. 1990); Robertson v. Dean Witter Reynolds, Inc., 749 F.2d 530, 533-534 (9th Cir. 1984).  
19 For purposes of evaluating a motion to dismiss, the court “must presume all factual allegations of the  
20 complaint to be true and draw all reasonable inferences in favor of the nonmoving party.” Usher v.  
21 City of Los Angeles, 828 F.2d 556, 561 (9th Cir. 1987). Any existing ambiguities must be resolved  
22 in favor of the pleading. Walling v. Beverly Enters., 476 F.2d 393, 396 (9th Cir. 1973).

23 However, mere conclusions couched in factual allegations are not sufficient to state a cause  
24 of action. Papasan v. Allain, 478 U.S. 265, 286 (1986); see also McGlinchy v. Shell Chem. Co., 845  
25 F.2d 802, 810 (9th Cir. 1988). The complaint must plead “enough facts to state a claim for relief  
26 that is plausible on its face.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007). Courts  
27  
28

1 may dismiss a case without leave to amend if the plaintiff is unable to cure the defect by  
2 amendment. Lopez v. Smith, 203 F.3d 1122, 1129 (9th Cir. 2000).

3 **IV. DISCUSSION**

4 Defendant moves to dismiss on the grounds that: (1) Plaintiffs fail to allege injury-in-fact  
5 that would give them standing to maintain an action in federal court; (2) Plaintiffs fail to state a  
6 claim under the Wiretap Act, because they do not allege disclosure of the “contents of a  
7 communication”; (3) Plaintiffs fail to state a claim under the Stored Communications Act, because  
8 they do not allege disclosure of the “contents of a communication” and because the same conduct  
9 cannot be a violation of both the Wiretap Act and the Stored Communications Act; (4) Plaintiffs fail  
10 to state a claim under the UCL because they lack standing, since they have not alleged that they have  
11 lost money or property; (5) Plaintiffs fail to state a claim under Cal. Penal Code § 502 because  
12 Defendant’s activities do not amount to the type of “hacking” or “breaking into a computer” that the  
13 law was intended to prohibit; (6) Plaintiffs fail to state a claim under the CLRA, because such claims  
14 can only be brought by consumers; (7) Plaintiffs fail to state a claim for Breach of Contract, because  
15 they do not allege that they suffered appreciable or actual damage; (8) Plaintiffs fail to state a claim  
16 under Cal. Civ. Code §§ 1572 and 1573, because they do not allege that they relied upon  
17 Defendant’s representations or were damaged by them; and (9) Plaintiffs fail to state a claim for  
18 Unjust Enrichment, because Plaintiffs cannot assert unjust enrichment while simultaneously alleging  
19 a breach of contract. (Motion at 6-24.)

20 Plaintiffs respond that: (1) Plaintiffs have alleged a violation of their statutory rights, which  
21 is a sufficient allegation of injury-in-fact to give them standing; (2) Plaintiffs state a claim under the  
22 Wiretap Act, because Plaintiffs allege that Defendant disclosed the contents of Plaintiffs’  
23 communications to entities that were not intended recipients of those communications, and the  
24 communications were not “readily accessible to the general public”; (3) Plaintiffs state a claim under  
25 the Stored Communications Act, because Plaintiffs allege that Defendant disclosed the contents of  
26 Plaintiffs’ communications to entities that were not intended recipients of those communications,  
27  
28

1 and the communications were not “readily accessible to the general public”;<sup>4</sup> (4) Plaintiffs state a  
2 claim under the UCL, because they have alleged facts sufficient to establish standing under the  
3 UCL, and have alleged that Defendant violated each of the three “prongs” of the UCL; (5) Plaintiffs  
4 state a claim under Cal. Penal Code § 502, because they allege that Defendant accessed their  
5 personal data in an unauthorized way; (6) Plaintiffs state a claim under the CLRA, because they are  
6 “consumers” within the meaning of the CLRA; (7) Plaintiffs state a claim for Breach of Contract,  
7 because they have alleged actionable damages caused by the diminution in value of Plaintiffs’  
8 personal information; (8) Plaintiffs state a claim under Cal. Civil Code §§ 1572 and 1573, because  
9 they have pleaded in sufficient detail Defendant’s fraudulent actions; and (9) Plaintiffs state a claim  
10 for Unjust Enrichment in the alternative to Breach of Contract, because they are entitled to  
11 simultaneously allege the existence of an express contract and maintain a claim for unjust  
12 enrichment. (Opp’n at 4-25.) The Court addresses each ground in turn.

13 **A. Injury-in-Fact**

14 At issue is whether Plaintiffs have alleged injury-in-fact sufficiently to establish standing.

15 To satisfy the standing requirements of Article III, a plaintiff must show that he has suffered  
16 an “injury in fact” that is (a) concrete and particularized and (b) actual or imminent, not conjectural  
17 or hypothetical. Gest v. Bradbury, 443 F.3d 1177, 1181 (9th Cir. 2006) (citing Friends of the Earth  
18 v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167, 180-81 (2000)). The injury required  
19 by Article III can exist solely by virtue of “statutes creating legal rights, the invasion of which  
20 creates standing.” Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010) (quoting Warth v.  
21 Seldin, 422 U.S. 490, 500 (1975)). In such cases, the “standing question . . . is whether the  
22 constitutional or statutory provision on which the claim rests properly can be understood as granting  
23 persons in the plaintiff’s position a right to judicial relief.” Id. (quoting Warth, 422 U.S. at 500)).

---

24  
25 <sup>4</sup> Plaintiffs do not distinguish between their claims under Title I of the ECPA (the Wiretap  
26 Act) and Title II of the ECPA (the Stored Communications Act). (See Plaintiffs’ Opposition to  
27 Facebook’s Motion to Dismiss Consolidated Class Action Complaint 11-17, hereafter, “Opp’n,”  
28 Docket Item No. 86.) Instead, Plaintiffs appear to assume that the same allegations suffice to state a  
claim under both the Wiretap Act and the Stored Communications Act. (See id. at 11.)

1 Here, Plaintiffs allege as follows:

2 From at least February 2010, and until May 21, 2010, Defendant transmitted to  
3 advertisers communications which disclosed both users' identities and the URL of the  
4 webpage the user was viewing when that user clicked on an advertisement. (Complaint  
5 ¶¶ 31-33.) By divulging user identities and other user information to advertisers without user  
6 consent, Defendant intentionally violated, *inter alia*, 18 U.S.C. § 2511(3)(a). (*Id.* ¶ 57.)  
7 Both Plaintiffs were registered users of Defendant's services during the relevant time period.  
8 (*Id.* ¶¶ 4, 5.) Both Plaintiffs clicked on at least one third-party advertisement displayed on  
9 Defendant's website during the relevant time period. (*Id.*)

10 Based on the allegations above, and without addressing the merits of the claim, the Court  
11 finds that Plaintiffs allege a violation of their statutory rights under the Wiretap Act, 18 U.S.C. §§  
12 2510, *et seq.* The Wiretap Act provides that any person whose electronic communication is  
13 "intercepted, disclosed, or intentionally used" in violation of the Act may in a civil action recover  
14 from the entity which engaged in that violation. 18 U.S.C. § 2520(a). Thus, the Court finds that  
15 Plaintiffs have alleged facts sufficient to establish that they have suffered the injury required for  
16 standing under Article III.<sup>5</sup>

17 Defendant's contention that at the pleading stage of a class action, each individual plaintiff  
18 must include allegations sufficient to establish injury-in-fact as to each of them is mistaken.  
19 (Motion at 6-7.) In Hepting v. AT&T Corp.,<sup>6</sup> the court rejected a similar argument. In Hepting, the  
20 court considered allegations that the defendant had "created a dragnet" which collected the contents  
21 of its customer's communications. *Id.* at 1000. The court found that it would be impossible for "any  
22 one plaintiff [to] have failed to demonstrate injury-in-fact if that plaintiff effectively demonstrates  
23 that all class members have so suffered." *Id.* The court held that the mere fact that the named  
24 plaintiffs each alleged that they were the defendant's "customers during the relevant time period"  
25 was sufficient to establish that the defendant's alleged conduct "would have imparted a concrete  
26 injury on each of them." *Id.* Similarly, if Plaintiffs here are able to show that Defendant transmitted

---

27 <sup>5</sup> A plaintiff may satisfy the injury-in-fact requirements to have standing under Article III,  
28 and thus may be able to "bring a civil action without suffering dismissal for want of standing to  
sue," without being able to assert a cause of action successfully. See Doe v. Chao, 540 U.S. 614,  
624-25 (2004) (stating that a plaintiff may have "injury enough to open the courthouse door, but  
without more [may have] no cause of action" under which he can successfully obtain relief).

<sup>6</sup> 439 F. Supp. 2d 974 (N.D. Cal. 2006).

1 the contents of its users’ communications in the manner alleged, they will have effectively  
2 demonstrated that all of the users of Defendant’s website suffered the same injury, which will  
3 necessarily mean that each individual Plaintiff will have demonstrated that he was injured.

4 Accordingly, the Court DENIES Defendant’s Motion to Dismiss on the ground that Plaintiffs  
5 have failed to allege injury-in-fact sufficient to establish standing.

6 **B. Wiretap Act**

7 At issue is whether Plaintiffs state a claim under the Wiretap Act.

8 The Wiretap Act states that an entity “providing an electronic communication service to the  
9 public shall not intentionally divulge the contents of any communication (other than one to such  
10 entity, or an agent thereof) while in transmission on that service to any person or entity other than an  
11 addressee or intended recipient of such communication or an agent of such addressee or intended  
12 recipient.” 18 U.S.C. § 2511(3)(a).

13 Here, Plaintiffs allege as follows:

14 When a user of Defendant’s website clicks on an advertisement banner displayed on  
15 that website, the user is asking Defendant to send an electronic communication to the  
16 advertiser who supplied the advertisement. (Complaint ¶ 56.) However, users do not expect  
17 and do not consent to Defendant’s disclosure of all contents of that communication. (Id.)  
18 Users expect that certain aspects of their communications concerning advertisers—namely,  
19 their identities and the webpage they were viewing at the time they clicked on an  
20 advertisement—will be configured by Defendant to be private. (Id.)

21 Based on the allegations above, the Court finds that there are two possible ways to  
22 understand Plaintiffs’ allegations. On the first view, Plaintiffs allege that when a user of  
23 Defendant’s website clicks on an advertisement banner displayed on that website, that click  
24 constitutes an electronic communication from the user to Defendant.<sup>7</sup> Under this interpretation, the  
25 content of the user’s communication with Defendant is a request that Defendant “send [a further]  
26 electronic communication to [an] advertiser.” On the second view, Plaintiffs allege that when a user  
27 of Defendant’s website clicks on an advertisement banner, that click constitutes an electronic  
28

---

<sup>7</sup> This interpretation is embraced by Plaintiffs themselves in their Opposition, though the Consolidated Class Action Complaint itself is ambiguous on this point. (See Opp’n at 11-12, 16.)

1 communication from the user to the advertiser. Under this interpretation, Plaintiffs are merely  
2 “asking Defendant” to pass the communication along to its intended recipient, who is the advertiser.

3 The Court finds that as a matter of law, Plaintiffs cannot state a claim under the Wiretap Act  
4 under either interpretation. Under the first interpretation, the communication is sent from the user to  
5 Defendant. However, the Wiretap Act states that an “entity providing an electronic communication  
6 service to the public shall not intentionally divulge the contents of any communication (*other than*  
7 *one to such person or entity, or an agent thereof*) . . . “ 18 U.S.C. § 2511(3)(a) (emphasis added).  
8 Because, under the first interpretation, the communication at issue is one from a user *to* Defendant,  
9 Defendant cannot be liable under the Wiretap Act for divulging it. Under the second interpretation,  
10 the communication is sent from the user to an advertiser. However, the Wiretap Act states that an  
11 “entity providing an electronic communication service to the public shall not intentionally divulge  
12 the contents of any communication . . . to any person or entity *other than an addressee or intended*  
13 *recipient of such communication.*” *Id.* (emphasis added). Because, under the second interpretation,  
14 the communication at issue is a communication from a user to an advertiser, the advertiser is its  
15 “addressee or intended recipient,” and Defendant cannot be liable under the Wiretap Act for  
16 divulging it. Thus, because Plaintiffs cannot state a claim under the Wiretap Act on their own  
17 allegations, the Court dismisses Plaintiffs’ Wiretap Act claim.

18 Accordingly, the Court GRANTS Defendant’s Motion to Dismiss Plaintiffs’ Cause of Action  
19 under the Wiretap Act without prejudice, with leave to amend to allege specific facts showing that  
20 the information allegedly disclosed by Defendant was not part of a communication from Plaintiffs to  
21 an addressee or intended recipient of that communication, if so desired.

22 **C. Stored Communications Act**

23 At issue is whether Plaintiffs state a claim under the Stored Communications Act.

24 Under the Stored Communications Act, an entity providing an electronic communication  
25 service to the public “shall not knowingly divulge to any person or entity the contents of a  
26 communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1). However, a  
27 provider of an electronic communication service may divulge the contents of a communication to an  
28

1 addressee or intended recipient of such communication. Id. § 2702(b)(1). A provider of an  
2 electronic communication service may also divulge the contents of a communication with “the  
3 lawful consent” of an addressee or intended recipient of such communication. Id. § 2702(b)(3).

4 As discussed previously, Plaintiffs either allege that the communications at issue were sent to  
5 Defendant or to advertisers. Under either interpretation, Plaintiffs fail to state a claim under the  
6 Stored Communications Act. If the communications were sent to Defendant, then Defendant was  
7 their “addressee or intended recipient,” and thus was permitted to divulge the communications to  
8 advertisers so long as it had its own “lawful consent” to do so.<sup>8</sup> 18 U.S.C. § 2702(b)(3). In the  
9 alternative, if the communications were sent to advertisers, then the advertisers were their  
10 addressees or intended recipients, and Defendant was permitted to divulge the communications to  
11 them. Id. § 2702(b)(1). Thus, because Plaintiffs cannot state a claim under the Stored  
12 Communications Act on their own allegations, the Court dismisses Plaintiffs’ Stored  
13 Communications Act claim with prejudice.

14 Accordingly, the Court GRANTS Defendant’s Motion to Dismiss Plaintiffs’ Cause of Action  
15 under the Stored Communications Act without prejudice, with leave to amend to allege specific facts  
16 showing that the information allegedly disclosed by Defendant was not part of a communication  
17 from Plaintiffs to an addressee or intended recipient of that communication, if so desired.

---

23 <sup>8</sup> Plaintiffs do not contend that Defendant would be unable to give itself “lawful consent” to  
24 divulge Plaintiffs’ communications to Defendant. In similar situations, courts have held that a  
25 defendant cannot be liable under the Stored Communications Act for disclosing communications  
26 where the defendant was itself the “addressee or intended recipient” of those communications. See,  
27 e.g., In re Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 560-61 (N.D. Tex. 2005) (holding  
that a defendant was not liable under the Stored Communications Act for disclosing personal  
information of which it was the intended recipient, even if the defendant was “contractually bound  
by its privacy policy not to disclose [such] information” and could be held liable for breach of  
contract for doing so).

1 **D. UCL**

2 At issue is whether Plaintiffs state a claim for violation of the UCL.

3 To assert a UCL claim, a private plaintiff needs to have “suffered injury in fact and . . . lost  
4 money or property as a result of the unfair competition.” Rubio v. Capital One Bank, 613 F.3d  
5 1195, 1203 (9th Cir. 2010). A plaintiff’s “personal information” does not constitute property under  
6 the UCL. Thompson v. Home Depot, Inc., No. 07cv1058 IEG, 2007 WL 2746603, at \*3 (S.D. Cal.  
7 Sept. 18, 2007).

8 Here, Plaintiffs do not allege that they lost money as a result of Defendant’s conduct.  
9 Instead, Plaintiffs allege that Defendant unlawfully shared their “personally identifiable  
10 information” with third-party advertisers. (Complaint ¶¶ 1-3.) However, personal information does  
11 not constitute property for purposes of a UCL claim. Thompson, 2007 WL 2746603, at \*3.

12 Plaintiffs’ reliance on Doe 1 v. AOL, LLC<sup>9</sup> is misplaced. In AOL, the court considered  
13 claims under the UCL brought by plaintiffs whose personal and financial information had been  
14 disclosed to the public by an Internet service provider. Id. at 1111. Significantly, the AOL court  
15 found that the defendant’s “disclosure of members’ undeniably sensitive information,” including  
16 such “highly-sensitive financial information” as credit card numbers, social security numbers,  
17 financial account numbers and passwords, was “not something that members bargained for when  
18 they signed up and *paid fees for* [the defendant’s] service.” Id. at 1113 (emphasis added). The  
19 court’s opinion in AOL does not stand for the broad proposition that personal information of any  
20 kind “equates to money or property.” (See Opp’n at 9.) Rather, it indicates that a plaintiff who is a  
21 *consumer* of certain services (i.e., who “paid fees” for those services) may state a claim under  
22 certain California consumer protection statutes when a company, in violation of its own policies,  
23 discloses personal information about its consumers to the public. See AOL, 719 F. Supp. 2d at  
24 1111-13. Here, by contrast, Plaintiffs do not allege that they paid fees for Defendant’s services.  
25 Instead, they allege that they used Defendant’s services “free of charge.” (Complaint ¶ 12.)

26  
27 <sup>9</sup> 719 F. Supp. 2d 1102 (N.D. Cal. 2010).

1 Because Plaintiffs allege that they received Defendant’s services for free, as a matter of law,  
2 Plaintiffs cannot state a UCL claim under their own allegations. Thus, the Court dismisses  
3 Plaintiffs’ UCL claim with prejudice.<sup>10</sup>

4 Accordingly, the Court GRANTS Defendant’s Motion to Dismiss Plaintiffs’ Cause of Action  
5 under the UCL with prejudice.

6 **E. Cal. Penal Code § 502**

7 At issue is whether Plaintiffs state a claim under Cal. Penal Code § 502.

8 Cal. Penal Code § 502, the Comprehensive Computer Data Access and Fraud Act, was  
9 enacted to expand the degree of protection to individuals, businesses and government agencies from  
10 “tampering, interference, damage, and unauthorized access to lawfully created computer data and  
11 computer systems.” Cal. Penal Code § 502(a). With one exception, the subsections of Section 502  
12 that potentially apply in this case require that the defendant’s actions be taken “without permission.”  
13 See Cal. Penal Code §§ 502(c)(1), (2), (3), (6), & (7). Individuals may only be subjected to liability  
14 for acting “without permission” under Section 502 if they “access[] or us[e] a computer, computer  
15 network, or website in a manner that overcomes technical or code-based barriers.” Facebook, Inc. v.  
16 Power Ventures, Inc., No. C 08-05780-JW, 2010 WL 3291750, at \* 11 (N.D. Cal. July 20, 2010).  
17 Additionally, Section 502 creates liability for any person who “knowingly introduces any computer  
18 contaminant into any computer, computer system, or computer network.” Cal. Penal Code §  
19 502(c)(8).

20 In a recent case, this Court considered the meaning of the term “without permission” in  
21 Section 502. See Power Ventures, 2010 WL 3291750, at \*6. In Power Ventures, the Court found  
22 that the statutory language of Section 502, caselaw, and legislative intent all failed to provide clear

23

---

24 <sup>10</sup> Plaintiffs further contend that personal information itself: (1) “constitutes currency”; and  
25 (2) is a form of property. (See Opp’n at 6-11.) However, Plaintiffs offer no caselaw in support of  
26 these propositions. As another court has noted when confronted with a similar claim: “Nor has [the  
27 plaintiff] presented any authority to support the contention that unauthorized release of personal  
28 information constitutes a loss of property. Without any such authority, the Court is constrained to  
find that [the plaintiff] has not alleged any loss of property and therefore has not stated a valid claim  
under [the UCL].” Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008).

1 guidance as to how to interpret this term. Id. at \*6-10. The Court found that the statute would be  
2 unconstitutionally vague unless it was read narrowly, so as to provide adequate notice of the conduct  
3 which it criminally prohibits. Id. at \*10. The Court then held that the statute must be read to limit  
4 criminal liability to circumstances “in which a user gains access to a computer, computer network,  
5 or website to which access was restricted through technological means,” since anyone “applying the  
6 technical skill necessary to overcome such a barrier will almost always understand that any access  
7 gained through such action is unauthorized.” Id. at \*11. Applying that construction of the statute to  
8 the facts before it, the Court concluded that the defendant could only be held liable for a violation of  
9 Section 502 if the plaintiff could prove that the defendant “circumvented . . . technical barriers” that  
10 had been put in place to block defendant’s access to the plaintiff’s website. Id. at \*12.

11 Here, Plaintiffs’ allegations under those subsections of Section 502 which require a  
12 defendant to act “without permission” allege that Defendant acted “without permission” under that  
13 statute.<sup>11</sup> (Complaint ¶¶ 86-91.) However, Plaintiffs do not allege that Defendant circumvented  
14 technical barriers to gain access to a computer, computer network or website. To the contrary,  
15 Plaintiffs allege that Defendant caused “nonconsensual transmissions” of their personal information  
16 as a consequence of Defendant’s “re-design” of its own website. (Id. ¶¶ 34-36.) It is thus  
17 impossible, on Plaintiffs’ own allegations, for Defendant to be liable under the subsections of  
18

---

19 <sup>11</sup> Plaintiffs also allege a violation of Cal. Penal Code § 502(c)(8), which unlike the other  
20 sections of Cal. Penal Code § 502(c) does not require that a defendant act “without permission.”  
21 Cal. Penal Code § 502(c)(8) applies to any person who “knowingly introduces any computer  
contaminant into any computer, computer system, or computer network.” The term “computer  
contaminant” is defined as follows:

. . . any set of computer instructions that are designed to modify, damage, destroy,  
22 record, or transmit information within a computer, computer system, or computer network  
23 without the intent or permission of the owner of the information. They include, but are not  
24 limited to, a group of computer instructions commonly called viruses or worms, that are  
self-replicating or self-propagating and are designed to contaminate other computer  
25 programs or computer data, consume computer resources, modify, destroy, record, or  
transmit data, or in some other fashion usurp the normal operation of the computer, computer  
system, or computer network.

Cal. Penal Code § 502(b)(10).

26 Plaintiffs do not allege any facts suggesting that Defendant introduced computer instructions  
27 designed to “usurp the normal operation” of a computer, computer system or computer network.  
Thus, under California law Plaintiffs fail to state a claim under Cal. Penal Code § 502(c)(8).

1 Section 502 which require a defendant to act “without permission,” as there were clearly no  
2 technical barriers blocking Defendant from accessing its own website. Because Plaintiffs cannot  
3 state a claim under Section 502 for any action done “without permission” under their own  
4 allegations, the Court dismisses Plaintiffs’ claim under Cal. Penal Code §§ 502(c)(1), (2), (3), (6), &  
5 (7) with prejudice.

6 Accordingly, the Court GRANTS Defendant’s Motion to Dismiss Plaintiffs’ Cause of Action  
7 under Section 502 with prejudice as to Cal. Penal Code §§ 502(c)(1), (2), (3), (6), & (7), and without  
8 prejudice as to § 502(c)(8), with leave to amend to allege specific facts in support of their claim  
9 under § 502(c)(8), if so desired.

10 **F. CLRA**

11 At issue is whether Plaintiffs state a claim under the CLRA.

12 The CLRA provides protection to a specific category of consumers from damages suffered in  
13 connection with a consumer transaction. Robinson v. HSBC Bank USA, 732 F. Supp. 2d 976, 987  
14 (N.D. Cal. 2010). A violation of the CLRA may only be alleged by a consumer. Von Grabe v.  
15 Spring PCS, 312 F. Supp. 2d 1285, 1303 (S.D. Cal. 2003). Under the CLRA, a “consumer” is an  
16 individual who purchases or leases any goods or services for personal, family or household  
17 purposes. Schauer v. Mandarin Gems of Cal., Inc., 125 Cal. App. 4th 949, 960 (Cal. Ct. App. 2005).

18 Here, Plaintiffs allege that Defendant “allows anyone . . . to register for its services free of  
19 charge.” (Complaint ¶ 12.) As discussed previously, Plaintiffs’ contention that their personal  
20 information constitutes a form of “payment” to Defendant is unsupported by law. Since it is not  
21 possible for Plaintiffs to state a claim pursuant to the CLRA under Plaintiffs’ own allegations, the  
22 Court dismisses Plaintiffs’ CLRA claim with prejudice.

23 Accordingly, the Court GRANTS Defendants’ Motion to Dismiss Plaintiffs’ Cause of Action  
24 under the CLRA with prejudice.

25 **G. Breach of Contract**

26 At issue is whether Plaintiffs state a claim for breach of contract.  
27  
28

1 Under California law, to state a cause of action for breach of contract a plaintiff must plead:  
2 “the contract, plaintiffs’ performance (or excuse for nonperformance), defendant’s breach, and  
3 damage to plaintiff therefrom.” Gautier v. General Tel. Co., 234 Cal. App. 2d 302, 305 (Cal. Ct.  
4 App. 1965). California law requires a showing of “appreciable and actual damage” to assert a  
5 breach of contract claim. Aguilera v. Pirelli Armstrong Tire Corp., 223 F.3d 1010, 1015 (9th Cir.  
6 2000). Nominal damages and speculative harm do not suffice to show legally cognizable damage  
7 under California contract law. Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009).

8 Here, in regard to damages, Plaintiffs allege only that as a result of the alleged breach of  
9 contract, Plaintiffs “suffered injury.” (Complaint ¶ 109.) However, Plaintiffs fail to allege any  
10 actual damages in their Complaint. Thus, under California law Plaintiffs fail to state a claim for  
11 breach of contract.

12 Accordingly, the Court GRANTS Defendant’s Motion to Dismiss Plaintiffs’ Cause of Action  
13 for breach of contract, with leave to amend to allege specific facts showing appreciable and actual  
14 damages in support of their claim, if so desired.

15 **H. Cal. Civ. Code §§ 1572 and 1573**

16 At issue is whether Plaintiffs state a claim under Sections 1572 and 1573 of the California  
17 Civil Code.

18 Sections 1572 and 1573 deal with actual and constructive fraud. See Cal. Civ. Code §§  
19 1572, 1573. In California, the elements of a cause of action for fraud are: “(a) misrepresentation  
20 (false representation, concealment, or nondisclosure); (b) knowledge of falsity (or ‘scienter’); (c)  
21 intent to defraud, i.e., to induce reliance; (d) justifiable reliance; and (e) resulting damage.” Engalla  
22 v. Permanente Med. Group, 15 Cal. 4th 951, 974 (1997).

23 Here, Plaintiffs fail to allege that they relied upon any allegedly fraudulent  
24 misrepresentations by Defendant. Thus, under California law Plaintiffs fail to state a claim for fraud  
25 under either Cal. Civ. Code § 1572 or § 1573.

26  
27  
28



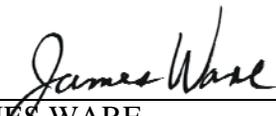
V. CONCLUSION

The Court GRANTS in part and DENIES in part Defendant's Motion to Dismiss as follows:

- (1) The Court DENIES Defendant's Motion to Dismiss on the ground that Plaintiffs lack standing under Article III;
- (2) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action under the Wiretap Act with leave to amend;
- (3) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action under the Stored Communications Act with leave to amend;
- (4) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action under the UCL with prejudice;
- (5) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action under Cal. Penal Code §§ 502(c)(1), (2), (3), (6), & (7) with prejudice, and as to § 502(c)(8) with leave to amend;
- (6) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action under the CLRA with prejudice;
- (7) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action for breach of contract with leave to amend;
- (8) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action under Cal. Civ. Code §§ 1572, 1573 with leave to amend; and
- (9) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action for unjust enrichment with prejudice.

Any Amended Complaint shall be filed on or before **June 13, 2011** and shall be consistent with the terms of this Order.

Dated: May 12, 2011

  
\_\_\_\_\_  
JAMES WARE  
United States District Chief Judge

1 **THIS IS TO CERTIFY THAT COPIES OF THIS ORDER HAVE BEEN DELIVERED TO:**

- 2 Benjamin Harris Richman brichman@edelson.com  
Charles Hyunchul Jung cjung@nassiri-jung.com  
3 Christopher Lilliard Dore cdore@edelson.com  
Donald Amamgbo damamgbo@amamgbolaw.com  
4 Eric David Freed eric@freedweiss.com  
Eric H. Gibbs ehg@girardgibbs.com  
5 Francis M. Gregorek gregorek@whafh.com  
James M. Penning jpenning@cooley.com  
6 Jay Edelson jedelson@edelson.com  
Jordan L. Lurie jlurie@weisslurie.com  
7 Kassra Powell Nassiri knassiri@nassiri-jung.com  
Matthew Dean Brown mbrown@cooley.com  
8 Matthew Joseph Zevin mzevin@stanleyiola.com  
Michael James Aschenbrener maschenbrener@edelson.com  
9 Reginald Von Terrell ReggieT2@aol.com  
Richard L. Seabolt rlseabolt@duanemorris.com  
10 Sean Patrick Reis [sreis@edelson.com](mailto:sreis@edelson.com)  
Sydney Jay Hall sydneyhalllawoffice@yahoo.com

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**Dated: May 12, 2011**

**Richard W. Wieking, Clerk**

By:           /s/ JW Chambers            
**Susan Imbriani**  
**Courtroom Deputy**