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[1] 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.[2] 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.

[1] 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.

[2] (See Defendant's Motion to Dismiss Consolidated Class Action Complaint, hereafter, "Motion," Docket Item No. 75.)

## II. BACKGROUND

In a Consolidated Class Action Complaint[3] filed on October 11, 2010, Plaintiffs allege as follows:

> Defendant is a Delaware corporation that maintains its headquarters in Santa Clara County, California. (Complaint ¶ 6.) Defendant operates the world's largest social networking website. (Id. ¶ 11.) Defendant allows anyone with access to a computer and Internet connection to register for its services free of charge. (Id. ¶ 12.) One of the few requirements Defendant places on its registrants is that they provide their actual names. (Id. ¶ 13.) Once registered, a user of Defendant's website may also post personal information to a "profile" webpage. (Id. ¶ 14.)
>
> Each user of Defendant's website has a user ID number which uniquely identifies that user. (Complaint ¶ 15.) If a person knows the user ID number or "username" of an individual who is a user of Defendant's website, that person can see the user's profile webpage and see the user's real name, gender, picture, and other information. (Id.)
>
> Defendant now "serves more ad[vertisement] impressions than any other online entity." (Complaint ¶ 18.) Because it possesses personal information about its users, Defendant's advertisers are able to target advertising to users of Defendant's website. (Id. ¶ 19.) Defendant's own policies prohibit Defendant from revealing any user's "true identity" or specific personal information to advertisers. (Id. ¶¶ 20-25.)
>
> When a user of Defendant's website clicks on an advertisement posted on the website, Defendant sends a "Referrer Header" to the corresponding advertiser. (Complaint ¶ 28.) This Referrer Header reveals the specific webpage address that the user was looking at prior to clicking on the advertisement. (Id.) Thus, Defendant has caused users' Internet browsers to send Referrer Header transmissions which report the user ID or username of the user who clicked on an advertisement, as well as information identifying the webpage the

[3] (Consolidated Class Action Complaint, hereafter, "Complaint," Docket Item No. 36.)

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

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

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

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

## III. STANDARDS

### A. Lack of Subject Matter Jurisdiction

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

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

**B. Failure to State a Claim**

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

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

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

## IV. DISCUSSION

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

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

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

**A. Injury-in-Fact**

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

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

---

[4] Plaintiffs do not distinguish between their claims under Title I of the ECPA (the Wiretap Act) and Title II of the ECPA (the Stored Communications Act). (See Plaintiffs' Opposition to Facebook's Motion to Dismiss Consolidated Class Action Complaint 11-17, hereafter, "Opp'n," 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.)

Here, Plaintiffs allege as follows:

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

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

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

---

[5] A plaintiff may satisfy the injury-in-fact requirements to have standing under Article III, 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).

[6] 439 F. Supp. 2d 974 (N.D. Cal. 2006).

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

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

**B. Wiretap Act**

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

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

Here, Plaintiffs allege as follows:

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

Based on the allegations above, the Court finds that there are two possible ways to understand Plaintiffs' allegations. On the first view, Plaintiffs allege that when a user of Defendant's website clicks on an advertisement banner displayed on that website, that click constitutes an electronic communication from the user to Defendant.[7] Under this interpretation, the content of the user's communication with Defendant is a request that Defendant "send [a further] electronic communication to [an] advertiser." On the second view, Plaintiffs allege that when a user of Defendant's website clicks on an advertisement banner, that click constitutes an electronic

[7] 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.)

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

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

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

**C. Stored Communications Act**

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

Under the Stored Communications Act, an 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." 18 U.S.C. § 2702(a)(1). However, a provider of an electronic communication service may divulge the contents of a communication to an

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

As discussed previously, Plaintiffs either allege that the communications at issue were sent to Defendant or to advertisers. Under either interpretation, Plaintiffs fail to state a claim under the Stored Communications Act. If the communications were sent to Defendant, then Defendant was their "addressee or intended recipient," and thus was permitted to divulge the communications to advertisers so long as it had its own "lawful consent" to do so.[8] 18 U.S.C. § 2702(b)(3). In the alternative, if the communications were sent to advertisers, then the advertisers were their addressees or intended recipients, and Defendant was permitted to divulge the communications to them. Id. § 2702(b)(1). Thus, because Plaintiffs cannot state a claim under the Stored Communications Act on their own allegations, the Court dismisses Plaintiffs' Stored Communications Act claim with prejudice.

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

[8] Plaintiffs do not contend that Defendant would be unable to give itself "lawful consent" to divulge Plaintiffs' communications to Defendant. In similar situations, courts have held that a defendant cannot be liable under the Stored Communications Act for disclosing communications where the defendant was itself the "addressee or intended recipient" of those communications. See, 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).

**D. UCL**

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

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

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

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

[9] 719 F. Supp. 2d 1102 (N.D. Cal. 2010).

Because Plaintiffs allege that they received Defendant's services for free, as a matter of law, Plaintiffs cannot state a UCL claim under their own allegations. Thus, the Court dismisses Plaintiffs' UCL claim with prejudice.[10]

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

**E. Cal. Penal Code § 502**

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

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

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

---

[10] Plaintiffs further contend that personal information itself: (1) "constitutes currency"; and (2) is a form of property. (See Opp'n at 6-11.) However, Plaintiffs offer no caselaw in support of these propositions. As another court has noted when confronted with a similar claim: "Nor has [the plaintiff] presented any authority to support the contention that unauthorized release of personal 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).

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

Here, Plaintiffs' allegations under those subsections of Section 502 which require a defendant to act "without permission" allege that Defendant acted "without permission" under that statute.[11] (Complaint ¶¶ 86-91.) However, Plaintiffs do not allege that Defendant circumvented technical barriers to gain access to a computer, computer network or website. To the contrary, Plaintiffs allege that Defendant caused "nonconsensual transmissions" of their personal information as a consequence of Defendant's "re-design" of its own website. (Id. ¶¶ 34-36.) It is thus impossible, on Plaintiffs' own allegations, for Defendant to be liable under the subsections of

---

[11] Plaintiffs also allege a violation of Cal. Penal Code § 502(c)(8), which unlike the other sections of Cal. Penal Code § 502(c) does not require that a defendant act "without permission." 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, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not 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 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).

Plaintiffs do not allege any facts suggesting that Defendant introduced computer instructions 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).

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

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

**F. CLRA**

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

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

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

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

**G. Breach of Contract**

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

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

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

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

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

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

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

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

Accordingly, the Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action under Cal. Civ. Code §§ 1572 and 1573, with leave to amend to allege specific facts in support of their claim, if so desired.[12]

**I. Unjust Enrichment**

At issue is whether Plaintiffs are entitled to state a claim for unjust enrichment in the alternative, given that they allege breach of an express contract.

Under California law, unjust enrichment is an action in quasi-contract. Gerlinger v. Amazon.com, Inc., 311 F. Supp. 2d 838, 856 (N.D. Cal. 2004). However, "as a matter of law, a quasi-contract action for unjust enrichment does not lie where . . . express binding agreements exist and define the parties' rights." Villager Franchise Systems, Inc. v. Dhami, Dhami & Virk, No. CVF046393RECSMS, 2006 WL 224425 (E.D. Cal. Jan. 26, 2006) (quoting Cal. Med. Ass'n v. Aetna U.S. Healthcare of Cal., 94 Cal. App. 4th 151, 172 (Cal. Ct. App. 2001)). Although Rule 8 of the Federal Rules of Civil Procedure allows a party to state multiple, even inconsistent claims, the rule does not allow a plaintiff invoking state law to assert an unjust enrichment claim while also alleging an express contract. Gerlinger, 311 F. Supp. 2d at 856.

Here, Plaintiffs allege that they assented to Defendant's "Terms and Conditions and Privacy Policy," and that the provisions of this Policy "constitute a valid and enforceable contract" between Plaintiffs and Defendant. (Complaint ¶¶ 101, 102.) Because Plaintiffs allege that an express contract existed between themselves and Defendant, they cannot also assert an unjust enrichment claim. Gerlinger, 311 F. Supp. 2d at 856. Since it is not possible to state a claim for unjust enrichment under Plaintiffs' own allegations, the Court dismisses Plaintiffs' unjust enrichment claim with prejudice.

Accordingly, the Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Cause of Action for unjust enrichment with prejudice.

---

[12] Any allegations of fraud must be pleaded with particularity. See Fed. R. Civ. P. 9(b).

## 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

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

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

**Dated: May 12, 2011**

**Richard W. Wieking, Clerk**

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

**United States District Court**
For the Northern District of California