KASSRA P. NASSIRI (215405)
(knassiri@nassiri-jung.com)
CHARLES H. JUNG (217909)
(cjung@nassiri-jung.com)
NASSIRI & JUNG LLP
47 Kearny Street, Suite 700
San Francisco, California 94108
Telephone: (415) 762-3100
Facsimile: (415) 534-3200

EDELSON MCGUIRE LLC
MICHAEL J. ASCHENBRENER
(maschenbrener@edelson.com)(*pro hac vice*)
CHRISTOPHER L. DORE
(cdore@edelson.com) (*pro hac vice*)
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370
Facsimile: (312) 589-6378

Attorneys for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: FACEBOOK PRIVACY LITIGATION

Case No. 10-cv-02389-JW

CLASS ACTION

PLAINTIFFS' OPPOSITION TO FACEBOOK'S MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT

ACTION FILED: 05/28/10

Date: March 28, 2011
Time: 9:00 a.m.
Judge: Hon. James Ware

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES

UNITED STATES COURT OF APPEALS CASES

UNITED STATES DISTRICT COURT CASES

STATE COURT CASES

FEDERAL STATUTES, RULES AND REGULATIONS

CALIFORNIA STATE STATUTES

AGENCY STATEMENTS AND LEGISLATIVE HISTORY

OTHER SOURCES

I. Introduction

For every wrong there is a remedy. Cal. Civ. Code § 3523. This maxim is as true and applicable in today's evolving Internet markets as it was when villagers paid for clay pots with livestock, when fortune-seekers paid for lumber with gold bricks, or when post-war suburbanites paid for television sets with cash. Here, Plaintiffs paid for Facebook access with their valuable personal information, which may be evolutionary, but it is not novel.

In this case, the wrong to be remedied is simple: Facebook revealed specific information about specific Facebook users to advertisers in violation of Facebook's contracts with the affected users and in violation of state and federal laws. What makes this wrong legally redressable is that the information revealed was specifically bargained for: Facebook promised to safeguard this information and provide access to Facebook in exchange for the information itself. In other words, Plaintiffs used this information as currency to obtain access to Facebook. Notably, Defendant does not even contest the validity of these contracts.

While this wrong—the wrong of misusing personal information that consumers exchange for online products—appears to have sprung newly out of Silicon Valley's blooming information economy, there is nothing new about exchanging currency—whatever its form, be it livestock, gold bricks, dollar bills, or information—for goods and services, which is exactly what Plaintiffs allege they did in this case.

Plaintiffs have alleged Defendant committed many wrongs at their expense. Fortunately for Plaintiffs, for every wrong there is a remedy.

II. Statement of Facts[1]

Facebook is the world's largest social networking website, with over 500 million registered users worldwide. (Consolidated Complaint ("Compl.") ¶ 11.) Facebook requires its registrants to provide their actual names in order to establish a profile and use the site. (*Id.* ¶ 13.) In addition to a username, each Facebook user has a unique user ID that is tied to that user's Facebook profile. (*Id.* ¶ 15.) Once registered, Facebook users share an unprecedented amount of personal information with Facebook, including birth date, place of birth, current and past addresses, present and past employment information, relationship status, personal pictures, and more. (*Id.* ¶ 14, 16.)

Facebook generates substantial revenues through its online advertising platform. (*Id.* ¶¶ 105, 107.) Facebook's advertising platform is particularly attractive to advertisers because Facebook has access to highly-personal information about its users. (*Id.*) If not for the inherent and identifiable value of personal consumer information, Facebook would be much less

---

[1] In its Introduction, Facebook repeatedly and improperly contradicts and blatantly mischaracterizes the well-pled factual allegations in Plaintiffs' Complaint. For example, Facebook improperly asserts that:

- "User IDs or Usernames were transmitted by Users' third-party web browsers—not by Facebook—to advertisers when Users clicked on advertisements." (Defendant's Motion to Dismiss ("MTD") at 2:12-13)
- "transmission of Internet addresses or 'URLs' that purportedly contained User IDs or Usernames to advertisers results from the standard operation of Users' web browsers (whether someone is using Facebook or any other website)." (MTD at 2:18-21)
- "when a Facebook User clicked on an advertisement on Facebook, the User's browser may have transmitted the Internet address of the site that the User was viewing on Facebook, which may or may not have contained the User's numerical User ID or Username." (MTD at 2:25-28)
- "Usernames were transmitted to advertisers by…a 'standard web browser function' effected Users' third-party we browsers—not Facebook" (MTD at 4:6-8)
- the User ID associated with a User's profile on Facebook may have been contained in the technical Internet address (the "URL") for a User's profile page on Facebook (e.g., http://www.facebook.com/profile.php?id=123456789), to allow Facebook to display the correct information on that page.") (citing Consolidated Class Action Compl. ¶ 33) (emphasis added) (internal citation omitted)

Nowhere do Plaintiffs state that Web browsers are responsible for the transmissions at issue. To the contrary, the Complaint makes clear that *Facebook*—not a third-party web browser—*caused the disclosing transmissions*. (Compl. ¶¶ 28, 31, 43.) Accordingly, the Court should disregard Facebook's contradictions and mischaracterizations of the factual assertions in the Complaint.

profitable. (*Id.* ¶¶ 57, 66, 86, 105-107, 114.)

Because personal information is so valuable to Facebook, Defendant places a high priority on instilling trust with its users. In a published statement, Facebook's CEO stated that the "trust [Facebook users] place in us as a safe place to share information is ***the most important part of what makes Facebook work***." (*Id.* ¶ 24) (emphasis added.) Facebook's Privacy Policy prohibits Facebook from sharing personal information with advertisers without user consent, including the user's identity. (*Id.* ¶ 20) ("We don't share your information with advertisers without your consent . . . we do not tell [advertisers] who you are…") Facebook makes similar representations in its Privacy Guide ("We never share your personal information with our advertisers") and in its Statement of Rights and Responsibilities ("We do not give your content or information to advertisers without your consent."). (*Id.* ¶¶ 21-22.) And in a published statement, Facebook's Director of Corporate Communications and Public Policy stated that "we never provide the advertiser any names or other information about the people who are shown, or even who click on, the ads." (*Id.* ¶ 23.)

But Facebook's privacy representations were false. Through deliberate design, Facebook intentionally caused users' browsers to transmit personal information, including the identity of Facebook users, to advertisers when those users clicked on ads. (*Id.* ¶¶ 28, 31, 43.) It wasn't until the *Wall Street Journal* exposed Facebook's practices that Facebook finally re-designed its website and ceased the nonconsensual transmission of users' personal information to advertisers. (*Id.* ¶ 33.)

III. Legal Standard

In reviewing a motion to dismiss, the court "accept[s] all well-pleaded factual allegations in the complaint as true, and determines whether the factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Cassirer v. Kingdom of Spain*, 580 F.3d 1048, 1052 (9th Cir. 2009) (internal citations omitted). A motion to dismiss must be denied if the complaint contains factual allegations that, when accepted as true, "plausibly give rise to an entitlement to relief." *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1941 (2009). Moreover, Fed. R. Civ. P. 8(a) requires a plain and short statement of a plaintiff's claim, a standard that "contains a powerful

presumption against rejecting pleadings for failure to state a claim." *Ileto v. Glock Inc.*, 349 F.3d 1191, 1199 (9th Cir. 2003).

As shown below, the Complaint puts Facebook on notice of the claims it must defend, and amply alleges facts that, taken as true, plausibly allow the Court "to draw the reasonable inference that [Facebook] is liable for the misconduct alleged." *Ashcroft*, 129 S. Ct. at 1940.

IV. Argument

A. Plaintiffs Have Article III Standing

1. Facebook's Invasion of Plaintiffs' Statutory Rights Creates Standing.

The United States Supreme Court has held that the "injury required by Article III may exist *solely* by virtue of statutes creating legal rights, the invasion of which creates standing . . ." *Warth v. Seldin*, 422 U.S. 490, 500 (1975).[2] Where a statute creates a private right of action, even a plaintiff who cannot establish actual damages has Article III standing. *See Edwards v. First American Corp.*, 610 F.3d 514, 517 (9th Cir. 2010) (because Real Estate Settlement Procedures Act of 1974 created a private right of action, plaintiff had standing even though no actual damages were alleged); *Sisley v. Sprint Communications Co.,* 284 Fed. Appx. 463, 466 (9th Cir. 2008) (reversing district court's dismissal of state statutory claim "for lack of a cognizable injury," because "[the plaintiff] alleged a violation of her state statutory rights which can constitute a cognizable injury sufficient to withstand a Rule 12(b)(1) motion"); *Hoang v. Reunion.com, Inc.*, No. C-08-3518 MMC, 2010 WL 1340535, *3-4 (N.D. Cal. Mar. 31, 2010) (finding standing under state consumer protection statute even though plaintiff could not allege actual injury).

Plaintiffs allege that from at least February 2010 through May 21, 2010, Facebook systematically disclosed users' identities and the URL of the web page the users were viewing when the users clicked on advertisements. (Compl. ¶¶ 31-33). Plaintiffs, who each clicked on an advertisement during the relevant time period (*Id.* ¶¶ 4-5), allege that Facebook disclosed their

---

[2] Internal quotation omitted and emphasis added.

personal information and thereby violated their statutory rights under § 2511(3)(a) of the Electronic Communications Privacy Act ("ECPA") and §§ 2702(a)(1) and 2702(a)(2) of the Stored Communications Act ("SCA") (Compl. ¶¶ 57, 65, 70).[3] Because § 2520 of the ECPA and § 2707 of the SCA create private rights of action for the alleged violations, Plaintiffs have Article III standing irrespective of whether they can establish actual damages.[4]

What's more, Plaintiffs have sufficiently established concrete injury traceable to Facebook's statutory violations. In *Hepting v. AT&T Corp.*, the plaintiffs brought claims under the same provisions of the SCA at issue here. 439 F. Supp. 2d 974 (N.D. Cal. 2006). Like Facebook, defendant AT&T claimed that the plaintiffs failed to allege injury-in-fact and lacked standing, arguing "all plaintiffs really have is a suggestion that AT&T provided a means by which the government *could have* [monitored their communications] had it wished." *Id.* at 999. Then Chief Judge Vaughn R. Walker disagreed, holding that "at the pleading stage, general factual allegations of injury resulting from defendant's conduct may suffice, for on a motion to dismiss we 'presume that general allegations embrace those specific facts that are necessary to support the claim.'" *Id.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). Judge Walker went on to rule that not only had the plaintiffs sufficiently alleged injury-in-fact, but that they also established concrete injury. The *Hepting* plaintiffs alleged that AT&T had violated the SCA by assembling a database of the contents of customer communications and enabling the government to search the database. Judge Walker held that defendant AT&T's "alleged creation of a dragnet to intercept all or substantially all of its customers' communications…necessarily inflict[ed] a concrete injury" on each of its customers. *Id.* at 1000-01.

Like the *Hepting* plaintiffs, Plaintiffs here have alleged that Facebook disclosed the contents

---

[3] *See* section IV(B), *infra*, arguing that Plaintiffs have stated a claim under both the ECPA and SCA.

[4] As the Supreme Court noted, "[f]or purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing courts must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party . . . standing in no way depends on the merits of the plaintiff's contention that the particular conduct is illegal." *Warth*, 422 U.S. at 500, 502.

of Plaintiffs' communications to third parties in violation of the ECPA and SCA. Accordingly, Plaintiffs have established concrete, particularized injury.

2. Plaintiffs Have Suffered Injuries in Fact and Incurred Appreciable Damages.

Plaintiffs' allegations demonstrate that they have suffered injury in fact sufficient to confer standing for Plaintiffs' remaining state law claims. Facebook's standing argument rests on three primary inaccurate premises: that Plaintiffs have failed to allege that they have lost money or property; that Plaintiffs have failed to allege that their PII was disclosed to third-parties in a way that caused loss of money or property; and that Plaintiffs have failed to allege that they paid Facebook in any way. All three premises are demonstrably false.

a. Personal Information Constitutes Currency.

"Data is currency," according to then-FTC Commissioner Pamela Jones Harbour. *FTC Roundtable Series 1 on Exploring Privacy* (Matter No. P095416), Dec. 7, 2009, p. 147.[5] "In many instances, consumers pay for free content and services by disclosing their personal information." (*Id*. at 148.)

Commissioner Jones is not alone in her assessment that personal data is currency. In *Property, Privacy, and Personal Data*, Berkeley School of Law Professor Paul M. Schwartz wrote:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).[6]

Commissioner Jones Harbour and Professor Schwartz may as well have been speaking specifically

---

[5] Available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf (last accessed January 28, 2011).

[6] Even the SEC has demonstrated its belief that personal information constitutes a form of currency and can form the basis of a sale of stock. 1999 WL 38281 (S.E.C. No-Action letter, Jan. 27, 1999); *See also* Jason Hubschman, *Note: The "Odd Duck Filing" and the Efficient Market Theory: Meeting SEC Registration Requirements for Internet Free Stock Programs*, N.Y. LAW SCHOOL LAW REVIEW, Vol. 44, p. 566 (2001).

about Facebook's business model, as Facebook consumers pay for "free" products by disclosing their personal information. (Compl. ¶ 104). Like many internet companies today, Facebook uses personal information to offer a particularly attractive advertising platform that can deliver highly-targeted ads to Facebook users. (*Id.* ¶ 105.) And Facebook has been wildly successful in parlaying its users' personal information into a multi-billion dollar valuation. (*Id.* ¶ 107.) It is the value of this user personal information for advertising that powers the economy of the "free" Internet, and specifically, Facebook's business. (Compl. ¶¶ 17, 104-107).

Even Microsoft Corp. explicitly supports this view that personal information is currency. In formal, written comments to the FTC, Microsoft stated that advertising is the engine driving the Internet economy, allowing web companies to offer their content and services without charging fees to consumers. *Protecting Consumer Privacy in an Era of Rapid Change,* Preliminary FTC Staff Report, Dec. 1, 2010, pp. 33-34, n. 89-90.[7] In its report, the FTC also notes that "the more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him. Not surprisingly, in recent years, there has been a dramatic increase in the number of companies whose business depends on the collection of increasingly detailed information about consumers." (*Id*. at 37.)

As alleged, personal user information is the very driver of Facebook's business and revenue—personal information is the currency Plaintiffs and the putative class members exchange for Facebook's products. (Compl. ¶¶ 13, 16, 104-107.) Accordingly, Plaintiffs' personal information has value and constitutes currency for purposes of consumer transactions with Facebook and for purposes of standing.

b. Plaintiffs' Personal Information Is Their Property.

Not only does personal user information constitute currency, but it also constitutes Plaintiffs' property. Facebook admits as much in its own Statement of Rights and Responsibilities (attached to Defendant's Motion to Dismiss as Exh. A). Facebook informs users that "You *own* all of the content

[7]Available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last accessed Jan. 28, 2011).

and information that you post on Facebook, and you can control how it is shared through your privacy and application settings." (*See* MTD at Exh. A, Para. 2; emphasis added). In turn, "Information" is defined as "facts and other information about you, *including actions you take*," and "post" is defined as "post on Facebook *or otherwise make available to us* (such as by using an application)." (*See* MTD at Exh. A, Para 17; emphasis added). Of course, few "facts" about a Facebook user are more basic than the user's identity and other PII provided to Facebook. Facebook users "post" the personal information that Facebook discloses to advertisers when they first sign up for Facebook and when they create their own unique username. Thus, by Facebook's own admission, Plaintiffs own the information that Defendant wrongfully disclosed to Facebook advertisers. This issue goes to the heart of the issue of the harm suffered by Plaintiff, which is the first element of standing. *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1125-26 (N.D. Cal. 2008) ("*Ruiz I*").

Typically, plaintiffs in lost data cases have attempted to argue that the harm suffered is that of the speculative increased risk of possible identity theft. *E.g.*, *Id.* at 1125. Whatever the shortfalls of that argument, it is not Plaintiffs' argument. Rather, Plaintiffs allege that they have already suffered injuries in fact because of Facebook's unauthorized disclosure of their personal information, which is their personal property. (Compl. ¶¶ 104-107.) In other words, Plaintiffs allege that they have suffered real damages now. (*Id*.)

(i) Plaintiff's harm is concrete and particularized.

In *Ruiz I*, the Court found (for purposes of Cal. Bus. & Prof. Code § 17200) that the plaintiff had not lost money or property because he provided no "authority to support the contention that unauthorized release of personal information constitutes a loss of property." 540 F. Supp. 2d at 1127. Plaintiffs in the instant matter have the authority that the plaintiff in *Ruiz I* lacked.

In *Doe 1 v AOL LLC*, 719 F. Supp. 2d 1102, 1113-14 (N.D. Cal. 2010), Judge Armstrong denied a motion for judgment on the pleadings with respect to CLRA and UCL claims (among others) for the disclosure of users' personal information. The court found that the plaintiffs suffered

injury resulting from AOL's disclosure of confidential member information. *Id.* at 1111. The court's reasons in *AOL* included:

- AOL represented that, as a matter of company policy, user PII would be safeguarded (*Id.* at 1111);
- AOL violated its representations regarding the privacy of member data (*Id.*);
- The published data included user names (*Id.*);
- Users did not bargain for AOL's collection and disclosure of user PII (*Id.*).

Similarly, in this case:

- Facebook represented that, as a matter of company policy, user PII would be safeguarded (Compl. ¶¶ 20-26);
- Facebook violated its representations regarding the security of customer PII (Compl. ¶¶ 27-30);
- The published data included user names (Compl. ¶ 28);
- Users did not bargain for Facebook's PII disclosures (Compl. ¶¶ 26-27).

And while AOL users paid for AOL's services with U.S. currency, Plaintiffs have alleged that they were required to offer valuable consideration in the form of personal information, which Plaintiffs have demonstrated equates to money or property. (Compl. ¶¶ 104, 106). In effect, *AOL* and the instant matter are functionally identical, and this Court should find that Plaintiffs have standing, just as the court found in *AOL*.

Thus, *AOL* provides the authority that the court in *Ruiz I* lacked to find that lost data constitutes loss of property.

(ii) Loss of PII is an actual harm, not a conjectural or hypothetical harm.

This value, and by extension, harm, is not theoretical either—PII has a market-definable actual value, just like baseball cards or used cars. For used cars, the tools for determining market value are car dealers, eBay, and Kelley Blue Book. In much the same way, the market for PII—both legitimate and illegitimate—defines the value of Plaintiff's user data.

There are existing and active markets that define values for a wide range of personal information. For example, full social networking credentials can be worth between $1 and $35. Thorsten Holz, *et al*., *Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones*, University of Mannheim, Laboratory for Dependable Systems (2008) ("[E]ach credential is a marketable good that can be sold in dedicated forums.").

"Personal information is now a valuable commodity, with readily available market prices—a consumer's address can be purchased for 50 cents, an unpublished number for $17.50, a Social Security number for a mere $8." Luis Salazar, *Privacy and Bankruptcy Law Part I: Technology Explosion Creates Personal Privacy Tensions*, Am. Bankr. Inst. J., Nov. 2006 at 18; *see also* John T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *1, 14 (2009), http://law.richmond.edu/jolt/v15i4/article11.pdf) ("PII is now a commodity that companies trade and sell. . . . PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets . . . . Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2402 (1996) ("[P]articularized information is a commodity that can be sold in a well developed market. . . . Therefore, the typical transaction between a merchant or seller and a consumer increasingly can be characterized as an exchange of goods or services for money *and information*.") (emphasis in original).

The idea that markets exist to buy and sell personal data is not novel. For example, in 2000, the FTC intervened in the bankruptcy of Toysmart.com in an effort to prevent it from selling a database full of consumers' personal information as part of liquidation. Toysmart had listed the consumer list as an "asset" and was fielding offers as high as $50,000. *FTC v. Toysmart.com LLC*,

2000 WL 34016434 (00-11341-RGS) (July 21, 2000).[8]

Accordingly, Plaintiff's PII has actual value as defined by the market, and the loss of it constitutes actual harm if for no other reason than Plaintiffs should be the ones profiting from the distribution of their personal data. (Compl. ¶ 106.) Plaintiffs did not provide consent for Facebook to reveal their valuable PII. (Compl. ¶¶ 26-27.) Therefore, Plaintiffs have lost the right to provide that data to entities in exchange for goods and services, because these entities have received the information from Facebook, thus depriving Plaintiffs of the chance to sell it to these entities. That is how Plaintiffs have lost money or property—Facebook has deprived them of the right to bargain with their own personal data, which Plaintiffs have shown is of real, demonstrable value.

Defendant's attempts to misconstrue Plaintiff's allegations as speculative harm are baseless. While the plaintiff in *Ruiz I* and other lost data may not have pled concrete and actual harm, Plaintiffs here have done so throughout their Complaint. Accordingly, Plaintiffs have demonstrated Article III standing as required.

B. Facebook Violated Both the Wiretap Act and the Stored Communications Act.

Facebook argues that Plaintiffs have failed to state a claim under the ECPA on the following grounds: (1) failure to allege disclosure of the contents of any communication, (2) failure to overcome the "addressee or intended recipient" exception to liability, and (3) failure to overcome the exception for disclosure of information "readily accessible to the general public." (Opp. at 10.) Because Facebook's central premise—that the communications at issue are between Plaintiffs and advertisers—is incorrect, Facebook's arguments are inapposite.

1. Facebook Disclosed the Contents of Communications Between Facebook and Plaintiffs.

Facebook argues that the alleged disclosure of User IDs and Usernames is not enough to state a claim because "a User ID or Username does not constitute the 'contents' of a communication, but

---

[8] *See also Judge Shelves Plan for Sale of Online Customer Database*, http://www.nytimes.com/2000/08/18/business/judge-shelves-plan-for-sale-of-online-customer-database.html, Aug. 18, 2000 (last accessed, January 12, 2011).

instead constitutes, at most, a User 'record,' which is governed by separate statutory provisions that do not prohibit disclosure." (Opp. at 10.) Facebook argues that "[u]nder the express provisions of § 2702(c)(6), Facebook may disclose such records to any person other than a governmental entity, including a third-party advertiser. (*Id.* at 12.) Facebook's arguments are based on the erroneous premise that a User's identity can never constitute the contents of a communication, even when combined and disclosed with other information. Facebook also utterly fails to address Facebook's disclosure of the contents of *communications between Facebook and Plaintiffs*.

Plaintiffs allege that when a Facebook User clicks on an ad, the User is "*asking Facebook* to send an electronic communication to the advertiser." (Opp at 12; Compl. ¶ 56 (emphasis added).) The act of "asking Facebook" to send an electronic communication to an advertiser is itself an electronic communication under the ECPA.[9] As Facebook must concede, the transfer of data between the user and Facebook is an electronic communication covered by the statute.

Plaintiffs allege that the contents of the communication that Facebook caused to be disclosed consisted of two distinct pieces of information: the referring URL (which reveals the Facebook page that the user was viewing when he or she clicked on an ad), and the Username or User ID uniquely identifying the user. (Compl. ¶ 31.) By causing these two pieces of information to be sent to the advertiser along with the user's request for the advertiser's landing page, Facebook disclosed much more than a mere customer record.

The ECPA's customer records exception is logically premised on the assumption that, in many situations, bare customer records are considered benign. To be sure, the disclosure of a list of Facebook members, with nothing more, may plausibly qualify for the customer records exception. But Plaintiffs do not allege that Facebook violated the ECPA simply because it revealed to third parties that Plaintiffs were in fact members of Facebook. Rather, Plaintiffs allege that Facebook

---

[9] 18 U.S.C. § 2510(12) ("'electronic communication'" means any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce"). Facebook argues in passing that referrer headers cannot constitute a communication. (Opp. at 10.) Not only is Facebook's position unsupported with case law, it is inconsistent with the ECPA's broad definition of an "electronic communication."

systematically disclosed User IDs and Usernames *with* other information that stripped Plaintiffs' and other users' identifying information of any innocuous qualities. (Compl. ¶¶ 31-33, 57, 66.) Said differently, Plaintiffs allege that Facebook disclosed to advertisers that a *particular user*, who was viewing a *particular Facebook page*, clicked on a *particular advertisement.* Facebook's disclosure reveals content, not just a customer record. (*Id.*)

Facebook argues that because a communication includes one piece of information (i.e., user identity) that alone could constitute a bare customer record, the entire communication should be construed as a customer record and hence exempt from the ECPA. However, if this argument were correct, Facebook could, for example, publish a list containing the names of every Facebook user who ever clicked an advertisement related to treatment for sexual dysfunction without ECPA liability just because the disclosure includes a customer record. The association of a particular user with his or her intentions, interests or preferences reveals content, and the customer records exemption gives no protection to such a disclosure. In this context, the identity of the User is not simply a customer record, but is instead part of the substance, purport or meaning of the User's communications with Facebook[10] and cannot be disclosed without consent from the User.[11]

What's more, the statutory "customer records" exception Facebook relies on explicitly carves out the type of content at issue here:

> Exceptions for Disclosure of Customer Records.— A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service *(not including the contents of communications covered by subsection (a)(1) or (a)(2))*—
>
> . . .
>
> (6) to any person other than a governmental entity.

---

[10] 18 U.S.C. § 2510(8) ("'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication").

[11] Plaintiffs also allege that Facebook disclosed the Facebook page Plaintiffs were viewing when they clicked an ad. (Compl. ¶ 31.) Because Facebook does not and cannot argue that this information falls within the customer record exception to liability, Plaintiffs have stated a claim under the ECPA.

(18 U.S.C. § 2702(c)(6) (emphasis added))

Plaintiffs allege that by deliberate design, Facebook causes the User's browser to transmit a referrer header to the advertiser disclosing the identity of the User. (Compl. ¶ 28.) This disclosure to advertisers of the contents of the immediately-preceding communication between the User and Facebook, without the User's consent, is a violation of the ECPA. And Facebook itself believes that Users' rights to keep information private and prevent non-consensual disclosures is an essential element of trust that makes Facebook work. In its Privacy Policy (*Id.* ¶ 20), Privacy Guide (*Id.* ¶ 21), Statement of Rights and Responsibilities (*Id.* ¶ 22), and Facebook Blog (*Id.* ¶ 23), Facebook represents to Users that it will safeguard and never disclose their identities to advertisers.

The three district court cases cited by Facebook in support of its attempt to characterize User identities as customer records are distinguishable and inapposite. Each case involved disclosure of bare customer account information pursuant to subpoenas. And none of the cited cases involved the disclosure of the content of communications.

In *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105 (E.D. Mich. 1998), the victim of an injurious message posted on the Internet served a civil subpoena on America Online ("AOL") to learn the identity of the message's author. AOL complied with the subpoena by providing "a two-page summary containing the basic identity information on the AOL account from which the [injurious] message originated. The summary revealed that [the plaintiff, Jessup] was the holder of the account." (*Id.* at 1107.) The plaintiff sued AOL, claiming a violation of the ECPA, and the district court found that the ECPA did not apply. But unlike the present case, the *Jessup* case did not involve any allegations that the contents of communications were disclosed. Facebook, unlike AOL, did not merely reveal basic identity information about Plaintiffs' accounts. Instead, Facebook revealed the fact that Plaintiffs sent a communication to Facebook requesting to be taken to a particular advertiser website. Moreover, the *Jessup* court noted that AOL's terms of service explicitly gave AOL the right to respond to "legal process served on AOL" and "disclose to private persons information that identifies a Member's AOL screen name(s) with the Member's actual name or other identity information." (*Id.* at 1108.) Here, in contrast, Facebook's terms of service not only

do *not* give Facebook the right to make such disclosures, but affirmatively promise that Facebook will never do so without consent.

Similarly, in *Freedman v. America Online, Inc.*, 325 F. Supp. 2d 638 (E.D. Va. 2004), the plaintiff had agreed to AOL's terms of service that explicitly gave AOL the right to disclose "a subscriber's telephone numbers, credit information, or screen names . . . in response to '*valid* legal process such as a search warrant, subpoena or court order....'" (*Id.* at 640.) In response to an *invalid* law enforcement subpoena, AOL disclosed basic account information about the plaintiff. The issue before the district court—wholly distinct from the issues presented in this case—was whether AOL knowingly or intentionally violated the statute by making the disclosures. And unlike the present case, there were no allegations in *Freedman* that AOL disclosed any part of a communication.

Finally, in *U.S. v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000), the issue before the district court concerned an invalid law enforcement subpoena and whether information obtained therefrom could be suppressed. And again, no part of any customer communications were disclosed in response to the subpoena.

In contrast, Facebook's repeated disclosures of personal user information were not prompted by a subpoena or other legal authority and were in direct contravention of Facebook's own policies. None of the cases Facebook relies on supports the proposition that a User's identity can never constitute the content of a communication. User IDs or Usernames, disclosed in combination with a referrer URL and sent along with a request for the advertiser's landing URL, reveal content and are not mere customer records subject to exclusion under the ECPA. By disclosing this content to advertisers, Facebook violated the ECPA.

2. Plaintiffs Did Not Intend for Advertisers to Receive their User Names or Web Pages They Were Viewing.

Facebook erroneously argues that "by Plaintiffs' own admission, the advertiser is the 'addressee' or 'intended recipient' of [the Referrer Header transmission containing Plaintiff's identities]." (Opp at 12-13.) But as argued above, the communication with advertisers is not the

disclosed communication, it is the *disclosing* communication. Facebook overlooks this critical distinction entirely.

Plaintiffs allege as follows:

> By clicking an advertisement banner displayed on Facebook.com, ***users are asking Facebook*** to send an electronic communication to the advertiser who supplied the ad. But pursuant to Facebook's Terms and Conditions and its Privacy Policy, users do not expect and do not consent to Facebook's disclosure of all contents of [the user's request to Facebook]. Facebook users expect that certain aspects of their communications concerning advertisers—namely, their identities and what Facebook page they were viewing at the time they clicked an ad—will be configured by Facebook to be private.

(Compl. ¶ 56; emphasis added.)

Plaintiffs do not allege that they intended for advertisers to be privy to Plaintiffs' communications with Facebook, but instead allege the opposite. Accordingly, Facebook may not assert the "addressee or intended recipient" exception to liability under the ECPA.

3. Plaintiffs' Preferences and Web Browsing Activities Are Not Readily Accessible to the General Public.

Finally, Facebook argues that because Users' profiles are configured to be "readily accessible to the general public," Facebook is not liable under the ECPA. (Opp. at 13.) Once again, Facebook misconstrues Plaintiffs' allegations.

As set forth above, Plaintiffs allege that Facebook improperly disclosed User *identities* to advertisers together with referral and destination URLs, not that Facebook disclosed information voluntarily published on User *profiles* to advertisers.[12] Facebook simply cannot argue that the specific identities of Users who clicked on specific ads, as well as the page that the User was viewing when he or she clicked on the ad, were readily accessible to the general public. Indeed, Plaintiffs allege that once news outlets exposed Facebook's improper disclosures, Facebook immediately ceased those disclosures. (Compl. ¶ 33.) Plaintiffs' allegations necessarily imply that

[12] Plaintiffs' general privacy concerns are heightened because advertisers may employ Usernames to navigate to an individual User's profile page to learn additional information about that User. However, this is not the crux of Plaintiffs' claims.

once Facebook discontinued its unlawful practice, the identities of Facebook Users who click on ads were no longer readily accessible to advertisers, much less the public.

C. Plaintiffs Have Properly Stated a Claim Under the UCL.

1. Plaintiffs have standing because they have alleged both injury in fact and loss of money or property.

As demonstrated above, Plaintiffs have standing under the UCL because they have alleged injury in fact and the loss of both money and property as a result of Facebook's unlawful conduct.

2. Plaintiffs have alleged that Facebook acted "Unlawfully" under the UCL.

"Violations of federal as well as state and local law may serve as the predicate for an unlawful practice claim under section 17200." *Munson v. Del Taco, Inc.*, 46 Cal. 4th 661, 676 (2009). As demonstrated throughout this Opposition, Plaintiffs have sufficiently pled statutory causes of action under the ECPA (Section IV(B)), the UCL (Section IV(C)), the CLRA (Section IV(E)), and the California Computer Crime Law (Section IV(D)), as well as common law claims for breach of contract (Section IV(F)), or in the alternative, unjust enrichment (Section IV(G)). Accordingly, Plaintiff's UCL claim should stand under the "Unlawful" prong of the UCL.

3. Plaintiffs have alleged that Facebook acted "Fraudulently" under the UCL.

Plaintiffs have alleged specific, particularized facts sufficient to state a claim under the "Fraudulent" prong of the UCL. A complaint satisfies the particularity requirements of Rule 9(b) if it alleges "the who, what, when, where, and how" of the alleged fraudulent conduct," and "set[s] forth an explanation as to why [a] statement or omission complained of was false and misleading." *AOL*, 719 F. Supp. 2d at 1112 (internal citations omitted). The purpose of Rule 9(b) "is to ensure that defendants accused of the conduct specified have adequate notice of what they are alleged to have done, so that they may defend against the accusations." *Concha v. London*, 62 F.3d 1493, 1502 (9th Cir. 1995). Plaintiffs' allegations readily meet this standard. Plaintiffs identify specific statements from Facebook published within its Statement of Rights and Responsibilities, its Privacy Guide, and several posts to its official corporate blog, in each instance representing that Facebook would not share identifying information with advertisers without users' express consent. (Compl.

¶¶ 20-24). Plaintiffs have specifically alleged that Defendant's representations were false and misleading because Facebook caused referrer headers containing Usernames, User IDs, and other sensitive PII to be sent to third-party advertisers. (Compl. ¶¶ 28-33). These allegations are more than sufficient to put Facebook "on notice" of the precise statements and conduct that Plaintiffs have alleged to be fraudulent.

Finally, Plaintiffs have sufficiently alleged reliance on Facebook's misrepresentations. Reliance is proven by showing that a misrepresentation "was an immediate cause of [plaintiff's] injury-producing conduct," though "the plaintiff need not demonstrate that it was the only cause." *In re Tobacco II Cases*, 46 Cal. 4th 298, 327 (2009). "It is not necessary that the plaintiff's reliance upon the truth of the fraudulent misrepresentation be the sole or even the predominant or decisive factor influencing his conduct." *Id.* Rather, it is sufficient to show that the misrepresentation played a "substantial part," meaning that Plaintiffs "in all reasonable probability would not have engaged in the injury producing conduct" but for the misrepresentation." *Hale v. Sharp Healthcare*, 183 Cal. App. 4th 1373, 1386-87 (2010).

In the class action context, "when the same material misrepresentations have actually been communicated to each member of a class, an inference of reliance arises as to the entire class." *Mirkin v. Wasserman*, 5 Cal. 4th 1082, 1095 (1993); *Jenson v. Fiserve Trust Co.*, 256 Fed. Appx. 924, 926 (9th Cir. 2007) (same). More generally, "a presumption, or at least an inference, of reliance arises wherever there is a showing that a misrepresentation was material." *In re Tobacco II Cases*, 46 Cal. 4th 298, 327 (2009). In turn, a misrepresentation is "material" if "a reasonable man would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question." *Id.* Typically, materiality is a question of fact. *Id.*

Plaintiffs have alleged that Facebook made repeated, public misrepresentations that Facebook would not share users' identities with third-party advertisers without the user's consent. (Compl. ¶¶ 20-24, 81). These public misrepresentations created an expectation among Plaintiffs and other users that Facebook would comply with its own policies and keep Plaintiffs' personal information private and secure. (Compl. ¶ 81). Because Facebook requires users to agree to and

abide by its Terms and Conditions and Privacy Policy, Facebook's misrepresentations were uniform and communicated to each proposed member of the Class, thereby creating an inference of reliance. At a minimum, it is clear that Facebook's policies relating to the dissemination of personal information would be a material consideration to potential users in determining whether to provide sensitive personal information in exchange for Facebook's services. Reasonable consumers such as Plaintiffs would have had serious reservations about sharing personal information with Facebook if they were aware that Facebook, contrary to its numerous public statements, routinely shared Usernames, User IDs, and User actions (i.e., which ads they clicked on) with third parties. For these additional reasons, Plaintiffs' allegations give rise to a presumption of reliance and state a claim under the "Fraudulent" prong of the UCL.

4. Plaintiffs have alleged that Facebook acted "Unfairly" under the UCL.

Plaintiffs have asserted sufficient facts to state a claim under the "Unfairness" prong of the UCL. In the context of the UCL, a business practice is "unfair" if the following factors are present: (1) substantial consumer injury; (2) the injury is not outweighed by any countervailing benefits to consumers or competition; and (3) the injury could not have been reasonably avoided by the consumer. *Camacho v. Auto Club of So. Cal.*, 142 Cal. App. 4th 1394, 1403 (2006).

Plaintiffs' allegations satisfy each element and establish that Facebook's practices were "Unfair" as defined by the UCL.[13] As discussed at length above, Plaintiffs have alleged how Facebook's disclosures of personal information have caused them concrete injury. Plaintiffs have not alleged—and Facebook has failed to identify—any countervailing benefit that flows from the provision of Usernames or User IDs to advertisers. Finally, Plaintiffs' allegations demonstrate that they could not have reasonably avoided their injuries, especially considering Facebook's repeated

---

[13] Defendant argues that Plaintiffs must plead their UCL "unfairness" claim with particularity under Rule 9(b). However, "where fraud is not an essential element of the claim, only allegations ('averments') of fraudulent conduct must satisfy the heightened pleading requirements of Rule 9(b)." *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1126 (9th Cir. 2009). However, because Plaintiffs' relevant allegations are sufficient even under the stricter pleading standards of Rule 9(b), Plaintiffs do not here attempt to distinguish between particularized factual allegations that do and do not sound in fraud.

representations that it was not sharing sensitive personal information with advertisers without its users' consent. As a result, Plaintiffs have properly pled a UCL "unfairness" claim.

D. Plaintiffs Have Stated a Claim Under Cal. Penal Code § 502.

In enacting Cal. Penal Code § 502, the express intent of the California legislature was to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer system" caused by the proliferation of unauthorized access to computers and computer data. Cal. Penal Code § 502(a). Because they seek protection from the unauthorized access of their personal data, Plaintiffs undoubtedly fall within the confines and intent of the statute.[14]

Facebook claims that Plaintiffs cannot state a claim under Section 502 because Plaintiffs "concede" that they "voluntary [sic] interacted with Facebook" and clicked on third-party advertisements. (Opp. at 19). Critically, Facebook overlooks the fact that Plaintiffs' voluntary interactions with Facebook were undertaken under the reasonable belief that Facebook would abide by its own Terms of Service and Privacy Policy. In particular, Facebook repeatedly represented that it would not share personal information with third-party advertisers without users' consent. Plaintiffs' submission of data and interaction with Facebook under the assumption that Facebook would abide by its own policies simply does not equate to Plaintiffs' consent to share their personal information with advertisers.

Facebook's claim that its Statement of Rights and Responsibilities provides Defendant with an irrevocable license to access and use any user content "anywhere on Facebook" also misses the

---

[14] Section 502 has not been strictly limited to instances of "hacking" or breaking into a computer" as Defendant rigidly defines these terms. For example, in *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039 (N.D. Cal. 2010), plaintiff alleged that defendants created and marketed software to automatically post ads on craigslist.com, provided services to post ads for customers, sold phone-verified accounts that could post ads without restriction, and offered other programs to avoid plaintiff's verification requirements for ads, all of which violated the terms of use of the craigslist.com website. The court found that plaintiff's allegations stated a claim under Section 502(c) because they established that defendants repeatedly visited the craigslist.com website for the purpose of obtaining information that they used to develop their unauthorized auto-posting programs and other services.

point. (MTD p. 19). Plaintiffs do not argue that Defendant unlawfully shared their information "anywhere on Facebook." Rather, Plaintiffs allege that Facebook unlawfully disclosed personal information to advertisers through the placement of Usernames, User IDs, and other information within Referrer Headers. It is clear that these actions extend beyond Facebook's site and go beyond any scope of consent that Facebook received from Plaintiffs relating to the use of Plaintiffs' personal information. Plaintiffs voluntarily clicked on third-party ads but did not authorize Facebook to *share their specific identities* with the advertiser. This distinction is crucial, as the disclosure that an anonymous user clicked on an advertisement is entirely different from the revelation that *a specific user* clicked on an advertisement from *the specific page that the user was viewing.* Because Facebook's actions expressly contradicted the Terms and Conditions that users agreed to, Facebook's access and dissemination of Plaintiffs' personal information occurred without permission. Accordingly, Plaintiffs' Section 502 claim should stand.

E. Plaintiffs Sufficiently Allege that Facebook Violated the CLRA.

The Consumer Legal Remedies Act ("CLRA") protects consumers from "unfair methods of competition and unfair or deceptive acts or practices." Cal. Civ. Code § 1761(d). The statute expressly provides that it "shall be liberally construed and applied to promote its underlying purposes, which are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection." Cal. Civ. Code § 1760. A "consumer" who suffers "any damage" as a result of any method, act, or practice prohibited by Section 1770 of the statute may assert a claim under the CLRA. Cal. Civ. Code § 1780(a).

The CLRA defines a "consumer" as "an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes." Cal. Civ. Code § 1761(d). Facebook's sole challenge to Plaintiffs' CLRA claim is that Plaintiffs are not "consumers" because Facebook's products are free are cannot be "purchased or leased." (MTD p. 21). As argued above, however, Facebook's products are not free. Facebook requires registrants to provide their actual names and other personal information as a prerequisite to using its products, and Facebook enjoys tremendous profits from its use of that information. Thus, Plaintiffs' use their personal information

to purchase Facebook products and services. For this reason, Plaintiffs are "consumers" within the meaning of the CLRA.

F. Plaintiffs Have Alleged Actionable Damages Resulting from Facebook's Breach of Contract.

Facebook argues that disclosure of personal information does not cause actionable damages sufficient to support a breach of contract claim. (Opp. at 23; citing *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 326-27 (E.D.N.Y. 2005).) But unlike the cases cited by Facebook, Plaintiffs here allege that their personal information was *the sole consideration provided in exchange for Facebook's services*. This distinction is critical to Plaintiffs' breach of contract claim.

Plaintiffs allege that in exchange for their use of Facebook's services, Plaintiffs transmitted their personal information to Facebook and that in turn, Facebook built its business model on that personal information to generate substantial advertising revenues. (Compl. ¶¶ 103-04, 105-07.) In other words, Facebook sought Plaintiffs' personal information as Facebook's benefit of the bargain. Because Plaintiffs' personal information was the primary (and indeed only) benefit Facebook bargained for, it is something of value and constitutes good consideration. *See Kremen v. Cohen*, 337 F.3d 1024, 1029 (9th Cir. 2003) (discussing whether personal information can constitute contract consideration).

The cases cited by Facebook are distinguishable, as not one of them involved a contract where personal information itself was the sole benefit of the bargain for the defendant. In *JetBlue*, *supra*, the defendant airline compiled personal information on each of its passengers, which it then sold to a data mining company. *JetBlue*, 379 F.3d at 304. The plaintiff sued for breach of JetBlue's privacy policy. The court considered the importance of the "nature of the contract asserted" and cited the Second Circuit's admonition that "damages in contract actions are limited to those that may reasonably be supposed to have been in the contemplation of both parties, at the time they made the contract, as the probable result of the breach of it." *Id.* at 327. In dismissing the breach of contract claim, the court concluded that the economic value of the plaintiff's personal information was not contemplated by the parties' contract and, therefore, the disclosure of that personal information

could not serve as the basis for the plaintiff's damages. *Id*. Obviously, that reasoning does not apply here.

Here, Plaintiffs have alleged that personal user information is critical to Facebook's success, and is indeed the very benefit sought by Facebook in its contract with Plaintiffs. And because Facebook understands that consumers demand safeguarding of their private information, Facebook made numerous, repeated, and unequivocal contractual promises to do so. Unlike in *JetBlue*, the safeguarding of Plaintiffs' personal information is at the heart of the contract breached by Facebook, and the damages flowing from unlawful disclosure of that information were contemplated by Facebook at the time of contracting.

JetBlue is distinguishable on an additional, equally important premise. The *JetBlue* court wrote that "there is absolutely no support for the proposition that the personal information of an individual JetBlue passenger had any value for which that passenger could have expected to be compensated. . . There is likewise no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large." *JetBlue*, 337 F.3d at 327. But the *JetBlue* court, writing in 2005, did not consider the arguments advanced here, namely that personal information increasingly represents the value provided by consumers and forms the sole consideration widely accepted by companies like Facebook in exchange for the provision of internet services. (*See* section IV(A)(2) *supra*.)[15] Indeed, Facebook, one of the largest and most successful pioneers of this new information economy, was barely one year old when the *JetBlue* decision was issued.

If Plaintiffs' personal information was freely available to companies like Facebook, then Plaintiffs would have nothing to offer in consideration for Facebook's services that Facebook couldn't already obtain for free. By disclosing Plaintiffs' personal information to advertisers, who

---

[15] Other examples of personal information as consideration abound. Many supermarket, for example, offer discounts in exchange for customer enrollment in "rewards programs" that are nothing more than "gimmicks designed to collect customer information." *Kremen*, 337 F.3d at 1029. And many internet sites offer consumers a chance to win a gift (like an iPod, for example) if they submit their personal information.

are under no obligation to safeguard it and who are free to sell and resell it to other third parties, Facebook has diminished Plaintiffs' ability to offer that information to others in exchange for goods and services.

The diminution in value of Plaintiffs' information may be small, or it may be substantial. But Plaintiffs need not provide a precise valuation of their damages at the pleading stage. Plaintiffs can, and will, provide evidence sufficient to quantify Plaintiffs' damages at the appropriate stage of these proceedings. However, Plaintiffs have sufficiently alleged that they suffered harm as a result of Facebook's breach, and this is sufficient to state a claim for breach of contract. *See Hepting*, 439 F.Supp. 2d at 999 ("at the pleading stage, general factual allegations of injury resulting from defendant's conduct may suffice"); *Landmark Screens, LLC v. Morgan, Lewis & Bockius LLP*, No. C-08-2581-JF, 2008 WL 4483817, at *6 (N.D. Cal. Oct. 2, 2008) ("the federal rules impose no requirement that plaintiff plead a specific amount of damage").

G. Plaintiffs Allegations State a Claim Under California Civil Code §§ 1572 and 1573.

Plaintiffs have sufficiently alleged that Facebook violated California Civil Code §§ 1572 and 1573.[16] As explained above, Plaintiffs have pled in detail the "who, what, where, when, and how" of Defendant's fraudulent conduct by identifying explicit, materially false statements by Facebook, reliance on Facebook's misrepresentations, and resulting damages. *AOL*, 719 F. Supp. 2d at 1112. These allegations satisfy Rule 9(b) and are sufficient to state a claim under Sections 1572 and 1573.

H. Plaintiffs Have Properly Alleged a Claim for Unjust Enrichment in the Alternative.

As detailed above, Plaintiffs have alleged sufficient facts to state a claim for breach of contract. However, in the event that the Court determines that Plaintiffs did not enter into an enforceable contract with Facebook, Plaintiffs' unjust enrichment claim should stand.

---

[16] Cal. Civ. Code § 1573 provides that actual fraud exists when a party to a contract suppresses "that which is true, by one having knowledge or belief of the fact" "with intent to deceive another party thereto, or to induce him to enter into the contract." Cal. Civ. Code § 1572 provides in relevant part that constructive fraud exists "[i]n any such act or omission as the law specially declares to be fraudulent, without respect to actual fraud."

Contrary to Facebook's blanket assertion, California courts recognize an independent cause of action for unjust enrichment. *See Villager Franchise Sys. v. Dhami, Dhami & Virk*, CF-F-04-6393, 2006 WL 224425 at *7 (E.D. Cal. Jan. 26, 2006) ("California law recognizes a cause of action for unjust enrichment" and requires a defendant to make restitution who has unjustly retained a benefit from plaintiff); *Gerlinger v. Amazon.Com, Inc.*, 311 F. Supp. 2d 838, 856 (N.D. Cal. 2004) ("Under California law, unjust enrichment is an action in quasi-contract"); *Hirsch v. Bank of America*, 107 Cal. App. 4th 708, 722 (2003) (finding that plaintiff stated a valid cause of action for unjust enrichment based on defendant's unjustified retention of excessive fees).

Because the existence of an enforceable contract is uncertain at this stage of the litigation, Plaintiffs may maintain a claim for unjust enrichment while simultaneously alleging the existence of an express contract. *See McBride v. Boughton*, 123 Cal. App. 4th 379, 388 (2004) ("restitution may be awarded in lieu of breach of contract damages when the parties had an express contract, but it was procured by fraud or is unenforceable or ineffective for some reason"). More generally, it is well established that under FRCP 8(d), a party may "allege inconsistent factual allegations" and "plead alternative theories of liability, even if those theories are inconsistent." *Cellars v. Pacific Coast Packaging, Inc.*, 189 F.R.D. 575 (N.D. Cal. 1999). Plaintiffs allege unjust enrichment in the alternative in the event that this Court rejects Plaintiffs' breach of contract claim. Facebook itself concedes that the Court may consider Plaintiffs' unjust enrichment claim as "some alternate legal theory that would give rise to a restitutionary remedy. (Opp. at 24). *See Nordberg v. Trilegiant Corp.*, 445 F. Supp. 2d 1082, 1100-1101 (N.D. Cal. 2006) ("plaintiffs may assert a claim for restitution based on a theory of unjust enrichment").

V. Conclusion

For the foregoing reasons, this Court should deny Facebook's motion to dismiss in full.

Dated: February 25, 2011

Respectfully submitted,
NASSIRI & JUNG LLP

s/ Kassra P. Nassiri
Kassra P. Nassiri
Attorneys for Plaintiffs and the Putative Class

Dated: February 25, 2011

Respectfully submitted,
EDELSON MCGUIRE, LLP

s/ Michael J. Aschenbrener
Michael J. Aschenbrener
Attorneys for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

The undersigned certifies that, on February 25, 2011, he caused this document to be electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of filing to counsel of record for each party.

Dated: February 25, 2011

EDELSON MCGUIRE LLC

By: s/ Michael Aschenbrener
Michael Aschenbrener