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 LLP
SEAN REIS (184044) (sreis@edelson.com)
30021 Tomas Street, Suite 300
Rancho Santa Margarita, CA 92688
Telephone: (949) 459-2124
Facsimile: (949) 459-2123

MICHAEL J. ASCHENBRENER (277114)
(mja@aschenbrenerlaw.com)
ASCHENBRENER LAW, P.C.
795 Folsom Street, First Floor
San Francisco, California 94107
Telephone: (415) 813-6245
Facsimile: (415) 813-6246

*ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO DIVISION**

IN RE: FACEBOOK PRIVACY LITIGATION

Case No. 10-cv-02389-JW

CLASS ACTION

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

ACTION FILED: 05/28/10

Date: October 17, 2011
Time: 9:00 a.m.
Judge: Hon. James Ware

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**CASES**

**STATUTES**



**OTHER AUTHORITIES**

## I. INTRODUCTION & FACTUAL BACKGROUND

In the Court's May 12, 2011 Order granting in part Defendant's motion to dismiss, the Court identified several pleading deficiencies and granted Plaintiffs leave to file an amended complaint as to certain causes of action. In their First Amended Class Action Complaint ("FAC"), Plaintiffs remedy each of the pleading deficiencies identified.

With respect to Plaintiffs' claim under the Stored Communications Act ("SCA"), Facebook again relies primarily on the "intended recipient" exception to liability available exclusively to electronic communication service ("ECS") providers, arguing that it cannot be liable for disclosing Plaintiffs' communications because Facebook was the "intended recipient" of such communications under 18 U.S.C. 2702(b)(3). However, Facebook's argument overlooks the fact that Plaintiffs also allege that Facebook is a remote computing service ("RCS") provider. (FAC ¶¶ 81, 83.) Because an RCS provider may not avail itself of the "intended recipient" exception under the SCA and Plaintiffs did not consent to Facebook sharing their personal information with third-parties (FAC ¶¶ 3, 34, 84), Facebook lacked consent to divulge Plaintiffs' communications and thus violated the SCA.

Facebook's challenges to Plaintiffs' remaining claims fare no better. Facebook argues that Plaintiffs fail to allege that they suffered actual and appreciable damages. But as demonstrated below, Plaintiffs now allege specific, non-conclusory facts that establish damages (FAC ¶¶ 16, 17, 22, 23, 122), and present case law from within this District that explicitly accepts Plaintiffs' damage theory. Accordingly, Facebook's challenge to Plaintiffs' breach of contract claim must fail.

Facebook similarly rehashes arguments in opposition to Plaintiffs' claims under Cal. Civil Code §§ 1572 & 1573 (actual and constructive fraud) and Cal. Penal Code § 502(c)(8). But the FAC explicitly addresses any deficiencies of the original complaint by alleging reliance on Facebook's misstatements (FAC ¶¶ 4, 5, 76, 126) and the particulars of Defendant's fraudulent conduct (FAC ¶¶ 27-33), and by alleging precisely how Facebook knowingly

introduced a computer contaminant into Plaintiffs' computers in violation of the California Computer Crime Law (FAC ¶¶ 3, 33-44, 104).

For these reasons, and as explained in further detail below, the Court should deny Facebook's Motion to Dismiss ("MTD").

## II. 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." *Cassierer v. Kingdom of Spain*, 580 F.3d 1048, 1052 (9th Cir. 2009). 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). "Once a claim has been adequately stated, it may be supported by showing any set of facts consistent with the allegations in the complaint." *Bell Atlantic v. Twombly*, 550 U.S. 544, 546 (2009). A complaint need only contain 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); Fed. R. Civ. P. 8(a).

As demonstrated below, the FAC 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.

## III. DISCUSSION

### A. Facebook, in Its Capacity as a Remote Computing Service Provider, Is Liable Under the SCA.

Facebook's fundamental challenge to Plaintiffs' SCA claim is that because Facebook was the "intended recipient" of Plaintiffs' communications under 18 U.S.C. 2702(b)(3), "Facebook had its own consent to divulge the communication to third-party advertisers." (MTD at 11.) Facebook's argument fails, however, because Facebook was acting as an RCS provider at the time that it non-consensually divulged the contents of Plaintiffs' communications. Because

unlike an ECS provider, an RCS provider may not avail itself of the SCA's "intended recipient" exception, Facebook is liable under the SCA.

**1. Facebook Was Acting as a Remote Computing Service Provider when It Divulged the Content of Plaintiffs' Communications.**

Depending on the particular service function that it is providing, Facebook functions as both an ECS and RCS provider.[1] In the context of an SCA claim, whether a service provider is an RCS provider or an ECS provider depends on the particular service function at issue. *See, e.g., Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 986 n.42 (C.D. Cal. 2010). Although Facebook allows users to send private messages to one another (the ECS function), Plaintiffs' claims concern Facebook's remote computing service.[2] Plaintiffs allege Facebook provided to them computer storage and processing services by allowing them to process, store, and share content, including pictures, videos, biographical information and more. (FAC ¶¶ 80-81.) Plaintiffs further allege that Facebook allows its users the choice to grant certain other users a license to view information stored on its remote computing service. (*Id.*) This content storage and sharing function forms the crux of Plaintiffs' claims and makes Facebook an RCS provider subject to section 2702(a)(2) of the SCA. *See, e.g., Viacom Int'l Inc. v. YouTube, Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008) (holding that YouTube is an RCS provider because it provides storage, processing and sharing of videos); *Crispin*, 717 F. Supp. 2d at 990 (holding that Facebook is an RCS provider and subject to § 2702(a)(2)).

Plaintiffs allege that the non-consensual disclosures occurred while Facebook users browsed stored content on Facebook's site (an RCS function). (FAC ¶ 44.) Plaintiffs also allege that they sent communications (*i.e.*, communications concerning their identities and which of

---

[1] Facebook provides both remote computing and electronic communications services (e.g., private messaging between users). As the Ninth Circuit recognized, an entity may be both an ECS and RCS provider. *Theofel v. Farey-Jones*, 341 F.3d 978, 1076-77 (9th Cir. 2003) (implying that some but "not all remote computing services are also electronic communications services"). Plaintiffs' claims here concern Facebook's remote computing service, not its electronic communications service.

[2] The "term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

their own stored content or friends' stored content they wished to view) to Facebook for the specific and sole purpose of using Facebook's remote computing services and did not authorize Facebook to use those communications for any other purpose.[3] (*Id.* ¶ 76.) Accordingly, in the context of Plaintiffs' allegations, Facebook was acting as an RCS provider and did not have Plaintiffs' consent to further divulge the subject communications to third parties. By divulging the contents of those communications to third-party advertisers without Plaintiffs' consent, Facebook violated section 2702(a)(2).

**2. As an RCS Provider, Facebook May Not Rely on the "Intended Recipient" Exception to Liability.**

Facebook argues that the SCA allows ECS providers to divulge the contents of a communication "with the lawful consent of the originator or an addressee or intended recipient of such communication." (MTD at 11.) But only ECS providers, and not RCS providers like Facebook, may avail themselves of the SCA's "intended recipient" exception.[4] Because Plaintiffs' claims implicate Facebook's RCS function (FAC ¶¶ 81, 83), the "intended recipient" exception does not apply here.

Depending on whether ECS or RCS is at issue, section 2702(b)(3) establishes different criteria for establishing an exception to the general rule against disclosure:

> Exceptions for disclosure of communications.— A provider described in subsection (a) may divulge the contents of a communication—
> . . .

[3] Section 2702(a)(2) prevents an RCS provider from divulging electronic communications sent to it "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the [RCS] provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."

[4] Indeed, information received by RCS providers, such as YouTube, often has no "intended recipient" in the way that an email message has an "intended recipient." For example, Facebook users who upload pictures may do so purely for storage purposes, and may or may not share those pictures with others. In that case, even the uploaded pictures have no "intended recipient," they are protected by section 2702(a)(2) and may only by divulged by Facebook with the user's consent. *See, e.g., YouTube*, 253 F.R.D. at 264-65 (construing § 2702(b)(3) to require subscriber consent in the case of RCS providers).

> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, **or the subscriber in the case of a remote computing service**;

(Emphasis supplied.)

Pursuant to the SCA, in its capacity as an RCS provider Facebook may divulge the contents of communications only with the consent of the subscriber (in this case, Plaintiffs). *See, e.g., Crispin,* 717 F. Supp. 2d at 973 n.17 ("An RCS provider can avail itself of all but one of the exceptions set forth in § 2702(b). An RCS provider may divulge the contents of a communication with consent of the 'subscriber,' while an ECS provider may divulge the contents with the lawful consent of an addressee or intended recipient of such communication. 18 U.S.C. § 2702(b)(3)."); *Flagg v. City of Detroit,* 252 F.R.D. 346, 349-50 (E.D. Mich. 2008) ("The potential importance of distinguishing between an "ECS" and an "RCS" lies in the different criteria for establishing an exception to the general rule against disclosure. The provider of an RCS may divulge the contents of a communication with the "lawful consent" of the subscriber to the service, while the provider of an ECS may divulge such a communication only with the "lawful consent of the originator or an addressee or intended recipient of such communication.") (citing 18 U.S.C. § 2702(b)(3)).[5]

Because Facebook was acting as an RCS provider, it may not assert the § 2702(b)(3) "intended recipient" exception. As a result, Facebook needs more than its own consent to divulge Plaintiffs' communications—it needs the consent of Plaintiffs, who are the "subscribers" under § 2702(b)(3). As alleged, Plaintiffs explicitly did not provide consent to Facebook to share their communications. (FAC, ¶¶ 3, 16, 27-34, 77, 79, 84.) Accordingly, the "intended recipient"

---

[5] Facebook cites in *In re Am. Airlines, Inc., Privacy Litig.*, 370 F. Supp. 2d 552, 560-61 (N.D. Tex. 2005) for the proposition that an RCS provider may give its own consent to disclose customer communications to third parties. The district court there, however, did not bother to determine whether the defendant was an ECS or RCS provider, nor did it consider whether the "intended recipient" is available to RCS providers. Similarly, the court in *Quon v. Arch Wireless Op. Co., Inc*., 529 F.3d 892, 900 (9th Cir. 2008) noted, without analysis or discussion, that the intended recipient defense may apply to an RCS provider. The holding of that case, however, did not depend on the truth of that statement, making it dictum. Moreover, for the reasons noted immediately below, the dictum in *Quon* defies the purpose of the SCA as it applies to RCS providers like Facebook.

exception does not exculpate Facebook and it is liable for divulging Plaintiffs' communications without consent under § 2702(a)(2).

### 3. Even Assuming the "Intended Recipient" Exception Could Apply to an RCS Provider, Facebook May Not Give Itself Consent to Divulge Plaintiffs' Communications.

Crediting Facebook's interpretation of the SCA would mean that virtually every RCS may disclose any communication by any user at any time. This interpretation undermines the clear purpose of the statute and creates an absurd result.

Liability under Section 2702(a)(2) is created by disclosing communications "received by means of ***electronic transmission*** from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." (Emphasis supplied). But the way that Facebook (and virtually all other RCS providers) provides remote computing services is to send and receive electronic communications directly to and from its users by means of electronic transmission. Plaintiffs (and all Facebook users) must send ***all*** of their communications directly to Facebook in order to use Facebook's services.[6]

Facebook's claim that it is not liable for disclosing Plaintiffs' communications because it was the "intended recipient" of those communications is illogical. If this reasoning were followed, all of the SCA's protections against unauthorized disclosure of communications would be eviscerated, and any RCS provider would be exonerated from any and all of its disclosures. Because all user communications carried or maintained on an RCS's computers are sent to it directly by the user, it is an "intended recipient" of *all* of the users' communications; and following Facebook's reasoning, any RCS may freely divulge any communication to any third

[6] There is no way, for example, for a user to store a picture on Facebook without sending that picture to Facebook. Similarly, there was no way for Plaintiffs to view stored content on Facebook without sending a communication to Facebook telling Facebook to display that content.

party.[7] If the Court makes the "intended recipient" defense available to an RCS provider in the manner Facebook suggests, it would defeat the plain purpose of section 2702(a)(2) and much of the SCA.[8]

It is axiomatic that a court may not adopt a plain language interpretation of a statutory provision that directly undercuts the clear purpose of the statute. In *Brooks v. Donovan,* 699 F.2d 1010 (9th Cir. 1983), the Ninth Circuit refused to adopt a plain language interpretation of a statute governing pension funds. The court reasoned that it "must look beyond the express language of a statute where a literal interpretation 'would thwart the purpose of the overall statutory scheme or lead to an absurd or futile result.'" *Id.* at 1011 (quoting *International Tel. & Tel. Corp. v. General Tel. & Elec. Corp.,* 518 F.2d 913, 917-918 (9th Cir.1975)).

In reaching its conclusion, the Ninth Circuit followed the Supreme Court's approach in *United States v. American Trucking Ass'ns.*, 310 U.S. 534, 60 S. Ct. 1059, 84 L. Ed. 1345 (1940). There the Court noted that "[w]hen [a given] meaning has led to absurd results . . . this Court has looked beyond the words to the purpose of the act. Frequently, however, *even when the plain meaning did not produce absurd results but merely an unreasonable one 'plainly at variance with the policy of the legislation as a whole,' this Court has followed that purpose, rather than the literal words.*" *Id.* at 543 (emphasis added; citations omitted). *See also Bosley Med. Inst., Inc. v. Kremer,* 403 F.3d 672, 681 (9th Cir. 2005) ("We try to avoid, where possible, an interpretation of a statute that renders any part of it superfluous and does not give effect to all of the words used by [the legislature.]") (internal quotation marks and citation omitted); *Hibbs v. Winn,* 542 U.S. 88, 101 (2004) ( "'[a] statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant . . . .'")

---

[7] For example, cloud-based financial services software would be able to disclose user financial data to third-parties, and online computer backup services that store customer data online would be able to sell that data to advertisers without consent.

[8] Not surprisingly, of the dozens of other courts to consider the "intended recipient" provision of section 2702(b)(3), Plaintiffs are aware of only one (*In re American Airlines, supra,* n.5) that held that a provider (ECS or RCS) may construe itself as the "intended recipient" and give itself consent to disclose communications, notwithstanding that every provider in those cases could have made the same argument Facebook makes here.

(quoting 2A N. Singer, Statutes and Statutory Construction § 46.06, at 181-86 (rev. 6th ed. 2000)).

Facebook seeks to give itself "its own consent to divulge [Plaintiffs'] communication[s] to third-party advertisers." This produces a nonsensical result under the SCA. Allowing RCS providers to "give their own consent" to disclose user communications would defeat most all of the consumer privacy protections in the statutes. This Court should preserve the intent and purpose of the SCA and reject Facebook's "intended recipient" argument.

**4. Facebook Disclosed the Contents of Plaintiffs' Communications.**

Facebook renews its argument that it merely disclosed customer records relating to Plaintiffs, and not the content of any of Plaintiffs' communications. In doing so, Facebook claims that it revealed nothing more than Plaintiffs' usernames, and cites to cases involving the disclosure of bare customer records. But Facebook also disclosed the URLs of the particular pages Plaintiffs were viewing when they clicked on ads (FAC ¶ 35) along with their identities, which courts have held in other contexts constitutes disclosure of content. This bundle of information, all of which was communicated to Facebook by Plaintiffs incident to their use of Facebook's remote computing services, revealed to advertisers much more than mere customer records.[9]

The Ninth Circuit has held in other contexts that disclosures of the URLs of the pages visited by a user (as Plaintiffs allege here) constitute the disclosure of *contents* of communication. In *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), the Ninth Circuit considered whether computer surveillance that enabled the government to learn the to/from addresses of the plaintiff's email messages, the IP addresses of the websites that he visited, and the total volume of information transmitted to or from his account constituted a search for Fourth

[9] In order to browse Facebook's website, Plaintiffs sent electronic communications to Facebook indicating which pages they wished to view. (FAC ¶ 74.) The SCA broadly defines an electronic communication as "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." 18 U.S.C. § 2510(12). The "substance" and "meaning" of Plaintiffs' communications was that Plaintiffs were interested in viewing particular content on Facebook's site. 18 U.S.C. § 2510(8).

Amendment purposes. In holding that it did not, the Ninth Circuit reasoned that the surveillance techniques the government employed were indistinguishable from the use of a pen register, and the surveillance did not acquire the contents of the plaintiff's communications. *Id.* at 509-10. The court paid careful attention to the government's acquisition of the IP addresses of websites that the plaintiff visited, concluding that IP addresses do not reveal content:

> IP addresses constitute addressing information and do not necessarily reveal any more about the underlying ***contents of communication*** than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed … the [United States Supreme] Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

*Id.* at 510 (emphasis supplied).[10]

But the court went on to observe that had the government acquired ***URLs*** of the pages viewed by the plaintiff, content would be revealed and the surveillance might be constitutionally problematic:

> Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas ***a technique that captures URLs would also divulge the particular articles the person viewed***. *See Pen Register Application*, 396 F.Supp.2d at 49 ("[I]f the user then enters a search phrase [in the Google search engine], that search phrase would appear in the URL after the first forward slash. ***This would reveal content***....").

[10] In coming to this conclusion, the court relied on the fact that even though a website like the *New York Times* may contain hundreds or thousands of pages, it typically has only one IP address. *Id.* at n.5.

*Id.* at n.6 (emphasis supplied).

Plaintiffs allege that Facebook revealed the precise content that the Ninth Circuit found problematic in *Forrester*: the URLs that Plaintiffs were viewing at the time they clicked on Facebook advertisements. By disclosing the URLs along with Plaintiff's identities, Facebook divulged more than mere customer records—it divulged the content of Plaintiffs' communications.[11]

Ultimately, none of Facebook's SCA defenses withstands recent, relevant case law or long-held canons of statutory interpretation. As an RCS, Facebook may not give itself consent to reveal customer communications. Furthermore, the data Facebook disclosed to third-parties constitutes the content of Plaintiffs' communications and not mere customer records. Accordingly, Plaintiffs request that the Court deny Facebook's motion to dismiss their SCA cause of action.

**B. Plaintiffs Have Cured the Defects in Their Breach of Contract Claim that the Court Previously Identified.**

In dismissing Plaintiffs' breach of contract claim without prejudice from their Consolidated Complaint, the Court articulated two bases for the dismissal: (1) Plaintiffs only alleged they "suffered injury" without alleging facts demonstrating specific, actual damages (Order at 15); and, (2) "Plaintiffs' contention that their personal information constitutes a form of 'payment' to Defendant is unsupported by law" (Order at 12 n.10). Facebook reiterates these arguments in its motion to dismiss, arguing that Plaintiffs have not addressed these defects in the FAC.

Facebook's arguments ignore several of Plaintiffs' amended allegations as well as recent case law specifically embracing Plaintiffs' damage theory. As to the first basis, Plaintiffs have cured any pleading defect by specifically alleging actual, non-speculative damages. As to the

[11] Facebook's reliance on *Sams v. Yahoo!, Inc.*, No. 10-cv-5897-JF (HRL), 2011 WL 1884633 (N.D. Cal. May 18, 2011) is inapposite. That case did not involve the disclosure of particular URLs, and instead involved disclosure of mere "user identification information." *Id.* at *7.

second basis, Plaintiffs can now cite to new, relevant case law supporting their position that personal information constitutes a form of payment.

**1. Plaintiffs Have Alleged "Actual and Appreciable" Damages.**

In order to state a cause of action for breach of contract, Plaintiffs must plead four elements: "[1] the contract, [2] plaintiffs' performance (or excuse for nonperformance), [3] defendant's breach, and [4] damage to plaintiffs therefrom." *Gautier v. Gen. Tel. Co*., 234 Cal. App. 2d 302, 305 (1965).

Defendant concedes in its motion to dismiss that Plaintiffs have sufficiently pleaded the first three elements. Thus, the only issue is whether Plaintiffs have sufficiently alleged "actual and appreciable damage" flowing from Facebook's breach. *Aguilera v. Pirelli Armstrong Tire Corp*., 223 F.3d 1010, 1015 (9th Cir. 2000).

The FAC contains extensive specific, non-conclusory allegations of actual and appreciable damages flowing from Defendant's breach of its contract with Plaintiffs and the putative class. First, Plaintiffs allege facts concerning Facebook's business model of using its users' personal information to generate substantial advertising revenue, which provides the foundation for Plaintiffs' theory of damages. (FAC ¶¶ 16-23.)

Then, Plaintiffs specifically allege the exact form of the damages that they suffered:

> As a result of Facebook's misconduct and breach of the Agreement described herein, Plaintiffs and the Class suffered damages. Plaintiff and the Class members did not receive the benefit of the bargain for which they contracted and for which the[y] paid valuable consideration in the form of their personal information, which, as alleged above, has ascertainable value to be proven at trial. In other words, Plaintiff and each Class member gave up something of value, PII, in exchange for access to Facebook and Facebook's privacy promises. Facebook materially breached the contracts by violating its privacy terms, thus depriving Plaintiff and Class members the benefit of the bargain. Thus, their actual and appreciable damages take the form of the value of their PII that Facebook wrongfully shared with advertisers.

(FAC ¶ 122.)

As alleged, Plaintiffs have suffered damages because the personal information they provided to Facebook in exchange for access to Facebook and Facebook's contractual promise

not to share that personal information has concrete, ascertainable value. (FAC ¶¶ 16, 17, 22, 23 122.) Plaintiffs' loss or diminution of that personal information as a result of Facebook's unauthorized disclosure constitutes actual harm.

Robust and established markets exist that can provide valuations for numerous pieces of personal information and allow individuals and entities to purchase and exchange personal information. (FAC ¶ 23.) In the absence of consent, Plaintiffs should be the ones profiting from the distribution of their personal data, not Facebook. Plaintiffs did not provide consent for Facebook to reveal their valuable personal information to advertisers or other third-parties. (FAC ¶¶ 4, 5, 34, 116.) Therefore, Plaintiffs have lost the right to sell that data to the entities that now no longer need to pay Plaintiffs for it because they obtained it from Facebook. That is how Plaintiffs have suffered damages. Facebook has deprived them of the right to sell their own personal data, which Plaintiffs have alleged is of real, demonstrable value.

While Plaintiffs intend to introduce expert testimony as to the specific value of Plaintiffs' personal information at issue, Plaintiffs need not identify the specific value associated with the personal information at this procedural stage. *See Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 999 (N.D. Cal. 2006) ("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"). Accordingly, Plaintiffs have sufficiently pleaded concrete, appreciable damages as required in this district.

**2. Plaintiffs' Theory of Damages Is Supported by Recent Case Law.**

Recently, a court in this district denied a motion to dismiss a breach of contract claim based on damages allegations identical to those in the instant case. *Claridge v. RockYou*, No. 09-cv-6032-PJH, Dkt. 47 (N.D. Cal. April 11, 2011).[12] Thus, it can no longer be said that there is

[12] Judge Hamilton issued the order denying the defendant's motion to dimsis in *Claridge* six weeks after Plaintiffs in the instant case filed their opposition to Facebook's motion to dismiss and nearly a month after Facebook filed its reply in support of its motion.

no case law supporting Plaintiffs' contention that personal information constitutes a form of payment.

In *Claridge*, the plaintiff offered the exact same damages theory as Plaintiffs in this case allege: that he paid for access to "free" online services with his personal information, and RockYou breached its contract with him by failing to protect his personal information. *Id*. at 6. In particular, the plaintiff in *Claridge* alleged that the defendant caused unauthorized third-parties to gain access to personal information provided to the defendant in exchange for online services. *Id*. at 2. He further alleged that his personal information had actual and concrete value, and the unauthorized sharing of it caused him economic injury. *Id*. at 6. On this basis, the plaintiff alleged that the defendant breached its contract with users in which it represented that it would not to allow third-party access to personal information. *Id*. at 12-13.

The court in *Claridge* held that the plaintiff had adequately alleged concrete, particularized harm for purposes of Article III standing and denied the defendant's motion to dismiss the breach of contract claim. In finding that the plaintiff had standing, the court expressly embraced the damages theory at issue here:

> On balance, the court declines to hold at this juncture that, as a matter of law, plaintiff has failed to allege an injury in fact sufficient to support Article III standing. Not only is there a paucity of controlling authority regarding the legal sufficiency of plaintiff's damages theory, but the court also takes note that the context in which plaintiff's theory arises – i.e., the unauthorized disclosure of personal information via the Internet – is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts. For that reason, and although the court has doubts about plaintiff's ultimate ability to prove his damages theory in this case, the court finds plaintiff's allegations of harm sufficient at this stage to allege a generalized injury in fact."

*Id*. at 7. Addressing the breach of contract claim directly, the court stated:

> Moreover, the damage element inherent in contractual claims parallels the type of concrete, nonspeculative injury that must be pled in order to adequately allege injury in fact under Article III. See, e.g., Buttram v. Owens-Corning Fiberglas Corp., 16 Cal. 4th 520, 531 n. 4 (1997)("[T]o be actionable, harm must constitute something more than nominal damages, speculative harm, or the threat of future harm-not yet realized ...").

> For the reasons already noted at the outset, therefore, the court concludes that at the present pleading stage, plaintiff has sufficiently alleged a general basis for harm by alleging that the breach of his PII has caused him to lose some ascertainable but unidentified "value" and/or property right inherent in the PII. As such, the court declines to dismiss plaintiff's breach claims on grounds that plaintiff has failed to allege damages or harm as a matter of law.

*Id*. at 13. Accordingly, *Claridge* provides the case law to support Plaintiffs' damages allegations that this Court sought in ruling on Defendant's first motion to dismiss. Furthermore, as the court in *Claridge* noted, the "paucity" of case law concerning personal information as payment is not surprising given the context in which this issue arises is itself new. *Id*. Thus, the fact that little case law exists should not be held against Plaintiffs; the facts and issues are new, but that does not mean that Plaintiffs should be denied the right to make their case.

Facebook counters Plaintiffs' contentions with a footnote arguing that disclosure of personal information does not cause actionable damages sufficient to support a breach of contract claim. (MTD at 23 n.15; citing *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 326-27 (E.D.N.Y. 2005).) But the cases on which Facebook relies are readily distinguishable from the instant matter as not one of them involved a contract where personal information itself was the benefit of the bargain sought by the defendant.

In *JetBlue*, 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 parties' contract contemplated the exchange of U.S. currency for an airline ticket, not the economic value of the plaintiff's personal information that necessarily coincides with ticket purchasing and, therefore, the disclosure of that personal information could not serve as the basis for the plaintiff's damages. *Id*. In contrast, Facebook's contract with Plaintiffs contemplated the exchange of

personal information for Facebook's services. 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 damage resulting from the unauthorized disclosure of Plaintiff's personal information, which itself was the sole consideration provided by Plaintiffs, should have reasonably been contemplated by Facebook. Thus, *JetBlue* is not applicable in this instant matter.

*JetBlue* is distinguishable on an additional, equally important premise. The *JetBlue* court wrote that "[t]here 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 before Facebook was a multi-billion dollar entity, did not consider the arguments advanced here or the allegations in the instant FAC; namely, that there is now a robust market for personal information available to Plaintiffs and all consumers. (FAC ¶¶ 22-23.) Unlike the timeframe in which *JetBlue* arose, personal information now has significant compensable value in the economy at large.

*Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1199-1200 (D.N.D. 2004), is also distinguishable because the court ruled therein that the plaintiffs failed to allege *any* specific facts supporting their claim of damages. *Id*. In contrast, Plaintiffs here have alleged in great detail the specific basis of their claim of damages. While the Court may find the basis novel, Plaintiffs nonetheless thoroughly allege factual support for their claim of damages, which is more than sufficient to meet Plaintiffs' burden at the pleading stage. Besides, as the Court stated in *Claridge*, "the court also takes note that the context in which plaintiff's theory arises – i.e., the unauthorized disclosure of personal information via the Internet – is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts." *Claridge* at 7.

As thoroughly discussed herein, Plaintiffs have sufficiently alleged that they suffered actual and appreciable harm as a result of Facebook's breach. Furthermore, Plaintiffs' damages theory now finds legal support in a ruling on this identical issue in this district. In other words,

Plaintiffs' damages theory now finds support not only in economics and commerce, but in the law, as well.

Therefore, Plaintiffs ask the Court to hold that Plaintiffs have sufficiently alleged actual and appreciable damages, and deny Defendant's motion to dismiss their breach of contract claim.

### C. Plaintiffs' FAC Alleges Plaintiffs Relied on Defendant's Alleged Fraudulent Misrepresentations.

In dismissing without prejudice Plaintiffs' causes of action under §§ 1572 & 1573 of the California Civil Code, the Court ruled that Plaintiffs failed to allege "that they relied upon any allegedly fraudulent misrepresentations by Defendant." (Order at 15.) In the FAC, Plaintiffs have explicitly alleged that they relied on Facebook's false assertions that it would not share user PII without consent in contracting with and using Facebook. (FAC ¶¶ 4, 5, 76, 126.) Accordingly, having cured the lone pleading defect identified by the Court, Plaintiffs §§ 1572 and 1573 fraud claims should not be dismissed.

Facebook's remaining challenges to Plaintiffs' §§ 1572 and 1573 claims are without merit. Facebook first argues that Plaintiffs fail to plead facts sounding in fraud with particularity as required by Fed. R. Civ. P. 9(b). However, Plaintiffs have met their burden of pleading the "who, what, when, where, and how" of the alleged fraud. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). In particular, Plaintiffs specifically allege who committed the fraud (Mark Zuckerberg, ¶ 31; Facebook's Director of Corporate Communications, ¶ 30); what the fraud consists of (Facebook's Privacy Policy and public statements, ¶¶ 27-33); when the fraud was committed (April 5, 2010, ¶ 30; February 16, 2009, ¶ 31); where the fraud was committed (facebook.com, ¶¶ 27-33); and how it was committed (through official Facebook public communications) (¶¶ 27-33). These allegations are more than sufficient to put Facebook "on notice" of their alleged fraudulent conduct. *See Concha v. London*, 62 F.3d 1493, 1502 (9th Cir. 1995) (finding that 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").

Facebook's additional argument that Plaintiffs fail to specifically allege "when" they clicked on advertisements is irrelevant to §§ 1572 and 1573. Facebook's attempt to distort the pleading requirements of allegations sounding in fraud misses the point. Rule 9(b) requires that Plaintiffs specifically identify "when" the fraud occurred, not "when" Plaintiffs acted on the fraud. *See Vess*, 317 F.3d at 1106. And as discussed above, Plaintiff alleges that Facebook committed the fraud on February 16, 2009 and April 5, 2010, as well as all times that its Privacy Policy was available on facebook.com.

Furthermore, Plaintiffs explicitly detail what was false or misleading about Facebook's statements, and why it was false. *Id*. Namely, that Facebook promised it would not share Plaintiffs' personal information with third-parties but did so anyway. (FAC ¶¶ 27-34.) Therefore, Plaintiffs have met and surpassed their burden of pleading fraud, and the Court should deny Facebook's motion to dismiss.

**D. Defendant Introduced Computer Instructions that Usurped the Normal Operation of Plaintiffs' Computers in Violation of the CCCL.**

The Court granted Plaintiffs leave to re-plead their cause of action under Cal. Penal Code § 502(c)(8) with specific "facts suggesting that Defendant introduced computer instructions designed to 'usurp the normal operation' of a computer, computer system or computer network." (Order at 13 n.11.) Plaintiffs' FAC fully addresses the Court's concerns with detailed allegations and facts supporting its § 502(c)(8) claims. As a result, Plaintiffs request that the Court deny Defendant's motion to dismiss this cause of action.

Facebook's conduct, as alleged in detail in Plaintiffs' FAC, exemplifies the exact conduct proscribed by § 502(c)(8), which applies to any person who "knowingly introduces any computer contaminant into any computer, computer system, or computer network." Cal. Penal Code § 502(c)(8). The term "computer contaminant" is defined as "any set of computer instructions that are designed to . . . transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information." Cal. Penal Code § 502(b)(10).

As alleged, Facebook knowingly introduced a computer contaminant into Plaintiffs' computers by instructing Plaintiffs' computers and web browsers to transmit Plaintiffs' personal information without Plaintiffs' permission. (FAC ¶¶ 3, 33-44, 104.) As these detailed allegations and facts demonstrate, Facebook was in full control over whether the web browsers on Plaintiffs' computers transmitted Plaintiffs' personal information. Because of Facebook's explicit computer instructions controlling the handling and content of referrer headers, Defendant usurped the normal operation of Plaintiffs' computers, which would not have transmitted personal information via referrer headers if not for Facebook's explicit computer instructions to do so. (FAC ¶¶ 42, 104.)

Accordingly, Plaintiffs request that the Court dismiss Facebook's motion to deny Plaintiffs' Computer Crime Law cause of action.

## IV. CONCLUSION

In their FAC, Plaintiffs have fixed the pleading defects identified by the Court. Furthermore, Defendant's MTD does not offer any new arguments that warrant dismissal of Plaintiffs' remaining claims.

As discussed herein, Facebook may not avail itself of the "intended recipient" exception to the SCA's mandate not to disclose customer communications sent to Facebook because the FAC alleges it was acting as an RCS, not an ECS, when it disclosed Plaintiffs' communications. Accordingly, Facebook is liable under the SCA for its admitted practice of divulging Plaintiffs' communications without consent.

Additionally, Plaintiffs cured the defects in their Breach of Contract, statutory fraud, and Computer Crime Law claims. First, Plaintiffs' FAC contains specific and thorough allegations of actual and appreciable injuries. Moreover, Plaintiffs are now able to cite to case law from this District that adopts Plaintiffs' damage theory. Second, Plaintiffs' FAC contains explicit allegations that Plaintiffs relied on Facebook's fraudulent misrepresentations, thus curing the Court's lone identified concern with Plaintiffs' §§ 1572 and 1573 claims. Finally, Plaintiffs' FAC demonstrates exactly how Facebook introduced a computer contaminant into Plaintiffs'

computers that usurped the normal operation of Plaintiffs' computers and thereby transmitted personal data in violation of Cal. Civ. Code § 502(c)(8).

In the end, Plaintiffs have fixed every pleading defect identified by the Court and refuted all of Facebook's supposed bases for dismissal. As a result, Plaintiffs respectfully request that the Court deny Facebook's motion to dismiss Plaintiffs' FAC.

Dated: August 11, 2011

Respectfully submitted,
NASSIRI & JUNG LLP

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

Dated: August 11, 2011

Respectfully submitted,
EDELSON MCGUIRE, LLP

/s/ Sean Reis _____
Sean Reis
Attorneys for Plaintiffs and the Putative Class

Dated: August 11, 2011

Respectfully submitted,
ASCHENBRENER LAW, P.C.

_/s/ Michael Aschenbrener
Michael Aschenbrener
Attorneys for plaintiffs and the Putative Class