Paul R. Kiesel, Esq. (SBN 119854)
KIESEL BOUCHER LARSON LLP
kiesel@kbla.com
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
Interim Liaison Counsel

Edward D. Robertson, Jr.
Stephen M. Gorny
James P. Frickleton
Mary D. Winter
Edward D. Robertson III
chiprob@earthlink.net
BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
Fax: 913-266-2366
Interim Co-Lead Counsel

David A. Straite (admitted *pro hac vice*)
Ralph N. Sianni
Michele S. Carino
Lydia E. York
dstraite@stewartslaw.com
STEWARTS LAW US LLP
1201 North Orange Street, Suite 740
Wilmington, DE 19801
Tel: 302-298-1200
Fax: 302-298-1222
Interim Co-Lead Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

IN RE: FACEBOOK, INC. INTERNET TRACKING LITIGATION

Case No. 5:12-md-02314-EJD

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' CORRECTED FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Judge: Hon. Edward J. Davila
Date: October 5, 2012
Time: 9:00 a.m.
Crtrm.: 4

Trial Date: None

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

I. INTRODUCTION

Online advertisers and social media companies now track our every move over the internet and create remarkably detailed profiles that Professor Lori Andrews calls our alternative "digital selves." *See* Lori Andrews, "I know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy" (2012). Websites routinely place cookies on our computers when we surf the web, ostensibly to assist with identifying the user upon re-visits. Recently, however, these "tracking" cookies are being packaged with referrer headers and other information to track, in real time, our cyberspace destinations and the search terms we use to find them. Then our computers – usually without our knowledge – are programmed to transmit this data to aggregators for targeted advertising. That business model – part of Mark Zuckerberg's "Holy Grail" – becomes increasingly profitable the more data these companies gather about us. As U.S. Senator John Kerry said, "[t]hat's not just invasive – it's a little creepy." Sen. John Kerry, "We Need a Commercial Privacy Bill of Rights," *Think Progress Justice Blog* (Mar. 21, 2012).

Cookies were not originally meant for web tracking. Even Sir Tim Berners-Lee, the MIT researcher who helped to invent the web, expressed deep concern about the new practice. *See* Rory Cellan-Jones, "Web Creator Rejects Net Tracking," BBC News (Mar. 17, 2008). In 2009, researchers at the University of Pennsylvania and the Berkeley Center for Law and Technology released the first independent study on public reaction to being tracked online. They established that 66% of Americans were uncomfortable with web tracking. The number rose to 86% "when Americans are informed of three common ways that marketers gather data about people in order to tailor ads." *See* Joseph Turow, *et al*., "Contrary to What Marketers Say, Americans Reject Tailored Advertising" (Sept. 2009).

To offer citizens at least some fixed level of digital privacy and data protection, most of the developed world relies on a system of national (or even regional) government rules, often modeled on the European Union's Data Protection Directive.[1] The United States, in contrast, has no general

---

[1] *See* Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the (footnote continued)

national digital privacy or data protection law, and largely relies on a porous system of contract-based self-regulation. *See, e.g.*, Douglas Wood, "The Importance of Self-Regulation in Improving Digital Privacy," Corporate Counsel (July 10, 2012). Indeed, the very first principle of President Clinton's landmark 1997 *Framework for Global Economic Commerce* clearly states that "governments should encourage industry self-regulation and private-sector leadership." President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (July 1, 1997). Economic actors decide among themselves the extent to which privacy is to be protected. But the agreements are meaningless without enforcement. As President Clinton said, "[i]t is essential, therefore, to ensure personal privacy in the networked environment" and "consumers are entitled to redress if they are harmed by improper use or disclosure of personal information." *Id*. at Section II.5.

Forbes magazine recently noted that enforcement of our country's digital privacy self-regulation framework rests on a three-legged stool, consisting of federal enforcement by the Federal Trade Commission, state enforcement by States Attorneys General, and private enforcement largely in the form of privacy class actions. Kashmir Hill, "The FTC, 'Your Privacy Watchdog,' Does Have Some Teeth," *Forbes* (June 29, 2012). The FTC's enforcement efforts in this area are routinely mocked in the press[2] and in popular culture,[3], and of course State Attorney General efforts are limited to state laws that have largely not kept pace with the pace of technology. That leaves private enforcement as the

---

Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data; *see also* Australia's Privacy Act 1988 (amended in 2000 to cover the private sector broadly consistent with the EU Data Directive); Hong Kong Personal Data (Privacy) Ordinance, Ord. No. 81 of 1995 (amended June 27, 2012) (broadly consistent with the EU Directive); Japan's Personal Information Protection Law, Law No. 57 of 2003.

[2] *See, e.g.*, Peter Maas, "Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless," www.wired.com (June 28, 2012).

[3] *See, e.g.*, commentary by comedian Jon Stewart, host of "The Daily Show," noting on April 18, 2012 that a recent fine against Google, Inc. for stealing personal information leaking from home Wi-Fi routers would be less than the NFL fines players for doing a touchdown dance. Stewart also quipped, "Google, I am shocked. You stole people's personal information without their permission? That's Facebook's job."

most important of these three legs.

On July 2, 2012, Defendant Facebook asked this Court to dismiss the entirety of Plaintiffs' Complaint that demands Facebook be held accountable for its secret, unauthorized and purposeful tracking of its members' internet use. In the sections below, Plaintiffs respond to each of Facebook's early dismissal arguments. But Plaintiffs' necessarily claim-by-claim opposition should not obscure how extraordinary Facebook's request, taken as a whole, really is. Facebook asks this Court to hold as a matter of law that no legal remedy exists for the knowing, purposeful tracking of 150 million internet users (800 million globally) without their knowledge or consent. The impact of such a finding on the internet industry and society at large cannot be overstated. Why would any online or telecommunications company ever honor their contracts, terms of use or privacy policies ever again? Without enforcement, how can a system of regulation – let alone self-regulation - work? Facebook asks this Court to remove the third leg from the three-legged stool of privacy enforcement. That request should not be granted.

II. SUPPORTING FACTS

A. Facebook violated its own policies and the law.

Facebook's terms of use set not only the users' reasonable expectation of privacy, but also definitively limit the extent to which Facebook could permissibly track its users' internet activities. Facebook promised its members that it would not track their personal internet browsing history after they had logged-off of Facebook.[4] As noted in Plaintiffs' Corrected First Amended Consolidated Class Action Complaint ("FAC"), ¶16:[5]

[4] Mischaracterizing plaintiffs' pleading, which must be read as a whole, and overstating plaintiffs' burden at this initial pleading stage, Facebook's repeated claim that Plaintiffs rely exclusively on a single entry in Facebook's help center nonetheless underscores the centrality of that "single entry." A contractual promise is no less valid simply because it can be stated clearly on one sentence.

[5] References to specific paragraphs of the FAC hereinafter designated as "¶ ___."

1. **Facebook's online help center:** *Does Facebook use cookies if I don't have an account or have logged out of my account*?[6] "When you log out of Facebook, we remove the cookies that identify your particular account."

2. **Facebook's online help center:** *"How does Facebook use cookies?"* "We do not use cookies to create a profile of your browsing behavior on third-party sites or to show you ads..."

3. **Facebook's data use policy:** "We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plug-in). *This may include…if you are logged in to Facebook, your user ID*." (emphasis added).

4. **Facebook's privacy policy (April, 22 2010) – Facebook Exhibit C**: "Pre-Approved Third-Party Websites and Applications – In order to provide you useful social experiences off of Facebook, we occasionally need to provide General Information about you to pre-approved third-party websites and applications that use Platform at the time you visit them (*if you are still logged in to Facebook*)…*In addition, if you log out of Facebook before visiting a pre-approved application or website, it will not be able to access your information.* (emphasis added).

Facebook's own Engineering Director further assured the public that Facebook did not engage in post-log-out tracking: "We've said that we don't do it, and we couldn't do it without some form of consent and disclosure."[7]

But Facebook secretly did exactly that. Facebook disingenuously responds that its members "generally" authorize Facebook to set cookies. This case, however, is about much more then "the mere use of cookies." *See* Defendant's Motion to Dismiss at 6 (hereinafter "MTD at ___"). Facebook's contention belies basic tenets of privacy expectation. Facebook's logic is akin to saying that a photographer who shoots a supermodel in a studio has "general" permission to secretly photograph the model in private, without her knowledge and consent, and for the photographer's pecuniary gain. "General" permission to track while logged in does not permit Facebook to record a user's activity after log-out, then monetize that surreptitiously obtained data. This is the core of the

---

[6] Upon information and belief, Defendant's Exhibit D to the *Declaration of Sandeep Solanki*, entitled *Data Use Policy* from Sept. 23, 2011, provides a link to the exact help center page Plaintiffs cited in their complaint. Upon information and belief, Defendant's Exhibit C to the same Declaration, entitled *Privacy Policy* from April 22, 2010, does the same.

[7] Acohido, Byron, *How Facebook Tracks you across the Web*,USA TODAY, 11/16/11 *available* at http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1.

causes of action alleged in the FAC.

B. How Facebook Tracks Its Users

1. Cookies Generally

A server is a computer that stores data and makes that data available on the World Wide Web. A browser is a software application that allows a computer to access information on the World Wide Web. A cookie is a small text file created by a server. Some servers send cookies to their users' browsers when the user accesses the server. The browser stores the cookie in a directory on its computer.

Cookies often contain a unique identifier. They are helpful to servers because they allow the server to recognize the person or browser. When a user contacts a web server, the users' browser checks to see if that server has previously set any cookies on the users' computer. (¶ 39). If there were cookies set by that server, the users' browser sends those cookies back to the server. The server can then identify the exact person/browser accessing its server.

Cookies can be used to track and record specific information on the particular person/browser. For example, some companies set up data logs to record exactly when a person/browser accessed their server and exactly what they did on the server. Ordinarily, a server that has placed a cookie is only able to access that cookie if the user comes back to that same server. It would be the only time that the users' browser would recognize the server as matching the cookie on its machine.

2. Facebook's use of the "Like Button" and other Social Plug-ins to track users Internet browsing habits on websites other than Facebook.com

Facebook has crafted a way to gain access to its cookies even when a user is on non-Facebook websites. This information is invaluable to Facebook as it can then advertise that it knows what websites its users have visited, when they have visited them, and what precisely the user did on that particular web site. Facebook social plug-ins, including the Facebook "Like Button," are small symbols that appear on third-party web pages.[8] Social plug-ins allow users to share the content on

---

[8] The Like button has a thumbs-up symbol next to the word "Like," and users may click it in order to (footnote continued)

non-Facebook web pages with their Facebook friends. (¶60; MTD at 4, fn. 4).

Facebook uses social plug-ins to become aware of its users' internet browsing history on third-party sites. Facebook is able to do this by withholding the code for its social plug-ins from the servers that house them. Instead of giving the server the actual content, Facebook embeds a command in the social plug-in code that forces the user to contact Facebook's server directly in order to obtain the social plug-in code.[9]

The process works as follows. First, a user types in a web server's Uniform Resource Locator ("URL") and the user's browser sends a "GET" request to the web server in order to obtain the content of the web page they wish to view. This is shown as step 1 in the diagram below. The user's browser then checks to see if that particular web server has previously set any cookies on its machine. If it has, the user's browser sends the cookie from the user's machine along with the other information from the request to the first web server. Second, the web server sends the content of the web page to the user's browser, see step 2 in the diagram below, without the Facebook content because the web server does not have that content. Next, along with the content of the web page (minus the Facebook content), the web server sends an embedded command to the user's browser (which was created by Facebook) that automatically causes the user's browser to contact Facebook's server in order to receive the content for the Facebook social plug-in,[10] as shown in step 3 below. The user's browser sends that command to the Facebook server, the user's browser does the same browser check to see if the Facebook server has ever placed any cookies on the user's machine, the user's browser finds out that Facebook's server has placed cookies on the user's computer in the past and responds by sending the Facebook server the user's cookie information (that has been sitting in storage on the user's computer), along with all of the information from the electronic communication between the user and

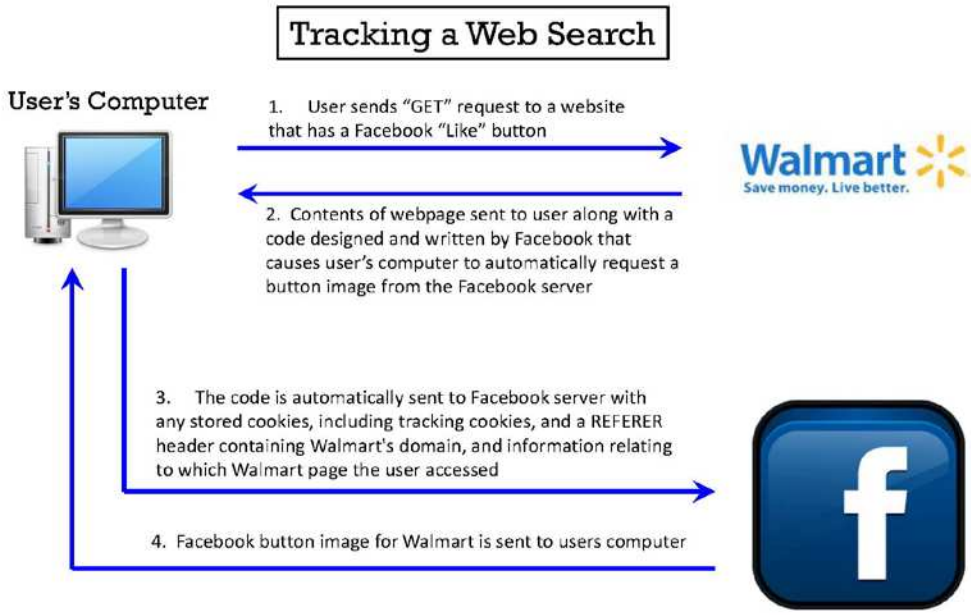
---

share their affinity for particular content with their Facebook Friends. See MTD at 4.

[9] When this happens, the user is completely unaware that they are interacting with Facebook's web server at any point. The command forces the users' computer to communicate with Facebook's server behind the computer screen where no user can see.

[10] Again, the user is completely unaware they are even interacting with Facebook's server.

the non-Facebook server.[11] Finally, Facebook logs this information and then sends the content of the Facebook social plug-in to the user's browser as shown in step 4 below, and the full web page shows up on the user's screen.[12] This process is illustrated below:



The practical implication of this system is that any time a user visits any website with a Facebook social plug-in, even though the user has no intention of sending information to or receiving

---

[11] In this scenario, because Facebook is actually a non-party to the communication between the user and the web server, the users computer (because of the command given it by Facebook in the HTML code) sends to the Facebook server the contents of the electronic communication between the user and the web server. The contents of the communication include, but are not limited to: the details of the communication (i.e. any purchases made, any comments posted, any links clicked on, etc.), the URL request from the user to the third-party website, the date of the communication, the time of the communication, the web address of the web pages clicked on, the identification of the content accessed on each page, the characteristics of the user's PC, mobile computer, cell phone, and browser, such as the IP address, universal device identifier ("UDID") on mobile devices, screen resolution, operating system and browser version.

[12] Facebook actually knows the content of the users' request to the third-party web server before the user even has a chance to see the full content of the page.

information from the Facebook server, the user is forced to interact with the Facebook server, without their knowledge or consent. When the user's browser interacts with the Facebook server, the browser sends to Facebook's server the cookies previously embedded by Facebook. These cookies contain personally identifying information. ***The browser also sends all of the content from the communication the user had with the web site***.

III. STANDARD OF REVIEW

Federal Rule of Procedure 8(a) only requires a plaintiff to plead each claim with sufficient specificity to "give the defendant fair notice of what the … claim is and the grounds upon which it rests." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal quotations omitted). *See also Skinner v. Switzer*, 562 U.S. ___, 131 S. Ct. 1289 (2011). (Rule 8(a)(2) requires only short and plain statement of plausible claim, not exposition of legal argument). "A complaint will survive a motion to dismiss when it contains sufficient factual matter, that when accepted as true, states a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662 (2009). Factual content is sufficient when it raises a right to relief above the speculative level. *Twombly,* 550 U.S. at 570; *see also Erickson v. Pardus*, 551 U.S. 89 (2007) (decided two weeks after *Twombly:* "[s]pecific facts are not necessary; the statement need only 'give the defendant fair notice of what the…claim is and the ground upon which it rests'"); *Starr v. Baca*, 652 F.3d 1202, 12 (9th Cir. 2011) (key pleadings tests are (i) "fair notice" of claim and (ii) allegations "sufficiently plausible" to warrant discovery). Facebook's detailed arguments show Facebook has fair notice of, and knows how to defend against, Plaintiffs' claims. Facebook's admission (MTD at 2-3, 5, 6, 11, 24, 26, 28, 34) that it promised *not* to follow users post-logout, and ultimately factual arguments about, for example, what is and is not a proscribed "intercept" under the Wiretap Act, demonstrates that putting Facebook "to the expense of discovery" is not "unfair." *Id.* A motion to dismiss a fraud claim under Rule 9(b) is the functional equivalent of a motion to dismiss under Rule 12(b)(6) for failure to state a claim. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1107 (9th Cir. 2003).

On a 12(b)(6) motion, the court accepts as true all of the complaint's factual allegations. *Twombly*, 550 U.S. at 555-56. The court must also construe those facts in the light most favorable to the plaintiff. *Love v. United States*, 915 F.2d 1242, 1245 (9th Cir. 1988). If dismissal is appropriate

under either Rule 12(b)(6) or (9)(b), the Court should grant leave to amend should unless the allegation of other facts could not possibly cure the defect. *Lopez v. Smith,* 203 F.3d 1122, 1130 (9th Cir. 2000); *Vess,* 317 F.3d at 1108.

IV. ARGUMENT

A. Plaintiffs' Allegations Confer Article III Standing.

1. Facebook's Statutory Invasions Give Rise to an Injury in Fact.

"The actual or threatened injury[13] required by Art. 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); *Edwards v. First American Corp.,* 610 F.3d 514, 516-517 (9th Cir. 2010), *cert. granted in part,* 131 S. Ct. 3022, 180 L. Ed 2d 843 (2011), *and cert. dismissed as improvidently granted,* No. 10-708, 2012 WL 2427807 (U.S. June 28, 2012); *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705, 711 (N.D. Ca. 2011); *see also Gaos v. Google Inc.*, 2012 WL 1094646 * 2 (N.D. Cal. Mar. 29, 2012) (Davila, J.). The standing question in such cases, like this one, is "whether the…statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *Id.* The FAC alleges that Facebook intercepted and tracked the electronic communications of each plaintiff in violation of various federal and state statutes.[14] These allegations establish "injury in fact" as a matter of law. *Id.*

Contrary to *Warth* and its progeny, Facebook asks the Court to engineer a "two-tiered injury-in-fact" standing test that requires not only the invasion of a statutory right, but some additional harm, presumably economic. But as *Gaos* properly recognized, *Warth* teaches that standing exists where, as here, the alleged invasion is to the plaintiff's own rights under the statute rather than to some generalized right. *Gaos,* at * 3. *Warth* and *Gaos* did not, as Facebook presupposes, require some

---

[13] Defendant concedes *sub silentio* that Plaintiffs have sufficiently pleaded Art. III causation and redressability.

[14] Count I (Wiretap Act), Count II (Stored Communications Act), Count III (Computer Fraud and Abuse Act), Count VIII (California Unfair Competition Law), IX (California Computer Crime Law), Count X (California Penal Code Invasion of Privacy Act), and Count XI (California Consumer Legal Remedies Act).

showing of additional harm, monetary or otherwise. *Gaos* held that the plaintiff had standing ***solely*** by virtue of a violation of the Stored Communications Act. *Id. In re Facebook* reached the same result. There, this Court found standing where plaintiffs had alleged a violation of the Wiretap Act. *In re Facebook,* 791 F. Supp. 2d at 711-12.[15]

Edwards, in which the plaintiff alleged a violation of the Real Estate Settlement Practices Act but did not allege any resulting monetary harm, makes the point. *Edwards,* 610 F. 3d at 516-17. The Ninth Circuit held that "the damages provision in RESPA gives rise to a statutory cause of action ***whether or not*** an overcharge occurred." *Id.* (emphasis added). Thus, the invasion of plaintiffs' statutorily protected rights establishes standing on its own, even absent additional allegations of harm. *Id.*

Just as in *Gaos,* Facebook cites no authority[16] holding that injury beyond a personal statutory violation is required to establish standing for a statutory cause of action. *See Gaos,* at *3. The allegations in the Complaint establish Article III standing.

2. <u>Plaintiffs Have Alleged Injury In Fact with Sufficient Specificity.</u>

Impliedly conceding that the invasion of statutory rights gives rise to injury in fact, Facebook retreats to challenging standing with fact based "inspecificity" arguments. (Facebook's MTD, 7-10).

---

[15] "If Plaintiffs' here are able to show that Defendant transmitted the contents of users' communications in the manner alleged, they will have effectively demonstrated that all…users…suffered the same injury, which will necessarily mean that each individual Plaintiff will have demonstrated that he was injured." 791 F. Supp. 2d at 711-712.

[16] Among many other distinctions: *In re JetBlue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y 2005), was a Rule 12(b)(6), not a Rule 12(b)(1) case. A Rule 12(b)(1) motion must clear a much higher hurdle. *See Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 907 (9th Cir.) (quoting *Lujan v. Nat'l. Wildlife Fed.*, 497 U.S. 871, 889 (1990). In *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), the plaintiffs did not allege they personally were affected by Defendant's practices violating specific statutes, and even so the court "probably would decline to say that it is categorically impossible for Plaintiffs to allege some property interest that was compromised by Defendant's alleged practices," but "at this point they have not done so." *DoubleClick*, a Rule 12(b)(6) case, did not address standing at all. *In re iPhone App. Litig*., 2011 WL 4403963 (N.D. Cal. Sep. 20, 2011), recognized that "statutory standing under the Wiretap Act does not require a separate showing of injury." In *Low v. LinkedIn Corp.*, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011), the plaintiff alleged only "'embarrass[ment] and humiliat[ion]'" from "'disclosure of his personally identifiable browsing history,'" which was "valuable personal property." *Id.* at *3. *Low* did not allege standing from the Defendant's invasion of his statutorily protected rights.

Facebook, however, ignores the longstanding rule that standing has nothing to do with the merits. *See, e.g., Warth,* 422 U.S. at 500 (standing "in no way depends on the merits" of claim of illegal conduct); *Bell v. Hood*, 327 U.S. 678, 682); *Maya v. Centex,* 658 F.3d 1068, 1068. General factual allegations suffice because the Court presumes "that general allegations embrace those specific facts that are necessary to support the claim. *Maya v. Centex,* 658 F.3d 1068, 1068 (citations omitted).[17] Thus, plaintiffs need only allege harm at this stage, not, as Defendant argues, ***prove*** it. *See, e.g., Steel Co. v. Citizens for a Better Env't,* 523 U.S. 83, 89, 94 (1998) (criticizing the dissent for an "attempt to convert the merits issue in this case into a jurisdictional one); *Maya*, 658 F.3d at 1068 (different degrees of evidence of standing required at different stages of litigation).

3. Plaintiff Davis' Litigation Cost's Establish Standing.

Defendant's suppositions about plaintiff Davis's consequential economic damages create at most a factual dispute not susceptible to resolution on a motion to dismiss, while further corroborating plaintiffs' numerous other bases for standing.[18]

B. THE FAC STATES FRAUD WITH PARTICULARITY.

Facebook claims that Rule 9(b) requires the dismissal of plaintiffs' § 502, UCL and CLRA claims. (MTD at 11). Fraud, however, is not an essential element under either the UCL or the CLRA. *See Comm. on Children's Television, Inc. v. Gen. Foods Corp.,* 35 Cal. 3d 197, 197 Cal. Rptr. 783, 673 P.2d 660 (1983) and *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097 (2003). Additionally, 9(b) requires only that in "all *averments of fraud* . . . , the circumstances constituting fraud . . . shall be

---

[17] *Maya v. Centex,* 658 F.3d 1060, 1067-68 (9th Cir. 2011), also found that the pleading standards enunciated in the 12(b)(6) cases of *Bell Atlantic Corp. v. Twombly,* 550 U.S. 544 (2007), and *Ashcroft v. Iqbal,* 556 U.S. 662 (2009), "are ill-suited to application in the constitutional standing context" because merits analysis is inapplicable for analyzing jurisdictional standing question. *See also In re Ins. Brokerage Antitrust Litig.*, 579 F.3d 241, 275 (3d Cir. 2009) "The named plaintiffs **only needed to allege** that they suffered an injury in fact and were not required to prove the merits of their case against the Gallagher Defendants to establish standing." (emphasis added)).

[18] *Native Village of Kivalina v. ExxonMobil Corp.*, 663 F. Supp. 2d 863, 877-78 (N.D. Cal. 2009) found plaintiffs had not alleged that any of the corporate defendants had caused the greenhouse gases that perhaps one day would require villager relocation. Plaintiffs' claims here are clearly more direct. Nor need plaintiff allege Art. III causation with the precision required to demonstrate proximate causation. *Id.*

stated with particularity." Fed. R. Civ. P. 9(b) (emphasis added). Rule 9(b) imposes no heightened pleading burden for non-fraud allegations. *Vess*, 317 F.3d at 1104. Where, as here, fraud is not the sole element of the claim, only the allegations of fraudulent conduct must comport with Rule 9(b), which plaintiffs' allegations do. *Vess*, 317 F.3d at 1105.

"Rule 9(b)…only requires the identification of the circumstances constituting fraud so that the defendant can prepare an adequate answer from the allegations." *Bosse v. Crowell Collier and Macmillan*, 565 F.2d 602, 611 (9th Cir. 1977). Asserting that the "who, what, when, where and how of the misconduct charged," is unpleaded (MTD at 11), Facebook ignores FAC ¶¶10-102, where plaintiffs document the who,[19] what,[20] when,[21] where,[22] and how[23] regarding Facebook's fraudulent conduct with great specificity. FAC ¶¶ 178 and 221 also specifically plead facts establishing reasonable reliance on the multiple false statements Facebook made in public pronouncements, policies, and in its privacy statements.

Facebook's argument that plaintiffs failed to plead reliance also fails because plaintiffs' allege that Facebook does not properly declare its privacy policies (FAC ¶ 97) and used a made-up word ("Honk") to circumvent P3P software protections. When exposed, Facebook simply said it no longer had a P3P privacy policy. *See* ¶ 100. It then re-engineered its privacy policy to a text statement that would allow it to set its cookies, thereby continuing to deceive the browsers, and ultimately, users. *See* ¶¶101-02. Users rely on their software to protect their privacy. Software relies on truthful statements from manufacturers. Plaintiffs have pled, in detail, the element of reliance.

---

[19] See ¶¶ 19 (Gregg Stefancik); 29 (Kent Matthew Schoen, Gregory Luc Dingle and Timothy Kendall); 33 (Kendall & Facebook).

[20] See ¶¶ 14 (Facebook conditions of membership & tracking cookies), 38-84 (how the tracking cookie methodology works).

[21] See ¶ 85, which alleges a long history of privacy abuses. Other dates abound in the complaint describing when discrete acts were taken.

[22] See ¶9 denoting the location of Facebook's company headquarters where it may be inferred the majority, if not the totality of the conduct at issue, was planned and executed.

[23] See ¶¶ 38-84. In this case the "what" and the "how" are almost synonymous.

An action based on the UCL "to redress an unlawful business practice 'borrows' violations of other laws and treats these violations, when committed pursuant to business activity, as unlawful practices independently actionable under section 17200 *et seq*. and subject to the distinct remedies provided thereunder." *Farmers Ins. Exchange v. Superior Court*, 2 Cal.4th 377, 383 (1992). Therefore, any other claim in the FAC can serve as the predicate unlawful practice for Plaintiffs' UCL claim.

C. THE COMPLAINT STATES A CLAIM UNDER THE WIRETAP ACT.

The "paramount object" of the Wiretap Act "is to protect effectively the privacy of communications." *Gelbard v. United States*, 408 U.S. 41, 48 (1972). Plaintiffs' FAC validly pleads a valid Wiretap Act Claim because its alleges: (1) Facebook's surreptitious tracking constituted an "interception;" (2) Facebook intercepted the "contents" of communications; (3) Facebook used a "device" to intercept; (4) Facebook was not a party to the intercepted communication; and (5) neither Plaintiffs nor third-party websites consented to interceptions while Plaintiffs were logged-off of Facebook.

1. <u>Facebook "Intercepted" Plaintiffs' Communications.</u>

The Wiretap Act defines "intercept" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4). Facebook, however, asks this Court to adopt an illogical definition of intercept supported by neither statute nor case law, or, failing that, to engage in technical fact finding at this pleadings stage. Facebook relies on *Konop v. Hawaiian Airlines, Inc.*, to define "intercept" to mean "to stop, seize, or interrupt in progress or course before arrival." MTD at 12, citing 302 F.3d 868, 874 (9th Cir. 2002). In *Konop*, the 9th Circuit rejected a Wiretap Act claim where plaintiffs alleged that defendant acquired information out of long term electronic storage on a secured website. The Ninth Circuit held that the "intercept" be made "contemporaneously" with the electronic communication and not while it is in electronic storage. The Court merely found that the dictionary definition of intercept, which Facebook now cites, supported that interpretation. The Ninth Circuit did not, however, usurp legislative authority and rewrite the statute to adopt the much more stringent non-statutory dictionary definition Facebook suggests. *Id*. at 878. Requiring that a Wiretap Act defendant "stop, seize or interrupt" a

communication would lead to absurd results, frustrating the purpose of the Act. Under Facebook's interpretation, a traditional police phone tap would not be qualify because there would be no stopping, seizing or interrupting and the telephone call would go through without delay.

The statute's clear terms only require an "acquisition of contents" and Plaintiffs' allegations concerning Facebook's use of persistent tracking cookies satisfy the intercept requirement. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 22 (1st Cir. 2003) (contemporaneity requirement may be inapplicable to Wiretap Act cases concerning electronic communications); *Mortenson v. Bresnan Communications, LLC*, 2010 WL 5140454 (D. Mont. 2010); *Chance v. Avenue A*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 513 (S.D. N.Y. 2001).[24] In *Pharmatrak*, the defendant placed cookies on the plaintiffs' computers to track their web usage on certain pharmaceutical websites. *Pharmatrak* at 13. Upon a plaintiff's first visit to one of the sites, a persistent cookie was placed on his or her computer. *Id*. On subsequent visits, the defendant used the cookie to relay the plaintiff's URL strings back to the defendant "simultaneous" to the plaintiff's transmissions to third-party websites. *Id*. at 22. The *Pharmatrak* Court held that "[e]ven those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception." *Id.*

Plaintiffs' FAC alleges the same scenario. Facebook obtains the intercepted information in real-time. ¶ 82. Facebook's receipt is at least contemporaneous, if not simultaneous with the request--

---

[24] This case is distinguishable from *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) in two very important ways. First, the *Doubleclick* court found it "important to note" that plaintiffs "can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways: (1) visiting the DoubleClick Web site and requesting an 'opt-out' cookie; and (2) configuring their browsers to block any cookies from being deposited." *Id*. at 504-05. In the instant case, neither of those options is available to the Plaintiffs because Facebook required tracking cookies to be deposited on users' computers as a condition of accessing its network while users were logged in; so, Plaintiffs could not block the Facebook cookies nor could the Plaintiffs op-out. More importantly, Facebook assured its users that it would not track them post logout and made affirmative representations that it would delete its tracking cookies when users logged out.

Second, the *Doubleclick* court also found it "important to note" that DoubleClick did not track individual users; but rather, "DoubleClick collects information based upon the computer's Web activity, regardless of whether one person or one hundred people happen to use that computer. In the same vein, if one person uses multiple computers, DoubleClick would be unable to identify and aggregate the person's activity on different computers." *Id*. at n. 7. In the instant case, because Facebook's tracking cookies are linked to individual users' accounts, Facebook did track individual users (including the Plaintiffs) and identified and aggregated their personal activity.

"Facebook actually receives this information before the content of the user's request shows up on the user's screen." ¶¶ 68, 80. As the Court stated in *Pharmatrak*, where the defendant "acquired the same URL query string (sometimes containing personal information) exchanged as part of the communication between the pharmaceutical client and the user", these "separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement." *Pharmatrak*, 329 F.3d at 22.[25] *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010), explained that "'contemporaneous' does not mean 'in flight' or 'in the middle' or any football metaphor." *Id.* at 706. The Court continued, "[t]here is no timing requirement in the Wiretap Act and judges ought not add to statutory definitions." Instead it is "contemporaneous by any standard" when the Wiretap defendant and the victims "receive[] each message with no more than an eyeblink in between." *Id*. *See also Councilman*, 418 F.3d 67 (Wiretap Act's "broad definition of electronic storage was to enlarge privacy protections for stored data…not to exclude email messages stored during transmission from those strong protections"). *Szymuszkiewicz* thus rejects a reading of interception that imports a timing requirement, and embraces a reading of "interception" that means "wrongfully took."

The same analysis applies to this case. The FAC plead an interception.

2. Facebook Intercepted the "Contents" of Communications.

The Wiretap Act defines "contents" to mean "information concerning the substance, purport, or meaning of the communication." 18 U.S.C. 2510(8). Plaintiffs' FAC (¶¶ 78, 79, 82, 84, 142) alleges the interception of eleven items with each communication: (1) URL strings, including the date and time of each page visited, (2) the identification of the contents accessed on each page, (3) the user's name, (4) age, (5) gender, (6) email address, (7) IP address, (8) universal device identifier, (9)

---

[25] *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1152-54 (C.D. Cal. 2007), does not change the result. (Facebook MTD at 12). That Central District of California case did not address persistent tracking cookies. Instead, it dealt with an e-mail re-routing and copying program. 567 F. Supp. 2d. at 1154. *Cf. United States v. Councilman,* 418 F.3d 67, 79 (1st Cir. 2005 (en banc) (finding an interception under the Wiretap Act where electronic communication is acquired "during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage.")

screen resolution, (10) operating system, and (11) browser. Ultimately, Facebook knows which websites its members visited, when they visited them, and what the member did there.

The interception of URL strings alone is the interception of "content." *United States v. Forrester*, 512 F.3d 500, 510, fn. 6 (9th Cir. 2008) (URL constitutes "content" because URL "identifies a particular document within a website that a person views and reveals much more information about a person's Internet activity"); *In re Application of the United States for an Order Authorizing the use of a Pen Register and Trap,* 396 F. Supp. 2d 45 (D. Mass. 2005) (URL constitutes "content" because the "substance" and 'meaning' of the communication is that the user is conducting a search for information on a particular topic."). Facebook cites no contrary authority.

URL strings for article pages reveal more content than URLs for search phrases. Consider the URL in the footnote below.[26] As with the search phrase, the URL string reveals the information the user is seeking. In addition, by simply following the link, one can see the full contents of the communication back to the user.

Brown v. Waddell is also instructive. 50 F.3d 285 (4th Cir. 1995). In that case, police investigators obtained permission to track telephone numbers of persons that were "paging" a criminal suspect. The officers also obtained "pager clones" which intercepted additional number codes, one of which indicated that the caller was "en route." *Id.* at 287-88. The Fourth Circuit held that these additional numbers were "contents" under the Wiretap Act. *Id.* at 294. If numbers on a pager constitute "content," so too must actual words and numbers contained within a URL string.

Plaintiffs' FAC goes further than necessary, alleging Facebook intercepted more than just URL strings. The FAC also alleges the interception of URL strings commensurate with the long list of personally-identifiable information. *See, e.g.*, ¶ 82.

[26] http://www.washingtonpost.com/politics/fda-clears-first-over-the-counter-rapid-test-for-the-virus-that-causes aids/2012/07/03/gJQAONTsKW_story.html.

3. Facebook Used a "Device" to Intercept Communications.

The Wiretap Act defines an "electronic … device" broadly as "any device or apparatus which can be used to intercept a[n] … electronic communication." 18 U.S.C. §2510(5). The ordinary meaning of "device" is "a thing made for a particular purpose" or "a plan or scheme for effecting a purpose." Random House Dictionary 2012.[27] As a matter of law, web servers and computers are "devices." *See Szymusziewicz* at 707; *see also In re Pharmatrak* at 18-19. No court has ever found that servers, browsers, cookies, or any schemes using them to intercept communications are not "devices." Plaintiffs' FAC identifies at least seven devices Facebook uses to illegally track users post log-out: (1) cookies; (2) browsers; (3) computers; (4) Plaintiffs' servers; (5) Facebook's servers; (6) the plan or scheme Facebook put together to effect its purpose of tracking users while logged-off; or (7) a combination of all of the above. FAC ¶ 38-84. Plaintiffs have properly pled the "device" element.

4. Facebook Was Not a Party to the Intercepted Communications.

Facebook also argues its secret, post-logout tracking justified. Facebook says it was a party to the communications between its members and third-party websites since plaintiffs' browsers transmitted communications to Facebook. MTD at 15. But Facebook's reliance upon *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011) is misplaced. Here, plaintiffs have not alleged that Facebook intercepted communications while plaintiffs were ***on*** Facebook.com or even while they were surfing the web while ***logged-in*** to Facebook. Instead, the FAC alleges Facebook tracked plaintiffs when they were ***logged-off***, at a time when Facebook promised it would not intercept its members's communications with other websites and at a time when its members did not intend to send ***any*** messages to Facebook. It is illogical (and contrary to how courts have interpreted the law) for Facebook to secretly track its members and then claim it was a "party" to any communication. *In re Apple iPhone Application Litigation*, Case No. 11-MD-02250-LHK, *Order Granting in Part and Denying in Part Defendants' MTD* at 22. (where plaintiffs had not intended any

[27] http://www.dictionary.reference.com/browse/device

communication, a Wiretap Act defendant like Apple "cannot manufacture a statutory exception through its own accused conduct"); *see also Pharmatrak* at 22.

5. Neither Plaintiffs Nor the Third-Party Websites They Visited "Consented" to the Interceptions.

a. The question of consent is not appropriate for a motion to dismiss.

Found separately in 18 U.S.C. §2511(2)(d), the consent exception is an affirmative defense that Facebook bears the burden of establishing. *See Pharmatrak*, 329 F.3d at 19. Thus, it is not appropriately the subject of this motion to dismiss.[28] *Scott v. Kuhlmann*, 746 F.2d 1377, 1378 (9th Cir. 1984) (citing Wright & Miller, *Federal Practice and Procedure*, § 1277 at 328-30) (affirmative defenses may not be raised in a motion to dismiss unless there are no disputed issues of fact); *Conway v. Geithner*, 2012 WL 1657156, at *2 (N.D. Cal. 2012) (citing *Kuhlman* for the same proposition). Facebook's argument boils down to the remarkable proposition that the FAC does not disprove Facebook's factually based affirmative defense. No Rule 12(b)(6) cases support such a distortion of plaintiffs' burden.

b. Facebook's Members Traded Limited Tracking Rights (while logged-in) in Exchange for Facebook's Service; Members Did not Consent to Post Log out Privacy Intrusions.

Consent "should not be casually inferred." *Pharmatrak*, 329 F.3d at 20. A medical patient may consent to one form of treatment and refuse another. A landowner may consent to one trespass but not another. So too may a web user consent to one cookie function but not another. *Id*. at 19. Emphasizing the factual nature of the inquiry, determining consent is, thus, a two-part inquiry. First a court must determine the "dimensions of consent." *Id*. Then it must "ascertain whether the interception exceeded those boundaries." *Id*. Facebook's argument improperly infers consent for *all* tracking based upon a narrow consent agreement it reached with its members for *limited* tracking

[28] Even when a Defendant can prove consent, the Plaintiff may overcome such a showing by proving an exception to the exception – that the interception was done for the "purpose of committing any criminal or tortious act." 18 U.S.C. §2511(2)(d).

during Facebook sessions. The FAC, however, details the boundaries of the plaintiffs' consent. *See* ¶¶ 16, 17, 21, 25, 86-102, 140, 141.

Even Facebook's hand-selected documents permit the reasonable inference that plaintiffs did not consent to tracking after log out, and that discovery will produce further evidence of lack of consent. The privacy policies of both April 22, 2010 and December 22, 2010 promised users that Facebook would not disclose information about them to "pre-approved" third-party websites after log-out. See Facebook Exhibit C at 4 ("if you log out of Facebook before visiting a preapproved application or website, it will not be able to access your information"). Facebook's own Engineering Director admitted, in regards to post log-out tracking, "*we couldn't do it without some form of consent and disclosure*."[29] The FAC alleges the absence of that consent, justifying discovery on this highly fact intensive inquiry.

c. Facebook Improperly Asks the Court to Consider Incomplete Evidence Outside the Pleadings.

At this pleading stage, Facebook directs the Court to certain hand-selected, incomplete evidence. Facebook, however, has failed to provide the Court with all documents describing its relationship with the plaintiffs. For example, Facebook neglected to provide the Data Use Policy that governed Facebook's relationship with its members between December 22, 2010 and September 23, 2011 – a full nine months of the class period.[30] Moreover, Facebook also failed to provide its Help pages—the very representations explicitly assuring its members that Facebook would not track them post- logout.

---

[29] See http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1. Plaintiffs regret the use of newspaper accounts in this response, but are given little choice since Facebook has moved to dismiss on the issue of consent before Plaintiffs have had the opportunity to conduct discovery.

[30] This document was used as an Exhibit by Facebook in *Ung v. Facebook*, a privacy case in this district in which Facebook was represented by the same counsel. 2011-CV-02829. Formal discovery may reveal other undisclosed policies.

In a misguided effort, Facebook provides CNN.com's publicly available Privacy Policy[31]. But CNN is just one of thousands of third-party websites that Facebook members visit. To prevail at this early juncture, Facebook must prove consent on the part of every website, not just a select one like CNN.com. Importantly, at this threshold stage, Plaintiffs cannot ascertain how many other documents exist between Facebook and CNN – or any of the other thousands of third-party sites –relevant to the issue of third party consent. Plaintiffs should have the opportunity to conduct discovery on affirmative defenses Facebook has raised to that the trier of fact can assess the matter. The issue of consent is not ripe for consideration.

d. Third Party Web Sites, including CNN.com, Did Not Consent.

Even if it were proper to treat Facebook's motion as one for summary judgment, Facebook has provided no evidence that ***any*** third-party web site consented to Facebook's tracking of logged-out members, let alone that ***all*** of them consented. In fact, the lone third-party privacy policy Facebook provides disproves its own argument. Facebook's Exhibit A to the *Declaration of Kyle C. Wong*, CNN.com's online Privacy Policy, states that "the use of these technologies by these third parties is subject to their own privacy policies and is not covered by this privacy statement." CNN.com's privacy policy thus defers to Facebook's privacy policy for all issues regarding the use of cookies. Because Facebook's privacy policies prohibit the use of cookies to track personal browsing history after logout, CNN.com's privacy policy gives Facebook no greater freedom to do so. Indeed other third-party web sites have privacy policies similar to CNN.com which preclude post log-out tracking.[32]

---

[31] This policy was only applicable to a limited part of the class period.

[32] Washington Post's online Privacy Policy: "If personally identifiable information is being provided to and/or maintained by any company other than these, our policy is that we will not transfer that personally identifiable information unless notice is given prior to transfer." *Available at* http://www.washingtonpost.com/privacypolicy/2011/11/18/gIQASIiaiN_story_1.html. The New York Times online Privacy Policy states, "if you have registered to use the NYT Services, we will not sell, rent, swap or authorize any third party to use your e-mail address or any information that personally identifies you without your permission." *Available at* http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html#e.

e. Consent Cannot be Inferred from Product Use.

Facebook also argues that third-party web site operators consented to post log-out user tracking because they chose to implement Facebook's social plug-ins and this supposed consent was amorphously "part of the regular process by which third-party websites obtain Facebook content to display on their page." MTD at 15. However, consent cannot be inferred (particularly at this stage) from the mere use of a product or the creation of a business relationship. *See Pharmatrak,* 329 F.3d at 20. Facebook cites three cases for its argument. All are distinguishable and none establish such a rule.[33]

As in *Pharmatrak,* there is before this Court no evidence that third-party websites were aware that Facebook was using social plugins to facilitate tracking in direct contravention of its privacy policy. Further, Facebook's Statement of Rights and Responsibilities includes a provision "applicable to developers/operators of applications and websites" requiring third-party websites to promise that they will "not give (Facebook) information that (they) independently collect from a user or a user's content without that user's consent."(Facebook Exhibit A, at 3). Accordingly, if third-party websites agreed to Facebook's post log out tracking, those websites breached their contract with Facebook and have subjected them to liability from their own visitors and users. Just as in *Pharmatrak,* there is no basis to find that third-party web sites consented to Facebook's interceptions. That is a factual determination that must await discovery.

D. THE COMPLAINT STATES A CLAIM UNDER CALIFORNIA'S INVASION OF PRIVACY ACT, PENAL CODE § 631.

The California legislature wrote California's Invasion of Privacy Act (CIPA) broadly to "protect the right of privacy" from "advances in science and technology… and the development of

---

[33] Unlike *In re Toys 'R' Us, Inc., Privacy Litigation,* 2001 WL 34517252, at * 7 (N.D. Cal. Oct. 9, 2001) the FAC includes no allegations that suggest such collaboration beween third-party websites and Facebook. Further, Facebook's reliance on *In re Doubleclick, Inc., Privacy Litigation,* 154 F. Supp. 2d 497 (S.D. N.Y. 2001) and *Chance v. Avenue A, Inc.,* 165 F. Supp. 2d 1153 (W.D. Wa. 2001) is equally misplaced. As the *Pharmatrak* Court stated "*Doubleclick* and *Avenue A* do not set up a rule contrary to the district court's reading of them, that a consent to interception can be inferred from the mere purchase of a service, regardless of circumstances." *Pharmatrak,* 329 F.3d at 20.

new devices and techniques…." Cal. Penal Code § 630. The Act must be interpreted with this purpose in mind. To further this objective, the Act prohibits "any unauthorized connection" or any attempt to read or learn the contents of any communication by means of "any machine, instrument or convenience, or in any other manner." Plaintiffs have averred that Facebook used technology to "access, intercept and collect Plaintiffs' and Class Members' personally identifiable information and . . . interactions with certain websites after log-out . . ." *See* ¶200. Intentionally, see ¶130, Facebook "directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiffs, Class Members and California-based web entities" without consent. *See* ¶¶ 103-106, 203, 204 and 208. These allegations provide fair notice of the nature of Plaintiffs § 631 claim.

1. The Statute Was Designed to Cover Advances in Technology, Which Include Electronic Communications.

Facebook asks this Court to be the first to hold that the Act excludes electronic communications. Not only is this request contrary to the statute's purpose and terms, but it is contrary to established law as well. For instance, in *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011), customers of an internet service provider alleged that the defendants monitored their online activities in violation of § 631. The Court overruled a motion to dismiss, explaining that the case arose "out of a practice of tracking individuals' internet habits and harnessing that data to sell and deliver targeted advertisements based on their web browsing history." *Id*. at 1024. The data retrieved "was used to sell advertising tailored to subscribers' interests…." These allegations are virtually identical to Plaintiffs' allegations against Facebook. *See* ¶¶ 12-14, 31, 200.

The authority Facebook cites for this unprecedent concept is inapposite. For example, *People v. Suite*, 101 Cal. App. 3d 680 (1980) and *Tavernetti v. Super. Ct.*, 22 Cal. 3d 187 (1978) involve the suppression of telephone evidence in a criminal matter and pre-date the entire issue of internet communications by several decades. *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855 (N.D. Cal.

2011), did not even involve the CIPA.[34]

2. Plaintiffs Did Not Know Facebook Was Tracking Them; Therefore Facebook was not a Participant to the Communication.

Facebook claims it is a party to the electronic communication such that § 631 does not apply. The authority Facebook cites, however, shows otherwise. *Rogers v. Ulrich*, 52 Cal. App. 3d 894 (1975) and *Warden v. Kahn*, 99 Cal. App. 3d 805 (1979) simply hold that eavesdropping cannot occur when the aggrieved party knows that someone is listening: "only a third party can listen secretly to a private conversation." *Rogers*, 52 Cal. App. 3d at 899. Here, Plaintiffs allege that Facebook (a third-party) tracked Plaintiffs' internet browsing activity — communications with other websites — after they were logged out of Facebook without plaintiffs' knowledge and consent. *See* ¶¶ 15-37, 71-84. This factual scenario states a claim pursuant to § 631.

3. Plaintiffs' Allegations Satisfy the Statutory Prerequisites.

Facebook asserts that Plaintiffs fail to allege (1) the use of a "machine, instrument or contrivance"; (2) that Facebook made an "unauthorized connection with any telegraph or telephone wire, line, cable or instrument"; and (3) that Facebook obtained the "contents" of any communication. MTD at 18. First, a computer is a machine. A cookie is a "contrivance," which is defined as "a device, especially a mechanical one" and separately as "a plan or scheme." Plaintiffs' FAC ¶ 42 alleges that Facebook "implants a number of cookies onto the internet user's computer." The cookie is software that carries an electronic plan that allows Facebook to participate in communications between users and others. These allegations are sufficient.

The words "connection" and "contents" are similarly broad. Plaintiffs' FAC ¶¶ 103-106, 203, 204 allege an unauthorized connection. "[P]ersonally identifiable information and other data, including information concerning their interaction with certain websites" is "content." *See* ¶ 200.

---

[34] Facebook also cites *Lacourt v. Specific Media*, No. SACV 10-1256-GW, 2011 WL 1661532 C.D. Cal. Apr. 28, 2011), in which the Court comments that application of the Invasion of Privacy Act to the conduct alleged was not "obvious." (Facebook's MTD at 17). Since the Court granted leave to amend and did not comment on why it believed the allegations failed to state a claim, this remark is not particularly instructive.

4. Plaintiffs Aver that Facebook Knew The Contents Of The Data It Retrieved

Facebook tracked users' browsing history and used what it learned to increase advertising revenue. See ¶¶ 12-14, 200. Use of the data requires knowledge of its content. Otherwise, it would have no value.

E. THE COMPLAINT STATES A CLAIM UNDER THE STORED COMMUNICATIONS ACT.

"[T]he Stored Communications Act protects individuals' privacy and proprietary interests." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004). It provides a cause of action against:

> a person who intentionally accesses without authorization a facility through which an electronic communication service is provided, or who intentionally exceeds an authorization to access that facility, and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in storage in such a system.

18 U.S.C. § 2701(a)(1). The statute "was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address." *See Crispin v. Christian Audiger, Inc.*, 717 F. Supp. 2d 965, 971 (C.D. Cal.) (citations omitted). The SCA is best interpreted "by considering its operation and purpose in light of the technology that existed in 1986." *Id*. at 972 n.15.

Facebook argues that the Complaint fails to allege that it accessed a "facility" and took communications from "electronic storage" and that it nevertheless had authority to do so. When Facebook tracks a member's internet browsing history, the user's browser conversation is captured and ultimately transmitted to Facebook, wherein Facebook stores the information permanently. Such electronic storage as the SCA contemplates includes retaining an email on a server after delivery to the recipient. *Doe v. City and County of San Francisco*, No. C10-04700 TEH, 2012 WL 2132398, *2 (N.D. Cal. Jun. 12, 2012). Thus, turning temporary information into a permanent record on a third party's facility is exactly the type of privacy invasion the SCA seeks to prohibit.

The SCA does not define "facility." However, "Congress intended the term to include the physical equipment used to facilitate electronic communications." *Council on Am.-Islamic Relations*

Action Network, Inc. v. Gaubatz, 793 F. Supp. 2d 311, 334 (D.D.C. 2011). Here, Plaintiffs allege a detailed system of communications between and among numerous physical means of communication, including the user's hardware, browser and the Facebook server, which result in Facebook obtaining information the SCA prohibits. *See* ¶¶ 38-84. Regardless, discovery is appropriate to further allow plaintiffs to further demonstrate how these physical means of communication constitute a "facility." *Gaubatz*, 793 F. Supp. 2d at 336 (denying a motion to dismiss because defendants' argument that plaintiffs' own office computers are not a facility "may or may not turn out to have merit upon further development of the factual record").

Impliedly conceding that the Act covers its conduct, Facebook retreats to the position that it had permission to violate the Act. This argument is belied by the very assurance Facebook gave to its customers. *See* ¶ 15. Consent to place cookies and track members during log-in in exchange for Facebook access is not tantamount to consent to secretly use those cookies in a manner in which the terms of use prohibited.

F. THE COMPLAINT STATES A CLAIM UNDER PENAL CODE § 502 (COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT)

By enacting § 502, the California legislature expanded the protection afforded to individuals from unauthorized access to both their personal computers and individual data. Cal. Penal Code § 502(a). Pursuant to Section 502 (e)(1), any person who suffers "damage or loss by reason of a violation of any of the provisions of subdivision (c)…" may bring a civil action against the violator. Plaintiffs have asserted claims pursuant to Sections 502(c)(1), (6), and (7) which require allegations that Facebook accessed their computers or data "without permission." Plaintiffs also assert a claim pursuant to Section 502(c)(8), which requires allegations that Facebook introduced a "contaminant" into their computers. Facebook argues that Plaintiffs have not alleged (1) the absence of permission, (2) unlawful access, (3) that Facebook tracking cookies are contaminants, and (4) cognizable damages.

1. The Allegations Show Facebook Tracked Post-Logout Without Permission.

Plaintiffs allege that Facebook lacked permission to keep tracking cookies on Plaintiffs' computers after logout, see ¶¶ 16, 19, and to access those cookies when Plaintiffs visited third party web sites after logout. *See* ¶¶ 17, 20-25, 103-106.

Facebook contends Plaintiffs consented to post-log out tracking because they generally consented to the use of use of cookies while logged in and "the Privacy Policy does not limit Facebook's use of cookies based on whether a User is logged in or not." *See* MTD at 15. Facebook's argument fails due to its admitted contrary assurances in its online help center. *See* section C.2, *supra*. To the extent Facebook argues that its privacy assurances should be interpreted differently, that is for the trier of fact to decide.

Facebook, like the burglar that found that door unlocked, further argues it cannot have acted "without permission" because it did not overcome any "technical or code-based barriers" to track users after log-out. MTD at 24. That argument is based upon the inapposite *Facebook, Inc. v. Power Ventures, Inc.*, No. C08-05780 JW, 2010 WL 3291750 (N.D. Cal. 2010). *Power Ventures* addressed the concern that web site operators such as Facebook could unilaterally change terms of service anytime, subjecting users to criminal penalties under § 502. *Power Ventures* instituted the "overcoming of technical barriers" requirement to limit criminal liability to users who knowingly gained unauthorized access.

However, *Power Ventures* does not apply where, as here, the web site operator Facebook violates its own published terms of service. As Facebook has argued elsewhere,[35] no notice is required to tell Facebook what Facebook itself has done.

[35] In *Facebook, Inc. v. ConnectU, LLC*, 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007), Facebook successfully argued during the motion to dismiss stage that ConnectU exceeded the terms and conditions of use and accessed Facebook "without permission." Facebook is judicially estopped from arguing a contrary position now.

2. The FAC Alleges that Facebook Unlawfully Accessed Plaintiffs' Computers and Data.

Section 502 defines access as "to gain entry to, instruct or communicate with the logical, arithmetical, or memory function resources of a computer…." § 502 (b)(1). This is exactly what Facebook did when it tracked its members post logout. Facebook's reliance upon *Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29 (2007) is misplaced because in *Chrisman* an on duty police officer used a police computer he had permission to use, to obtain information he was authorized to obtain. The Court found that the officer's actions were legal for these reasons. *Id*. at 35.

Unlike *Chrisman*, as soon as the Plaintiffs logged out, Facebook was on notice that its help center promise was operative and that Facebook ***no longer had permission*** to access Plaintiffs' computers. *See People v. Lawton*, 48 Cal. App. 4th Supp. 11, 14 (1996) ("permissible use of hardware to access impermissible levels of software is a violation of that section."); *see also Weingand v. Harland Financial Solutions, Inc*., 2012 WL 2327660, 2 (N.D. Cal. 2012) (denying motion to dismiss § 502 claim where terminated employee "received permission to access [employer's] computer system based on his representations that he sought to get his 'personal files' after his termination, but that he had no authority with respect to the additional files he accessed.").

3. The FAC Alleges that Facebook's Cookies are Contaminants.

Facebook argues that its cookies are not contaminants because they are "standard web browser functions." MTD at 26. However, a "computer contaminant" is "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." § 502(b)(10). The tracking cookies Facebook implanted on Plaintiffs' computers were designed and intended to transmit Plaintiffs' information back to Facebook without the owner's intent or permission. Facebook's tracking cookies are, therefore, "contaminants" within § 502(b)(10).

4. Damages and Losses.

Plaintiffs have pleaded damages and losses. *See* ¶¶ 109-129. Section 502(e)(1) also allows "compensatory damages," defined as "any expenditure reasonably and necessary incurred by the owner or lessee to verify that a computer system … or data was or was not altered, damages, or

deleted by the access." Plaintiffs have pleaded the aforementioned damages and loss which includes retaining a computer expert to investigate Facebook's unauthorized access to their computer systems and data, see ¶¶ 109-110, and paying for proactive measures designed to prevent Facebook from gaining unauthorized access to Plaintiffs' computers again. *See* ¶¶ 128-120.

G. THE FAC STATES A CLAIM UNDER THE UCL.

Facebook argues that Plaintiffs have not (1) suffered an economic injury, (2) pleaded with Rule 9(b) specificity,[36] (3) alleged a predicate violation, nor (4) satisfied the UCL's "unfair" prong. MTD at 27-29. Like the CLRA, the UCL's reach is broad and remedial. *See, e.g., Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 320 (2011) (citing Cal. Bus. & Prof. Code § 17200) ("The UCL prohibits, and provides civil remedies for, unfair competition, which it defines as 'any unlawful, unfair or fraudulent business act or practice.' Its purpose is to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services."). The UCL covers "anything that can properly be called a business practice and that at the same time is forbidden by law." *Id*. "[U]nder the UCL, standing extends to "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." *Id*. at 321-22.

1. <u>Plaintiffs Pled Economic Injury.</u>

Under the UCL, a plaintiff pleads an economic injury by alleging that he "enter[ed] into a transaction, costing money or property, that would otherwise have been unnecessary." *Kwikset Corp*., 51 Cal.4th at 323; *Southern California Housing Rights Center v. Los Feliz Towers Homeowners Ass'n*., 426 F. Supp. 2d 1061, 1069 (C.D. Cal. 2005) (plaintiff had standing under UCL "based on loss of financial resources in investigating this claim"). Plaintiffs pled economic injury, see ¶¶ 109-129, as well as out-of-pocket economic loss as a result of Facebook's conduct. See ¶¶ 109-110, 128-120.

2. <u>Plaintiffs Have Alleged a Predicate Violation.</u>

"The UCL also creates a cause of action for a business practice that is "unfair" even if not specifically proscribed by some other law." *Fraley v. Facebook, Inc*., 830 F. Supp. 2d 785, 812 (N.D.

---

[36] See discussion at IV B.

Cal. 2011). The Ninth Circuit approved two tests to determine whether a practice is unfair. *Id*. Under the balancing test, a court examines the impact of the unfair practice on the victim, balanced against the reasons, justifications and motives of the alleged wrongdoer. *See Rubio v. Capital One Bank*, 613 F.3d 1195, 1205 (9th Cir. 2010). Under the public policy test, Plaintiffs must show that Facebook's policy of tracking its users after logout "violates public policy as declared by specific constitutional, statutory or regulatory provisions." *Id*.

Under the balancing test, Facebook's practice is unfair because Facebook has no legitimate purpose (e.g. public safety, privacy preservation) to track Plaintiffs beyond their consent. Under the public policy test, it is a violation of both public policy and "Section 5 of the FTC Act" for Facebook to misrepresent its data collection as it did when it represented that tracking cookies would be deleted upon logout. *See* Notice of Federal Trade Commission, File No. 102 3185, ScanScout Inc., 76 FR 71564-01, 2011 WL 5592938 (November 18, 2011) (consent agreement settling alleged violations of federal law prohibiting the unfair deceptive practice of misrepresenting that consumers could prevent the company from collecting data about their online activities by changing their browser settings to prevent the implantation of cookies.).

H. THE COMPLAINT STATES A CLAIM UNDER THE CONSUMER LEGAL REMEDIES ACT.

Facebook argues that Plaintiffs are unable to assert a claim under the CLRA because: (1) Plaintiffs have not suffered damages; (2) Plaintiffs are not consumers; (3) the CLRA does not apply to software; and (4) Plaintiffs failed to plead with Rule 9(b) specificity. None of Facebook's arguments has merit.

Plaintiffs pled damages, including statutory damages. *See* ¶¶109-129. "California courts have recognized that 'damage' in CLRA parlance is not synonymous with 'actual damages,' and may encompass 'harms other than pecuniary damages.'" *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1111 (N.D. Cal. 2010) (disclosure of plaintiffs' personal information encompassed as damages under CLRA); *see also Motschenbacher v. R. J. Reynolds Tobacco Co*., 498 F.2d 821, 825 n. 10 & 11 (9th Cir 1974) (citing *Canessa v. J. I. Kislak, Inc*., 97 N.J. Super. 327, 351 (Law Div. 1967)) ("If there is value in it, sufficient to excite the cupidity of another, why is it not the property of him who gives it

the value and from whom the value springs?").

Plaintiffs are consumers because 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). The consideration for Facebook membership is the payment of personal information to Facebook. *See* ¶¶ 111-125. This personal information has value to Facebook;[37] it allows Facebook "to deliver ads" that are "valuable to advertisers" because it allows advertisers to "target [their] specific audience." Def. Decl. of Solanki, Ex. A, §§ 10-11. Because the CLRA is to be "liberally construed and applied" to protect consumers from "unfair and deceptive business practices," Cal. Civ. Code § 1760, the bartered for exchange of Plaintiffs' personal information in exchange for the use of Facebook's social networking service, falls within domain of the CLRA.

Facebook argues that the CLRA does not apply to software, but this position cannot be stretched to include any product or service that includes software as only one component of the product or service, otherwise the vast majority of goods and services whose use relates to software (i.e. automobiles, telephones, appliances, and all consumer electronics) would be exempt from the CLRA. Indeed, Facebook's cases cited in support of this proposition deal ***exclusively*** with the purchase of software. In *Ferrington v. McAfee, Inc.*, No. 10-cv-01455-LHK, 2010 WL 3910169 (N.D. Cal. Oct. 5, 2010), for example, the court held that virus protection software was not a "good" or "service" covered by the CLRA. *Id*. at 19; *see also In re Apple iPhone Application Litig*., No. 11-md-02250-LHK, 2011 WL 4403963 at 10 (N.D. Cal. Sept. 20, 2011) ("to the extent Plaintiffs' allegations are based *solely* on software, Plaintiffs do not have a claim under the CLRA" (emphasis added)), *rev'd on other grounds, In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2012 WL 2126351 at 10 (N.D. Cal. June 12, 2012).

Facebook sells a social networking ***service,*** not software, see ¶ 9, even if software is tangentially involved in the service. The CLRA covers Facebook's social networking service. Cal.

---

[37] Plaintiffs need not allege or prove their personal information had economic value they could trade on some market in order to sufficiently allege that they agreed to provide that information to Facebook during Facebook sessions in order to gain system access.

Civ. Code § 1761(b) ("'Services' means work, labor, and services for other than a commercial or business use, including services furnished in connection with the same or repair of goods."). Facebook has cited no cases to the contrary.

Finally, Plaintiffs have pled their claims with the requisite specificity, as set forth in section IV B, *supra*.

I. THE COMPLAINT STATES A CLAIM FOR CONVERSION.

Historically, "[c]onversion is the wrongful exercise of dominion over the property of another." *Farmers Ins. Exch. v. Zerin,* 61 Cal. Rptr. 2d 707, 709 (1997). A claim for conversion requires the plaintiff's ownership or right of possession at the time of the conversion, the defendant's conversion by a wrongful act of disposition of property rights and damages. *Burlesci v. Petersen,* 68 Cal. App. 4th 1062, 80 Cal. Rptr. 2d 704, 706 (1998).

Personal information is among the most important intangible property a person has in the digital age – the bits and bytes of digital data that identify us. Possession of personal information has value – to each of us as we exercise our interest in being known only to those we choose, and to others, who would utilize personal digital information to turn us into sources of profit.

Unsurprisingly, there is a trend to expand the reach of conversion beyond its hide-bound history:

> [The] conception that an action for conversion lies only for tangible property capable of being identified and taken into actual possession is based on a fiction on which the action of trover was founded—namely, that the defendant had found the property of another which was lost—and that such conception has become, in the progress of law, an unmeaning thing which has been discarded by most courts....

Annotation, *Nature of Property or Rights Other than Tangible Chattels Which May Be Subject of Conversion,* 44 A.L.R.2d 927, 929 (1955), quoted in *FMC Corp. v. Capital Cities/ABC, Inc.*, 915 F.2d 300, 304-05 (7th Cir. 1990) (recognizing the "modern trend of state law in protecting against the misuse of confidential business information through conversion actions" (citing *Annis v. Tomberlin & Shelnutt Associates, Inc.,* 195 Ga. App. 27, 392 S.E.2d 717 (1990) (affirming jury verdict for conversion of confidential information); *Conant v. Karris,* 165 Ill. App. 3d 783, 117 Ill. Dec. 406, 520 N.E.2d 757 (1987) (upholding a claim for the conversion of confidential information); *Datacomm Interface, Inc. v. Computerworld, Inc.,* 396 Mass. 760, 489 N.E.2d 185 (1986) (upholding damages

award for conversion of circulation list copy); *Kremen v. Cohen*, 337 F.3d 1024, 1033 (9th Cir. 2003) (recognizing conversion of intangible property). Thus, the modern trend recognizes that misuse of the confidential information becomes the gravamen of conversion, not the deprivation of property that had previously been the tort's hallmark.

Plaintiffs have alleged ownership or right to this specific personal information, its wrongful disposition and damages. *See Kremen* 337 F.3d at 1029.[38] This states a cause of action. *See id.*

J. THE COMPLAINT STATES A CLAIM FOR TRESPASS TO CHATTELS.

A claim for trespass to chattels based on accessing a computer system involves: (1) an intentional and unauthorized interference with the owner's possessory interest in the computer system; and (2) unauthorized use proximately resulted in damage to the owner. *eBay, Inc., v. Bidder's Edge*, 100 F. Supp. 2d 1058, 1070,1071 (N.D. Cal. 2000). California generally recognizes a trespass claim where the defendant exceeds the scope of the consent. *Id.* at 1071; *Baugh v. CBS, Inc.*, 828 F. Supp. 745, 756 (N.D. Cal. 1993) (even conduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to state a claim). In *Bidder's Edge,* the Court found that an unauthorized and intentional search of eBay's electronic database constituted a trespass to eBay's property. Similarly, Plaintiffs here allege an unauthorized and intentional use of their private information (names, account information, browsing history, purchasing habits) by Facebook and that they were damaged as a result, giving rise to liability. *See* ¶103-129; *see also* Restatement (Second) of Torts § 256 (1965).

K. THE COMPLAINT STATES A CLAIM FOR INTRUSION UPON SECLUSION.

An action for invasion of privacy by intrusion upon seclusion has three elements – (1) an intrusion into a private place, conversation, or matter, (2) in a manner highly offensive to a reasonable person, who (3) has a objectively reasonable expectation of seclusion or solitude in the place, conversation or data source. *Smith v. Capital One Fin. Corp*., 2012 U.S. Dist. LEXIS 66445, 8-9

[38] Facebook's argument that Plaintiffs consented to its post-logout tracking is addressed at section C.V., *supra*

(N.D. Cal. May 11, 2012). The intrusion need not be physical, *Deteresa v. American Broadcasting Cos., Inc*., 121 F.3d 460, 465 (9th Cir. 1997), but includes "unwarranted sensory intrusions such as eavesdropping, wiretapping, and visual or photographic spying." *Turnbull v. ABC*, 2004 U.S. Dist. LEXIS 24351, 35-36 (C.D. Cal. Aug. 19, 2004).

1. Plaintiffs Had Objectively Reasonable Expectation Of Seclusion Or Solitude.

As a matter of law, one has reasonable expectation of privacy in one's home computer. *See United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. Cal. 2007); *see also United States v. Peden*, 2007 U.S. Dist. LEXIS 61354 (E.D. Cal. Aug. 9, 2007); *Dietemann v. Time, Inc.* 449 F.2d 245 (9th Cir. 1971). Under certain circumstances, the expectation of privacy includes a workplace computer. *Sanders v. American Broadcasting Companies*, 20 Cal. 4th 907, 918 (Cal. 1999). Plaintiffs have sufficiently alleged that they had a reasonable expectation of privacy from electronic intrusion whether that activity took place at home or at work.

2. Intrusion Was In A Manner Highly Offensive To A Reasonable Person.

Facebook argues that "Plaintiffs fail to allege that Facebook used this [surreptitiously collected] information at all, let alone that it was used for an "offensive or improper purpose." Facebook conflates *what* was done with the information with *how* the information was obtained. Rather than engaging in "target advertising" or "routine commercial behavior," Plaintiffs have alleged that Facebook engaged in surreptitiously taking information it promised not to take. *See Taus v. Loftus*, 40 Cal. 4th 683, 751 (Cal. 2007) ("Wiretapping or surreptitious recording of conversations violates the rights of those wiretapped or recorded, because such intrusions violate well-defined expectations of privacy"); *Ribas v. Clark*, 38 Cal. 3d 355, 361 (Cal. 1985) ("[S]ecret monitoring denies the speaker an important aspect of privacy of communication -- the right to control the nature and extent of the firsthand dissemination of his statements"). Plaintiffs claim that Facebook surreptitiously obtained information reasonably thought by its members to be secure states a claim for intrusion upon

seclusion.[39]

L. PLAINTIFFS WITHDRAW THEIR CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT.

Plaintiffs withdraw their CFAA claim.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

---

[39] *See also Luken v. Edwards*, 2011 U.S. Dist. LEXIS 47545, 22-23 (N.D. Iowa May 3, 2011); *Cozzolino v. Maricopa County*, No. CV-04-2229-PHX-FJM, 2006 U.S. Dist. LEXIS 44567, 2006 WL 1794761, at *2 (D. Ariz. June 27, 2006)); *Amati v. City of Woodstock*, Ill., 829 F. Supp. 998, 1010-11 (N.D. Ill. 1993); *Fowler v. Southern Bell Tel. & Tel. Co.*, 343 F.2d 150, 156 (5th Cir. 1965); *Binkley v. Loughran*, 714 F. Supp. 776, 780 (M.D.N.C. 1989); *Cavallaro v. Rosado*, No. CV054009939, 2006 Conn. Super. LEXIS 2919, 2006 WL 2949143, at *4 (Conn. Super. Ct. Oct. 5, 2006); and W. Page Keeton et al., Prosser & Keeton on the Law of Torts § 117, at 884-85 (5th ed. 1984) (citing eavesdropping on telephone calls by wiretapping as an example for the tort of intrusion into the seclusion of another).

V. CONCLUSION

Privacy is a cherished right in this country. The law defines the parameters of privacy, recognizes its importance and provides remedies for its violation. Plaintiffs' FAC accuses Facebook of engaging in tortious, illegal conduct deliberately designed to violate those rights for the basest of reasons – profit. At this stage of the proceedings, plaintiff's factual allegations are held to be true. The FAC invokes the remedies provided for in the law, and plaintiffs have done all that is procedurally necessary to grant them the right to fully explore and prove the wrongs perpetrated by this defendant. As such, the Motion to dismiss must be denied.

DATED this 31ST day of July, 2012.

Respectfully submitted,

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.

/s/ *Edward D. Robertson Jr.*
Edward D. Robertson, Jr.
James P. Frickleton
Mary D. Winter
Edward D. Robertson III
11150 Overbrook Road, Suite 200
Leawood, KS 66211
chiprob@earthlink.net
Telephone: (913) 266-2300
Facsimile: (913) 266-2366
Interim Co-Lead Counsel

KIESEL BOUCHER LARSON LLP
Paul R. Kiesel, Esq. (SBN 119854)
8648 Wilshire Boulevard
Beverly Hills, CA 90211
kiesel@kbla.com
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
Interim Liaison Counsel

STEWARTS LAW US LLP

/s/ David A. Straite
David A. Straite (admitted *pro hac vice*)
Ralph N. Sianni
Michele S. Carino
Lydia E. York
1201 North Orange Street, Suite 740
Wilmington, DE 19801
dstraite@stewartslaw.com
Telephone: (302) 298-1200
Facsimile: (302) 298-1222
Interim Co-Lead Counsel

Stephen G. Grygiel
John E. Keefe, Jr.
Jennifer Harwood
KEEFE BARTELS LLC
170 Monmouth Street
Red Bank, NJ 07701
Telephone: (732) 224-9400
Facsimile: (732) 224-9494
sgrygiel@keefebartels.com
Plaintiffs' Steering Committee Member

Michael S. Schwartz
Mark S. Mandell
Zachary Mandell
MANDELL, SCHWARTZ & BOISCLAIR, LTD.
1 Park Row
Providence, RI 02903
msmandell@msb-atty.com
Telephone: (401) 273-8330
Facsimile: (401) 751-7830
Plaintiffs' Steering Committee Member

Barry R. Eichen
Daryl L. Zaslow
Tom Paciorkowski
EICHEN CRUTCHLOW ZASLOW & MCELROY LLP
40 Ethel Road
Edison, New Jersey 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273
beichen@njadvocates.com
Plaintiffs' Steering Committee Member

Stephen M. Gorny
BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
steve@bflawfirm.com
Telephone: (913) 266-2300
Facsimile: (913) 266-2366
Plaintiffs' Steering Committee Member

Andrew J. Lyskowski
Erik A. Bergmanis
BERGMANIS LAW FIRM, L.L.C.
380 W. Hwy. 54, Suite 201
P.O. Box 229
Camdenton, MO 65020
alyskowski@ozarklawcenter.com
Telephone: (573) 346-2111
Facsimile: (573) 346-5885
Plaintiffs' Steering Committee Member

William M. Cunningham, Jr.
Peter S. Mackey
Peter F. Burns
BURNS CUNNINGHAM & MACKEY PC
P.O. Box 1583
Mobile, AL 36633
wmcunningham@bcmlawyers.com
Telephone: (251) 432-0612
Facsimile: (251) 432-0625
Plaintiffs' Steering Committee Member

William H. Murphy, Jr.
Tonya Osborne Baña
MURPHY, FALCON & MURPHY, P.A.
One South Street, 23rd Floor
Baltimore, MD 21202
billy.murphy@murphypa.com
Telephone: (410) 539-6500
Facsimile: (410) 539-6599
Plaintiffs' Steering Committee Member

Margery S. Bronster
Robert Hatch
BRONSTER HOSHIBATA
1003 Bishop Street, Suite 2300
Honolulu, Hawaii 96813
mbronster@bhhawaii.net
Telephone: (808) 524-5644
Facsimile: (808) 599-1881
Special State AG Advisory Committee Member

Richard P. Ieyoub
Michael Reese Davis
L. J. Hymel
Tim P. Hartdegen
HYMEL, DAVIS & PETERSEN, LLC
10602 Coursey Blvd.
Baton Rouge, LA 70816
rieyoub@hymeldavis.com
Telephone: (225) 298-8188
Facsimile: (225) 298-8119
Special State AG Advisory Committee Member

Grant Woods
GRANT WOODS PC
Two Renaissance Square
40 N. Central Ave., Suite 2250
Phoenix, AZ 85004
gw@grantwoodspc.net
Telephone: (602) 258-2599
Facsimile: (602) 258-5070
Special State AG Advisory Committee Member

Mike Moore
MIKE MOORE LAW FIRM, LLC
10 Canebrake Blvd.
Suite 150 Flowood, MS 39232
mm@mikemoorelawfirm.com
Telephone: (601) 933-0070
Facsimile: (601) 933-0071
Special State AG Advisory Committee Member