COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
MATTHEW D. BROWN (196972)
(brownmd@cooley.com)
JEFFREY M. GUTKIN (216083)
(jgutkin@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Defendant
FACEBOOK, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

In re: Facebook Internet Tracking Litigation

Case No. 5:12-md-02314 EJD

DEFENDANT FACEBOOK, INC.'S REPLY IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFFS' CORRECTED FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT (FED. R. CIV. P. 12(b)(1) & 12(b)(6))

DATE:	October 5, 2012
TIME:	9:00 a.m.
COURTROOM:	4
JUDGE:	Hon. Edward J. Davila
TRIAL DATE:	None Set

Dockets.Justia.com

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

Plaintiffs' opposition to Facebook's motion to dismiss ("Opposition") is a public policy statement about social media companies and their online practices that distorts what Plaintiffs' sprawling 43-page Complaint[1] actually alleges. Only after several pages of discussion on the overall state of national and state privacy regulation and citation to over 20 outside sources (none of which are referenced in the Complaint) do Plaintiffs even mention their own lawsuit.

Nothing in Plaintiffs' Opposition changes the fact that, despite claiming an outlandish entitlement to between $15 billion and $1.5 trillion in damages, Plaintiffs have not pled facts sufficient to demonstrate Article III standing. Nowhere in the Complaint or the Opposition do Plaintiffs allege how they personally suffered injury as a result of Facebook's alleged conduct. Nor does the Opposition explain Plaintiffs' inability to plead fraud claims with particularity. In fact, as Plaintiffs tacitly concede, the Complaint does not identify any allegedly false or misleading statement from Facebook related to cookies that any named Plaintiff allegedly relied upon, or even saw. Facebook's Privacy Policy, by contrast, discloses that Facebook collects information when users visit third-party sites with Facebook features such as the Like button.

Plaintiffs seem keenly aware of the deficiencies in their pleading, attempting a factual "do-over" by adding a host of allegations that appear nowhere in (and sometimes contradict) the Complaint, and withdrawing their CFAA claim. But Plaintiffs cannot avoid dismissal by augmenting their pleading through the Opposition: when deciding the motion, the Court must, as a matter of law, disregard any allegations not found in the Complaint. Plaintiffs' abrupt abandonment of their claim under the CFAA—which they have asserted since the outset of this litigation—is also telling. This baseless claim is no outlier; every one of Plaintiffs' claims suffers from similar and equally fatal defects. The Court should dismiss the Complaint in its entirety.

II. CLARIFICATION OF FACTS BEFORE THE COURT

A. Unpled Allegations.

The Opposition adds a jumble of new factual claims that are not contained in, or

[1] Capitalized terms have the same meaning as in Facebook's Motion to Dismiss ("Motion") unless otherwise stated.

reasonably inferable from, the Complaint. Indeed, the Opposition's six-page fact section contains numerous new factual assertions but *only two citations* to the Complaint. Plaintiffs, of course, cannot cure the deficiencies in their pleading through the briefing process. *E.g.*, *Schneider v. Cal. Dep't of Corrections*, 151 F.3d 1194, 1197 n.1 (9th Cir. 1998) ("The 'new' allegations contained in the . . . opposition motion . . . are irrelevant for Rule 12(b)(6) purposes."); *Head v. Bd. of Trs. of Cal. State Univ.*, 2006 WL 2355209, at *4 (N.D. Cal. Aug. 14, 2006) ("Missteps in the complaint cannot be rescued by argument in the briefs.").

The new facts riddling the Opposition—some of which actually contradict allegations in the Complaint—include the following:

- That Facebook embeds code on third-party websites that "forces the user to contact Facebook's server directly" from the websites. (Opp. 6.) In contrast, the Complaint claims users contact Facebook's server because the third party, not Facebook, "includes some special HTML code in the HTML for the website," which triggers a request to Facebook. (¶¶ 60-62.[2])
- That "Plaintiffs could not block the Facebook cookies nor could the Plaintiffs op[t]-out." (Opp. 14.) The Complaint contains no such allegation; in fact, the Complaint references Facebook's Privacy Policy, which states exactly the opposite.[3]
- That cookies are software. (Opp. 23.) The Complaint, to the contrary, alleges that cookies are passive "text files," not executable files that take any action. (¶¶ 38-40.)

The Court should disregard these and all other factual allegations that are not in the Complaint.

B. Privacy and Data Use Policies.

As Plaintiffs admit in the Complaint, "[u]se of Facebook is governed by the Statement of Rights and Responsibilities and several other documents and policies, including a Data Use Policy and a Privacy Policy . . . . [These] governing documents reflect that users consent to Facebook installing cookies on each user's computer, and . . . users consent to these cookies tracking and transmitting data to Facebook regarding each user's web browsing . . . ." (¶ 16.)

Plaintiffs' various theories of harm are based on their conclusory contention that when Facebook allegedly "tracked [their] internet use post-logout," it did so without their consent. (¶¶ 103-06.) Plaintiffs quote from only a single source in their Complaint to support this

[2] All references to "¶ x" refer to paragraphs in the Complaint, unless otherwise noted.

[3] Plaintiffs' Complaint alleges that Facebook "circumvented web browsing privacy P3P code" for the Internet Explorer browser, but does not allege that this would prevent users from deleting or blocking cookies. Nor does the Complaint allege that any Plaintiff used Internet Explorer.

allegation: Facebook's online Help Center. (¶ 16.)[4] In their Opposition, Plaintiffs frequently repeat their citation to this Help Center page. (Opp. 3 & n.4, 4 & n.6, 26, 27.) Yet, nowhere in the Complaint (or Opposition) do Plaintiffs allege that the Help Center forms part of the agreement between Plaintiffs and Facebook. And, more fundamentally, Plaintiffs have never claimed that they relied on, or even saw, this Help Center page during the proposed class period.

Plaintiffs' Opposition newly asserts four statements not mentioned in the Complaint:

- An FAQ allegedly from Facebook's Help Center, entitled "How does Facebook use cookies?" that has nothing to do with differences between logged-in and logged-out cookie use or any other allegation in this case. (Opp. 4 (second item in list).)
- A disclosure from Facebook's Data Use Policy, which became effective *just three days before the end of the proposed class period*, which reads in full: "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 the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID." (Opp. 4 (third item in list).)[5]
- A disclosure from Facebook's April 22, 2010 Privacy Policy which indicates that Facebook might *provide* some user information *to* (rather than receive user information *from*) third-party websites if users were logged in to Facebook. (Opp. 4 (fourth item in list).) This disclosure is irrelevant because it relates to information Facebook may send to other websites in certain circumstances. (*See id.*)
- A statement by a Facebook engineer in an article dated two months *after* the close of the proposed class period. (Opp. 4.)

Once again, Plaintiffs do not allege they saw, let alone relied on, any of these statements. Indeed, given the timing of some of these statements, it would be impossible for class members to rely upon them during the vast majority of the class period, if at all.

III. ARGUMENT

A. Plaintiffs Lack Article III Standing (All Counts).

1. Plaintiffs Fail to Allege Personal or Economic Injury that Could Confer Standing.

Plaintiffs' Opposition appears to abandon any theory that the mere placement of cookies on their browsers injured them personally or economically, a theory rejected by numerous courts

[4] Plaintiffs complain that Facebook "failed to provide its Help pages" (Opp. 19), but it is Plaintiffs', not Facebook's, obligation to provide factual support for their claims.

[5] On December 22, 2010, Facebook introduced a slightly modified version of its April 22, 2010 Privacy Policy. (*See* Solanki Decl. I/S/O Reply, filed herewith, ¶ 2, Ex. A.) The December 22, 2010 Privacy Policy contains no material changes in Facebook's disclosures regarding the collection of data when users visit third-party sites.

in any case. *See, e.g.*, *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *1-2, *4 (N.D. Cal. Nov. 11, 2011) (holding "cookies" theory of harm "too abstract and hypothetical to support" standing); *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *1 (C.D. Cal. Apr. 28, 2011) (dismissing claim that "cookies" collected personal information for failure to allege injury).[6]

Plaintiffs' sole assertion of economic harm is a one-sentence argument, without any legal authority, that Plaintiff Davis's "Litigation Cost's [sic] Establish Standing." (Opp. 11.) But those "costs" do not show injury at all, let alone injury caused by Facebook. (Mot. 9.) Instead, they appear to be costs of preparing their suit: an expert retained "through counsel" to advise Davis "and counsel," and a subscription to a service to track Facebook's terms of use. (¶¶ 109, 126-29.) Plaintiffs never made these allegations in Davis's original complaint. And Plaintiffs do not allege that Davis paid the expert, only that the expert "was paid." Plaintiffs even concede that these are "Litigation Costs," but argue that such costs "Establish Standing." (Opp. 11.) But the law is clear that "a plaintiff cannot achieve standing to litigate a substantive issue by bringing suit for the cost of bringing suit." *Steel Co. v. Citizens for a Better Evn't*, 523 U.S. 83, 107 (1998).

Moreover, even if Davis herself paid for a service to track Facebook's terms of use, Plaintiffs must demonstrate that their alleged injuries are "fairly traceable" to Facebook's actions. (Mot. 9.) But how would Davis—who purportedly believes that Facebook does not follow its policies—benefit from tracking the language of those policies? If her fear is that Facebook does not follow its own policies, as Plaintiffs allege, then future, post-Complaint changes in the language would not matter. Plaintiffs do not address this logical fallacy, or dispute that Davis's costs cannot save the other Plaintiffs from dismissal. (*See* Mot. 10 n.11.)

2. Plaintiffs Fail to Demonstrate that any Statute Allegedly Violated Confers Standing.

Plaintiffs seek to demonstrate standing by noting that certain of their claims arise under

[6] Plaintiffs try to distinguish these cases because they did not premise standing on statutory violations, but Facebook cited them for the proposition that they defeat any allegation that "tracking" hurt the "value" of Plaintiffs' information (Opp. 10 n.16), which Plaintiffs cannot and do not dispute.

statutes containing private rights of action.[7] But Plaintiffs mischaracterize the law: no court has held that merely alleging a statutory violation satisfies the standing inquiry. Although injury in fact "may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing . . . Art. III's requirement remains: the plaintiff still must allege a distinct and palpable injury to himself" under the statute. *Warth v. Seldin*, 422 U.S. 490, 500-01 (1975) (internal quotations and citation omitted).

Courts find allegations of "distinct and palpable" injury only when, unlike here, the pleadings set out specific examples of harm to the plaintiffs. In *Gaos v. Google Inc.*, the complaint described how, when the plaintiff ran searches, Google allegedly transmitted the exact words of her searches (some of which included her name or names of her family members) to third-party websites. 2012 WL 1094646, at *3. The Court dismissed six of Plaintiffs' seven claims for failure to allege injury in fact, but found standing for the SCA claim because the plaintiff, by "explain[ing] how and by whom that disclosure was made," showed that under the SCA's private right of action "the injury she suffered was specific to her." *Id.* at *3, *6. Here, in contrast, Plaintiffs offer only general allegations of Facebook's conduct. Because they fail to provide a single example of a third-party website they visited, a communication that was "tracked," or other injury "specific to them," Plaintiffs lack standing.

Moreover, three of Plaintiffs' causes of action arise under statutes that require economic injury as an element of the claim. These statutes—§ 502, and the CLRA, and the UCL[8]—cannot "be understood as granting persons [who have suffered no economic injury] a right to judicial relief," and thus cannot confer standing here. *See Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010) (finding standing despite the lack of economic injury only "[b]ecause the statutory

[7] This argument plainly does not apply to Plaintiffs' claims under common law torts. Thus, the Court should dismiss, for lack of standing, Plaintiffs' claims for invasion of privacy, intrusion upon seclusion, conversion, and trespass to chattels without further consideration. *See Gaos v. Google*, 2012 WL 1094646, at *3-4 (N.D. Cal. Mar. 29, 2012).

[8] Cal. Penal Code § 502 (right of action for one who "suffers damage or loss by reason of a violation"); Cal. Civ. Code § 1780 (right of action for "[a]ny consumer who suffers any damage as a result" of the defendant's allegedly unlawful conduct"); Cal. Bus. & Prof. Code § 17204 (right of action for "a person who has suffered injury in fact and has lost money or property").

text does not limit liability to instances" where plaintiff is economically injured); *Boorstein v. Men's Journal LLC*, 2012 WL 2152815, at *3 (C.D. Cal. June 14, 2012) (no standing where statute "expressly require[d] an injury resulting from a violation"). Plaintiffs do not allege the economic injury elements of these claims, requiring dismissal with prejudice.

B. Plaintiffs Have Not Alleged Fraud with Particularity (Counts VIII, IX & XI).

Plaintiffs do not dispute that claims sounding in fraud must be pled with particularity. Plaintiffs assert, however, that if fraud is not the "sole element" of the claim, then only "allegations of fraudulent conduct must comport with Rule 9(b)." (Opp. 12.) That is not the law. Even claims that do not require a showing of fraud must still be pled with particularity when they are part of the same course of alleged fraudulent conduct. (Mot. 11 (citing *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009)).) Here, Facebook showed that Plaintiffs' claims under § 502, the UCL, and the CLRA are all based on the same allegations of an overarching "scheme to defraud," and thus must be pled with particularity in their entirety. (Mot. 11-12.)

The Complaint does not come close to meeting Rule 9(b)'s heightened pleading standard. For instance, it does not specifically describe the circumstances surrounding Plaintiffs' review of, or reliance upon, any alleged misstatements. *Kearns*, 567 F.3d at 1126. Though they cite to a few alleged misstatements, Plaintiffs never once claim that any of them actually saw, let alone relied upon, those statements. Plaintiffs simply ignore the case law Facebook cited that the inability to plead exposure to and reliance upon such misstatements is fatal under Rule 9(b).[9] *Id.*; *see also In re Facebook PPC Adver. Litig.*, 2010 WL 3341062, at *9 (N.D. Cal. Aug. 25, 2010) (holding Rule 9(b) not met where plaintiffs alleged certain misstatements but did not allege reliance on those statements with sufficient specificity).

C. Plaintiffs' Wiretap Act Claim Must Be Dismissed (Count I).

As Facebook demonstrated, Plaintiffs fail to allege an "interception" under the Wiretap Act of the "contents" of an "electronic communication" using a "device." Facebook further

[9] Similarly, regarding Plaintiffs' "P3P" allegations, none of them alleges they used a browser implementing the P3P protocols, reviewed any Facebook disclosures regarding P3P, or relied on any such disclosures before visiting third-party websites.

showed how the Wiretap Act carves out transmissions where the defendant had consent of either the sender or the recipient, and that Facebook had consent from both. While Plaintiffs cite a handful of out-of-circuit cases in response, their position contradicts the overwhelming weight of authority, including case law binding on this Court.

1. Plaintiffs Do Not Allege In-Transit "Interception."

Plaintiffs base their Wiretap Act claim on an incorrect understanding of what constitutes an "interception" in the Ninth Circuit, which has determined that an interception must occur *during transmission* of the intercepted message. The court stated that this rule was consistent with the dictionary definition of "intercept," which is to "stop, seize, or interrupt . . . ." (Mot. 12 (citing *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 874, 878 (9th Cir. 2002).) Plaintiffs ask this Court to ignore *Konop* because, they posit, this definition only means to "block," so something would not be "intercepted" unless it was prevented from "go[ing] through without delay." (Opp. 13-14.) But *Konop* made clear that "intercept" means acquiring ("seizing") a message *in transit*, not the blocking of that message. Plaintiffs offer no remotely plausible justification for this Court to disregard binding precedent.

As applied here, this "in transit" standard demands dismissal of the Wiretap Act claim. Plaintiffs allege that when their browsers access third-party websites with Facebook features, those websites display Facebook content that is not stored on the websites' own servers. To enable this display, the websites transmit code back to Plaintiffs' browsers that cause the browsers to send a second transmission to Facebook to trigger the loading of the Facebook features. (¶¶ 38-81; Opp. 6-7.) Plaintiffs argue that the second transmission is effectively a copy of, and thus an "interception" of, the first. But, even under Plaintiffs' theory, no communication was stopped, seized, or interrupted while in transit as the Act requires. *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (holding that even a scheme to immediately forward exact copies of communications did not "intercept" them while in transit).

Plaintiffs do not dispute that they fail to allege that Facebook intercepted any communication while it was in transit. Instead, they argue that no such allegation is necessary, because the First Circuit has held that "separate, but simultaneous and identical communications"

are enough. (Opp. 15 (citing *In re Pharmatrak, Inc.*, 329 F.3d 9, 22 (1st Cir. 2003)).[10]) Even under the *Pharmatrak* standard, Plaintiffs' claim would be dismissed because they allege communications that are neither "identical" nor "simultaneous": Plaintiffs allege first a transmission to a third-party website, then a subsequent transmission to Facebook that contains additional information. (¶¶ 38-81.) But *Pharmatrak* is not appropriately followed here in any case. First, the case relies upon outdated statutory language. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) (*Pharmatrak* not persuasive because it relies upon Supreme Court case interpreting statutory language that Congress removed from current statute). Second, the case criticizes the Ninth Circuit's approach to interpreting the Wiretap Act, which this Court is bound to follow. *Pharmatrak*, 329 F.3d at 21 (concluding that the Ninth Circuit's distinction "between materials acquired in transit, which are interceptions, and those acquired from storage, which purportedly are not . . . may be less than apt")).[11] The Court should decline Plaintiffs' invitation to ignore on-point Circuit precedent.

Similarly, Plaintiffs rely on *United States v. Szymuszkiewicz*, in which the Seventh Circuit acknowledged that the Ninth, Fifth, Third, and Eleventh Circuits interpret the Wiretap Act to impose timing requirements for interception, but declined to adopt such an approach.[12] 622 F.3d

---

[10] Plaintiffs also argue that *DoubleClick* is distinguishable because the plaintiffs there could have avoided tracking by requesting an opt-out cookie. (Opp. 14 n.24.) But as Facebook's Privacy Policy clearly disclosed, Plaintiffs can avoid "tracking" by blocking or deleting the cookies they object to. (Solanki Decl., Ex. A at 2 ("You can remove or block cookies using the settings in your browser . . . .").) Plaintiffs also argue that DoubleClick tracked computers' web activity, rather than tracking individual users. But the same is true here of Plaintiffs' allegations. Plaintiffs allege that Facebook's "datr" cookie identifies browsers, not individual users. (¶ 83.)

[11] The Ninth Circuit has stated that under the Wiretap Act and the SCA, electronic communications may be acquired only in one of two states: "during transmission," or from "electronic storage." *Konop*, 302 F.3d at 878 n.6. An "interception" under the Wiretap Act occurs only in the "very short" period where an electronic communication "travels across the wires at the speed of light." *Id.* at 878 & n.6. Otherwise, the communication is acquired under the SCA from "electronic storage." *Id.* at 879. The length between transmissions is immaterial; "milliseconds or days, it makes no difference." *Bunnell*, 567 F. Supp. 2d at 1153-54.

[12] The *Szymuszkiewicz* court openly criticized the Ninth Circuit and other jurisdictions for adopting the "in transit" requirement: "There is no timing requirement in the Wiretap Act and judges ought not add to statutory definitions." No. 07-CR-171, at *5 (Sept. 9, 2010). The Seventh Circuit later removed that dicta, Order, No. 07-CR-171 (Nov. 29, 2010), but its approach remains at odds with the Ninth Circuit's ruling on this issue.

701 (7th Cir. 2010). Not only is this decision incompatible with Ninth Circuit law, but it is factually distinguishable: *Szymuszkiewicz* concerned an email server that, when it received an email, assembled both the original message and an exact copy, and then delivered the two identical messages to the intended recipient and a hacker simultaneously. *Id.* at 704-06. Though it declined to adopt a timing requirement, the *Szymuszkiewicz* court stated in dicta that because the case involved the simultaneous delivery of identical transmissions to a hacker, the transmission was "contemporaneous by any standard." *Id.* The Complaint here fails under even that formulation, as it does not allege a simultaneous delivery of identical transmissions.

In sum, the Ninth Circuit has held that "interception" is limited to messages acquired in transit, and expressly rejected Plaintiffs' contrary argument. *Konop*, 302 F.3d at 878 n.6 ("While this argument is not without appeal, the language and structure of the [Act] demonstrate that Congress considered and rejected this argument."). Plaintiffs thus do not allege an interception.

2. Plaintiffs Identify No Intercepted "Contents" of a Communication.

A party asserting a Wiretap Act claim bears the burden of alleging that "contents" of a communication were intercepted. "[C]ontents" means "information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 2510(8). Data generated automatically does not qualify; "[r]ather, 'content' is limited to information the user intended to communicate, such as the words spoken in a phone call." *iPhone*, 844 F. Supp. 2d at 1061, 1067-68 (holding location data intercepted from mobile phones were not "contents").

Ignoring *iPhone*, Plaintiffs cite two cases that did not arise under the Wiretap Act. (Opp. 16 (citing *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008); *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)).) Plaintiffs misleadingly suggest that in *Forrester* the Ninth Circuit held that URL strings are "contents" under the Wiretap Act, but that court never even cited the Act.[13]

[13] The *Forrester* court held that for purposes of police searches and seizures, individuals have no right of privacy in many categories of online information, such as IP addresses or websites visited. Plaintiffs cite a footnote, where the court noted in dicta that government tracking of URLs "might be more constitutionally problematic." The statement has no relevance to whether URLs are "contents" under the Wiretap Act.

Plaintiffs also argue that a third case, *Brown v. Waddell*, held that sending numeric codes to a pager transmitted "contents"; thus, Plaintiffs conclude, any "words and numbers" in a URL string are also "contents." (Opp. 16 (citing 50 F.3d 285 (4th Cir. 1995)).) Not so. The pagers in *Brown* were used specifically to communicate numeric codes, such as call-back numbers and codes used to convey messages (e.g., "en route"). 50 F.3d at 287-88. In other words, the codes in *Brown* were the "information the user intended to communicate," not automatically generated data.

Applying their faulty definition, Plaintiffs argue that various types of information like "operating systems" or "browser versions" qualify as contents. (Opp. 15-16.) But these pieces of information consist only of data automatically generated by their browsers or third-party websites—not "information the user intended to communicate." *See iPhone*, 844 F. Supp. 2d at 1061. Plaintiffs thus fail to allege an interception of "contents."

3. Plaintiffs Fail to Identify any "Device" Under the Wiretap Act.

The Wiretap Act also requires the use of a "device." 18 U.S.C. § 2510(5)(a). Plaintiffs offer a list of six purported "devices" (Opp. 17), but the Complaint admits that four of the six are used in the ordinary course of the intended communication: cookies, browsers, computers, and Facebook's servers. (¶¶ 38-81.) As in *Crowley v. CyberSource Corp.*, these items cannot be "devices"; to hold they were would effectively read the "device" requirement out of the Wiretap Act. 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (rejecting theory that defendant's server was a "device" because "[s]uch a result would effectively remove from the definition of intercept the requirement that the acquisition be through a 'device'"); *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, at *4 (E.D. Pa. Dec. 13, 2007) (drive or server not "device"); *Conte v. Newsday, Inc.*, 703 F. Supp. 2d 126, 140 (E.D.N.Y. 2010) (rejecting server theory).

Plaintiffs also list "Plaintiffs' servers" as a "device," but the Complaint does not allege that Plaintiffs have servers. Finally, Plaintiffs ask the court to consider a hypothetical "scheme Facebook put together to effect its purpose of tracking users." (Opp. 17.) Not surprisingly, Plaintiffs offer no authority for their novel notion that a "device" can be an alleged scheme, rather than the physical device a plain reading suggests.

4. Facebook Was a Party to any Transmissions It Allegedly Received.

Plaintiffs allege that their browsers sent information directly to Facebook. (¶ 77; Opp. 6-7.) Because Facebook was a party to those alleged transmissions—in fact, was the sole recipient—they cannot be the basis for a Wiretap Act claim. 18 U.S.C. § 2511(2)(d) (no violation "where [defendant] is a party to the communication . . . ."); *see In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011) (where "the communication at issue is one from a user *to* Defendant, Defendant cannot be liable . . . ."); *Conte*, 703 F. Supp. 2d at 140 (no interception by "direct parties to the communications"); *Ideal Aerosmith,* 2007 WL 4394447, at *5 ("While [plaintiff] complains that [defendant] was not the intended recipient of the communication, that argument has no legal bearing where the communication was nonetheless sent to [defendant]."). Plaintiffs respond that Facebook should not be treated as a party because their browsers sent the transmissions when they were logged out. But, this argument confuses Facebook's status as the direct recipient with the issue of consent. Unlike *iPhone*, the Complaint does not allege that the transmission to Facebook was itself illegitimate. Plaintiffs admit that their browsers communicated with Facebook to enable Like button functionality and to enable them to view the Facebook content on webpages they sought to read. (¶¶ 60-63.) Thus, regardless of whether Plaintiffs were logged out, Facebook cannot be held liable for receiving a communication to which it was a party.

5. Third-Party Websites' and Plaintiffs' Consent Provide Two Additional, Independent Grounds for Dismissal.

Plaintiffs' consent, and the consent provided by websites that allegedly host Facebook features, also defeat the Wiretap Act claim. 18 U.S.C. § 2511(2)(d). Plaintiffs argue that consent cannot be decided on a motion to dismiss, but no decision Facebook has seen has so held, and Plaintiffs point to none.[14] To the contrary, as discussed below, many courts have dismissed

[14] As noted previously, *Pharmatrak*, which dealt with summary judgment, is not controlling or persuasive. In contrast to *Pharmatrak*, the Sixth Circuit has placed the burden of proving lack of consent on the plaintiff. *See United States v. Wuliger*, 981 F.2d 1497, 1503 (6th Cir. 1992) (finding clear error where court failed to assign to government the burden of proving the alleged victim's lack of consent to defendant's interception of her calls). And numerous courts within the Ninth Circuit and elsewhere have dismissed where consent was apparent from the relationship, just as it is here. (Mot. 16 & n.13.)

Wiretap Act claims on consent grounds. (Mot. 16 & n.13.)

First, Plaintiffs consented to Facebook's collection of information under the Privacy Policy in place during the proposed Class Period. Plaintiffs allege they were all Facebook users at that time and, thus, they were on notice of Facebook's practices as disclosed by the Privacy Policy. (¶¶ 5-8.) Plaintiffs admit that "users consent to Facebook installing cookies on each user's computer and . . . consent to these cookies tracking and transmitting data to Facebook regarding each user's web browsing . . . ." (¶ 16.) None of Plaintiffs' arguments overcome this disclosure, which applied for all but three days of the Class Period. (*See* Section II(B), above). And Plaintiffs never explain why a single post in the Help Center—that they never allege they saw or relied upon—overrides the consent provided under Facebook's Privacy Policy.

Second, the consent of third-party websites that host Facebook content provides an additional reason to dismiss. Where a defendant obtains information through the normal operation of its business relationship with a third party, courts presume that the third party consented. *See, e.g.*, *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) ("It is implicit in the web pages' code instructing the user's computer to contact [defendant], either directly or via [a third party] server, that the web pages have consented to [defendant's] interception of the communication between them and the individual user."). This case is no different: the decision of third-party websites to host Facebook features shows the websites' consent to Facebook's receipt of information.[15]

Plaintiffs' response here is to rely again on *Pharmatrak*, which held an inference of consent inappropriate where a third party "insisted there be no collection of personal data and the circumstances permit no reasonable inference that they did consent." 329 F.3d at 20. Here, in contrast, nothing suggests that an inference of consent is unreasonable. And regardless,

[15] Contrary to Plaintiffs' argument, *In re Toys R Us, Inc., Privacy Litigation* is indistinguishable. There, the court found consent where plaintiffs' complaint referred to third-party websites "as entities that are 'using' Coremetrics' technology, and that such other [third-party websites] are 'Coremetrics-enabled.'" 2001 WL 34517252, at *7 n.16 (N.D. Cal. Oct. 9, 2001). Similarly, Plaintiffs allege that the third-party websites hosting Like buttons are Facebook "partners," (¶¶ 60, 69, 83), and have "Facebook content integrated," (¶ 58). To distinguish *DoubleClick* and *Chance*, Plaintiffs again rely on *Pharmatrak*, which as noted above, is not persuasive.

Pharmatrak conflicts with Ninth Circuit law and should be disregarded.[16] (Mot. 16.)

D. Plaintiffs Fail to State a Claim for a Violation of Penal Code § 631 (Count X).

1. Section 631 Does Not Apply to Electronic Communications.

As Facebook demonstrated in its Motion, § 631 does not apply to electronic communications. Rather, by its terms, the law is limited to telegraphs, telephone wires, telephone lines, telephone cables, and telephone instruments.[17] As the California Court of Appeals has explained, "[w]iretapping, as the name itself suggests, refers to the interception of wire (*i.e.*, *telephone*) communications." *People v. Chavez*, 44 Cal. App. 4th 1144, 1150 (1996) (quotation omitted; emphasis added). Plaintiffs do not suggest how the statute can be read otherwise and instead cite *Valentine v. NebuAd, Inc.*, in which the court was never asked to consider the applicability of § 631 to electronic communications. 804 F. Supp. 2d 1022 (N.D. Cal. 2011).[18]

Additionally, the California legislature has expanded Penal Code statutes dealing with wiretapping to include electronic communications while leaving § 631 untouched. For instance, § 629 regulates wiretapping by law enforcement officers; the legislature has amended that law several times in the past 20 years expressly to include electronic communications within the wiretapping powers of the police.[19] Thus, although the Legislature has had multiple opportunities

---

[16] Plaintiffs' own examples of third-party privacy policies state that data collection by Facebook is ***not*** prohibited. *See* Washington Post, Privacy Policy http://www.washingtonpost.com /privacy-policy/2011/11/18/gIQASIiaiN_story_2.html ("Web sites that have links on our site . . . may also collect personally identifiable information directly from you.").

[17] The terms "wire," "line," "cable" and "instrument" as used in § 631 are all initially modified by the word "telephone" and so must be construed in light of that limitation. *People v. Henning*, 173 Cal. App. 4th 632, 643 (2009) (Cantil-Sakauye, J.) (construing phrase "false token or writing" to "require a false token or a false writing"); *Kelly v. Methodist Hosp. of S. Cal.*, 22 Cal. 4th 1108, 1121 (2000) ("[W]hen a statute contains a list … of items, a court should … giv[e] preference to an interpretation that uniformly treats items similar in nature and scope.").

[18] *Valentine* concerned a motion to dismiss based on standing and preemption and did not concern whether electronic communications were covered under the § 631.

[19] The Legislature has amended § 629 several times to expand that statute to encompass certain forms of electronic communications. Analysis of Sen. Bill No. 1016 (1995-96 Reg. Sess.) as amended May 9, 1995, attached as Ex. A to the Declaration of Kyle Wong (hereinafter "Wong Decl.") ("The purpose of this bill is *to extend* the present wiretapping law to also allow the interception of electronic communications . . . Federal law allows not only the interception of wire communications but also the interception of electronic communications."). In 2010, § 629

to expand § 631 in parallel fashion with § 629, it has chosen to maintain the original and existing limitation of these statutes to telegraph and telephone wires, lines and cables alone. *See Murphy v. Kenneth Cole Prods., Inc.*, 40 Cal. 4th 1094, 1106-08 (2007) (Statute did not impose a penalty where the word "penalty" was included in a related statutory section but omitted from the statute at issue).

2. Plaintiffs Concede Facebook Was a Party to the Communication.

Even if § 631 could apply to electronic communications, the Complaint makes clear that Plaintiffs' browser directly sends messages to Facebook. (*See* § III(C)(4); ¶ 77 (describing how the user's browser makes "a request to . . . Facebook").) Facebook is accordingly a party to the communication; otherwise, the "request" that Plaintiffs discuss in their Complaint would have no recipient. Plaintiffs only response is that Facebook cannot be a party because Plaintiffs did not know Facebook was allegedly "tracking" them. This is a red herring. Plaintiffs never challenge the fact that Facebook content is part of the webpages they wanted to view; that these webpages do not host the Facebook content themselves; and that in order to view the webpage the user's browser must contact Facebook. (¶ 60 ("When the CNN server receives th[e] request" from a user to view the website, "it responds with the HTML file […that] contains information from third parties, who partner with CNN to display content on the CNN home page").) According to Plaintiffs' own description, Facebook is a necessary party to the process that Plaintiffs themselves initiated—the downloading of a particular webpage, like www.cnn.com.

3. Plaintiffs Fail to Allege that Facebook Used a Machine, Instrument or Contrivance to Make an Intentional, Unauthorized Connection with a Telephone Wire, Line, or Cable.

As described in Facebook's Motion, Plaintiffs' complaint fails to plead facts that show Facebook used a "machine, instrument, or contrivance" to make an "unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument" to obtain the contents of communications. Plaintiffs' response, to the extent that it can be understood, is conclusory and meritless. While they claim that a cookie is a contrivance that allows Facebook "to participate in

---

was expanded again to cover additional forms of electronic communications. *See* Analysis of Sen. Bill No. 1428 (2009-10 Reg. Sess.) as introduced, attached as Ex. C to Wong Decl.

communications," the Complaint does not describe how a cookie is a contrivance *capable of creating a connection* with any telegraph or telephone line or cable as the statute requires. At best, the Complaint claims that Facebook's cookies are text files that store information (¶ 38 ("[A] cookie is a small text file"); ¶ 39 ("[C]ookies allow servers to store information . . . .")), not that they create a connection or are able to obtain the contents of a communication.[20]

4. Plaintiffs Fail to Allege that Facebook Used any Information Improperly Obtained.

Plaintiffs fail to rebut Facebook's arguments that the Complaint does not allege Facebook used any information improperly obtained. Indeed, Plaintiffs merely cite to four paragraphs in their Complaint, claiming that those allegations establish that Facebook used information it allegedly obtained improperly under § 631. (Opp. 24.) Yet these paragraphs say nothing of the sort; Paragraphs 12-14 merely allege that Facebook's revenue is attributable to "third party advertising" and that Facebook conditions membership on cookies. Paragraph 200 is similarly inapposite; it says nothing about Facebook's use of the allegedly intercepted data. Given this clear failure of pleading, Plaintiffs also have not stated a claim under the "use" prong of § 631.

E. Plaintiffs' Claim Under the SCA Must Be Dismissed (Count II).

The Opposition further confuses the Complaint's already-unworkable SCA allegations and improperly asserts new allegations that are nowhere to be found in the Complaint. Plaintiffs' claim must be dismissed, as it falls far outside the SCA's "narrow scope." *See Low v. LinkedIn Corp.*, 2012 WL 2873847, at *6 (N.D. Cal. July 12, 2012) (The "SCA is not a catch-all statute designed to protect the privacy of stored Internet communications" as "there are many problems of Internet privacy that the SCA does not address.") (internal quotations and citation omitted).

1. Plaintiffs' New Allegations are Improper and Fail to State a Claim.

Plaintiffs' Opposition asserts a new theory to support their SCA claim that contradicts both the Complaint and the plain language of the statute:

> 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

[20] Plaintiffs do not dispute that their claim under the second prong of § 631 fails. (Mot. 18.)

> contemplates includes retaining an email on a server after delivery to the recipient. 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.

(Opp. 24 (citation omitted).) Here, for the first time, Plaintiffs claim that Facebook has permanently stored "tracking" records, which somehow violates the SCA. The Complaint, by contrast, claims that Facebook accessed "persistent cookies on Plaintiffs' and Class Members' computers without their consent" and thereby "obtained electronic communication data in electronic storage in violation of the SCA." (¶ 149.) New allegations asserted through briefing must be disregarded. (*See* § II(A).)

Even if the Court considers this new allegation, it fails on the merits and does not support the SCA claim originally alleged. As Facebook showed in its Motion (which the Opposition fails to address), courts have routinely held that information stored permanently on a personal computer is not in "electronic storage" under the SCA. *E.g.*, *Toys R Us*, 2001 WL 34517252, at *3; (*see* Mot. 20). The one case Plaintiffs cite, *Doe v. City and County of San Francisco*, says nothing to the contrary, and did not even analyze the SCA's "electronic storage" requirement. *See* 2012 WL 2132398, at *2 (N.D. Cal. June 12, 2012).[21] In fact, none of Plaintiffs' allegations meet the statutory definition of "electronic storage": "any temporary, intermediate storage of a wire or electronic communication" or "storage of such communication by an electronic communication service for purposes of backup protection." *See* 18 U.S.C. § 2510(17).

2. Plaintiffs Fail to Allege How Facebook Accessed a "Facility."

Plaintiffs' Complaint makes clear that their personal computers were the supposed "facility" that Facebook allegedly accessed. (*See* ¶ 149 ("Facebook's access of persistent cookies on Plaintiffs' and Class Members' computers . . . *exceeded authorized access to those computers, which are facilities* through which an electronic communication service is provided." (emphasis added).) As Facebook explained (Mot. 20-21), courts have "concluded that an individual's

[21] The *Doe* court upheld a jury verdict that Defendants violated the SCA by accessing the plaintiffs' emails on a shared workplace computer. 2012 WL 2132398, at *1-2. Plaintiffs offer no explanation of how that fact pattern, even if it were relevant, involves "turning temporary information into a permanent record on a third party's facility . . . ." (Opp. 24.)

personal computer does not provide an electronic communication service" and therefore is not a "facility" under the SCA.[22] *E.g.*, *iPhone*, 844 F. Supp. 2d at 1057 ("[A]n individual's computer" does not "fit[] the statutory definition of a facility through which an electronic communication service is provided") (collecting cases). Now, however, Plaintiffs again abandon their Complaint, and raise a novel argument that they have alleged a "detailed system of communications between and among numerous physical means of communication," and that discovery is appropriate to determine how these systems "constitute a 'facility.'" (Opp. 25 (citation omitted).) Plaintiffs cannot change their allegation (again) to avoid on-point, adverse precedent by claiming for the first time that the "facility" in question is something other than their personal computers. (*See* § I.B.) Nor have they shown why they should be allowed discovery to fix their previous allegations or search for new ones.[23]

Additionally, Plaintiffs' new allegation asserts that "Facebook stores the information [*i.e.*, Users' Internet activity] permanently." In itself, this suggests that Facebook stores the challenged data *in Facebook's own facility*. This undermines Plaintiffs' claims for two reasons. First, the SCA requires that the "facility" be the location from which a defendant accesses communications in "electronic storage." *See* 18 U.S.C. § 2701(a) (providing liability for "whoever… *accesses without authorization a facility* through which an electronic communication service is provided… and thereby obtains… a wire or electronic communication *while it is in electronic storage in such*

[22] Plaintiffs have not alleged or identified an "electronic communication service," a necessary requirement under the SCA. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057 ("To state a claim under the SCA, Plaintiffs must allege that Defendants accessed without authorization 'a facility through which an electronic communication service is provided.'"). This too warrants dismissal. Moreover, Plaintiffs' failure to identify an electronic communications service prevents Facebook from availing itself of statutory exceptions that prevent SCA liability. *See* 18 U.S.C. § 2701(c) (providing SCA immunity for conduct authorized by an electronic communications service provider and for users of such services).

[23] Plaintiffs' citation to *Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 334 (D.D.C. 2011) does not address Facebook's argument that Plaintiffs' computers are not SCA "facilities" under their own allegations. *Gaubatz* states that "the [SCA] clearly is not triggered when a defendant merely accesses a physical client-side computer and limits his access to documents stored on the computer's local hard drive or other physical media." *Id.* at 335 (citation omitted). Because the Complaint alleges that Facebook accessed cookie files on Plaintiffs' personal computers (*see* ¶ 149), *Gaubatz* forecloses their claim.

system") (emphasis added). Additionally, under the statute's plain terms, one cannot obtain unauthorized access or exceed authorized access to communications in one's own facility. *See id.*

F. Plaintiffs Fail to State a Claim Under Penal Code § 502 (Count IX).

As an initial matter, Plaintiffs' withdrawal of their claim under the CFAA (Opp. 34) reinforces Facebook's arguments against Plaintiffs' § 502 claims because "§ 502 is the California equivalent of the federal [CFAA]." *Nexsales Corp. v. Salebuild, Inc.*, 2012 U.S. Dist. LEXIS 7890, at *8 (N.D. Cal. Jan. 24, 2012) (citing *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) ("[T]he necessary elements of Section 502 do not differ materially from" those of the CFAA.)). In any case, Plaintiffs fail to allege a § 502 claim.[24]

Not Without Permission: The Complaint does not allege that Facebook acted "without permission" as required under § 502. First, Plaintiffs consented to Facebook's use of cookies. (*See* § III(C)(5).) Second, Plaintiffs fail to allege that Facebook has "overcome[] technical or code-based barriers," which multiple courts in this District have required for an act to be "without permission." *In re iPhone Application Litig.*, 2011 WL 4403963, at *12 (N.D. Cal. Sept. 20, 2011) (finding "liability for acting 'without permission' under Section 502 if they . . . overcome[] technical or code-based barriers'"); *Facebook Privacy*, 791 F. Supp. 2d at 716.[25] In *Facebook Privacy*, the plaintiffs alleged that when a Facebook user clicked on an advertisement on the Facebook site, the URL of the webpage was transmitted to the third-party advertiser. 791 F. Supp. 2d at 709. The court dismissed the § 502 claims because the allegations concerned normal Internet browser operation, not the circumvention of technical barriers. *Id.* at 716. Here, too, Plaintiffs fail to allege that Facebook overcame any technical barriers in receiving information from cookies stored on users' browsers.[26] (Opp. 26.)

---

[24] Plaintiffs do not dispute that their § 502(c)(6) claim should be dismissed. (Mot. 26 n.25.)

[25] Plaintiffs' attempt to distinguish *Facebook, Inc. v. Power Ventures, Inc.*, 2010 U.S. Dist. LEXIS 93517 (N.D. Cal. July 20, 2010) (Opp. 26), which Facebook did not even rely on in its argument on the "without permission" prong, is misplaced given these more recent cases requiring the overcoming of technical barriers in circumstances similar to those here.

[26] Plaintiffs' assertion—made without citation—that Facebook is estopped from making this argument is meritless. Judicial estoppel applies only if a party takes one position then later "'seek[s] an advantage by taking a ***clearly inconsistent*** position.'" *Klamath Siskiyou Wildlands*

No Unlawful Access: Plaintiffs fail to allege that Facebook's purported use of cookies was unlawful "access" under § 502. Their attempt to distinguish *Chrisman* is meritless. In *Chrisman*, the defendant obtained information on a computer that he was allowed to use for work purposes, but not for personal use. *Chrisman v. City of L.A.*, 155 Cal. App. 4th 29, 35 (2007). The court held that this was not "access" under § 502 because when a defendant obtains information he is permitted to obtain under some circumstances, it is not unlawful access under § 502 to obtain that same information under other (potentially improper) circumstances. *Id.* Like in *Chrisman*, Facebook, by Plaintiffs' admission, "had permission" to set cookies and "obtain the information" stored on those cookies under certain circumstances.

Plaintiffs' authorities are inapposite because the defendants in those cases allegedly obtained information to which they *never* had access. *See People v. Lawton*, 48 Cal. App. 4th Supp. 11, 14 (1996) (using public access terminal to bypass security and penetrate nonpublic software); *Weingand v. Harland Fin. Solutions, Inc.*, 2012 WL 2327660, at *2 (N.D. Cal. June 19, 2012) (defendant had permission to access his personal files, but not other company files). Here, by contrast, Plaintiffs concede that Facebook had permission to set and read from cookies on Plaintiffs' computers. (¶ 16.)

Not "Contaminants": Plaintiffs also ignore multiple authorities from this District restricting "contaminants" to "'viruses or worms,' and other malware that usurps the normal operation of the computer or computer system." *iPhone*, 2011 WL 4403963, at *13. Plaintiffs do not argue that the Complaint alleges that Facebook cookies are such "malware." And the Complaint acknowledges (¶¶ 38-41) that cookies are standard web browser functions, which cannot be "contaminant[s]" under the statute. *See In re Facebook Privacy Litig.*, 2011 U.S. Dist. LEXIS 147345, at *14 (N.D. Cal. Nov. 22, 2011).

Ctr. v. Boody, 468 F.3d 549, 554 (9th Cir. 2006) (citation omitted and emphasis added). Nothing in Facebook's positions in *Facebook v. ConnectU, LLC*, 489 F. Supp. 2d 1087 (N.D. Cal. 2007), is inconsistent at all with its positions in this case. Facebook alleged in *ConnectU* that the defendant had violated Facebook's terms of use by conspiring with others to write code to access non-public information on Facebook's website. *Id.* at 1089. This is entirely different than Plaintiffs' allegations here that Facebook violated its terms of use by failing to delete cookies.

No "Damage or Loss": Plaintiffs do not allege damage or loss under § 502(e)(1), which allows compensatory damages only for costs incurred "to verify that a computer system . . . or data was or was not altered, damaged, or deleted by the access." That Plaintiffs' counsel retained a computer law expert to assist in this litigation (¶ 109) does not allege that any named Plaintiffs spent any money to have this expert verify whether their data was "altered, damaged, or deleted." Nor does any named Plaintiff's alleged enrollment in a privacy policy monitoring service (¶¶ 126-29) satisfy this definition. Plaintiffs state that this service notifies enrollees of any ***future*** changes to Facebook's Data Use Policy. (¶ 127.) But the statute refers to expenditures to determine whether data was affected by ***past*** access. Cal. Penal Code § 502(e)(1).

G. Plaintiffs' Claim Under the UCL Should Be Dismissed (Count VIII).

As explained in the Motion, Plaintiffs neither have standing under the UCL nor have they alleged that Facebook acted fraudulently, unlawfully, or unfairly. (Mot. 27-29.)

Standing: Plaintiffs lack standing under the UCL because they fail to allege economic injury and because Facebook is free. (Mot. 27-28.) Plaintiffs respond that they suffered economic injury because Facebook collected "personal information."[27] (Opp. 27.) But as Facebook explained in its Motion (Mot. 27), "a plaintiff's 'personal information' does not constitute money or property under the UCL." *iPhone*, 2011 WL 4403963, at *14; *Facebook Privacy*, 791 F. Supp. 2d at 717.

Fraud: Plaintiffs' UCL "fraud" claim should be dismissed because Plaintiffs fail to satisfy Rule 9(b)'s heightened pleading requirement, and also fail to allege the substantive elements of a UCL fraud claim—including misrepresentation and reliance. (Mot. 28.) A plaintiff "must allege he or she was motivated to act or refrain from action based on the truth or falsity of a defendant's statement . . . ." *Kwikset*, 51 Cal. 4th at 327 n.10. As explained above (*see* § III(B)), Plaintiffs do not identify any Facebook statement that they personally reviewed before visiting a third-party

[27] Plaintiffs also claim that their allegedly "out-of-pocket" litigation expenses provide them with standing under the UCL (Opp. 28), but that is not California law. *See Buckland v. Threshold Enters., Ltd.*, 155 Cal. App. 4th 798, 816 (2007) ("Because the costs were incurred solely to facilitate her litigation, her purchase does not constitute the requisite injury in fact . . . ."), *overruled on other grounds, Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 337 (2011).

website. Plaintiffs also consented to the activities they challenge. (*See* § II(B).)

Unlawful: Plaintiffs' UCL unlawful claim should be dismissed because Plaintiffs fail either to allege any predicate violation or necessary reliance. (Mot. 11-12, 28); *see Kwikset*, 51 Cal. 4th at 327 n.9. Plaintiffs fail to rebut these arguments. (*See* Opp. 13;[28] § III(B).)

Unfair: Plaintiffs' "unfair" claim fails substantively for several reasons. To start, Plaintiffs do not dispute that the reliance requirement applies to their claim under the UCL's unfair prong, and as explained above (§§ II(B), III(B)), Plaintiffs (1) do not identify any statement that they reviewed or induced them to act and (2) consented to Facebook's actions.

Plaintiffs also do not satisfy any of the three "unfairness" tests. First, Plaintiffs do not claim to meet the "substantial injury" test. (*See* Opp. 28-29.) Similarly, because Plaintiffs fail to show how they have suffered any injury (*see* §III(A)), Plaintiffs' Complaint does not satisfy the second test, which requires a balancing of the utility of the defendant's conduct against the harm to the alleged victim. *See Chang Bee Yang v. Sun Trust Mortg., Inc.*, 2011 WL 3875520, at *8 (E.D. Cal. Aug. 31, 2011) (no unfairness when "[p]laintiffs have not sufficiently alleged why they suffered any harm"). Also, because Plaintiffs consented to Facebook's activities (*see* §II(B)), that behavior is not "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *See Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 257 (2010) (no unfairness where no duty to sell membership mailing list); *Bardin v. DaimlerChrysler Corp.*, 136 Cal. App. 4th 1255, 1276 (2006) (no unfairness where no duty to disclose).

Finally, Plaintiffs fail to show the required legislatively declared public policy that is "tethered to specific constitutional, statutory, or regulatory provisions" under the third test. *See Drum*, 182 Cal. App. 4th at 257. Plaintiffs do not even attempt to defend the alleged "public policies" they relied upon in their Complaint. (*Compare* ¶ 180 *and* Mot. 29.) Instead, they cite to a consent agreement between the FTC and an advertising network, ScanScout, to argue that Facebook violated Section 5 of the FTC Act. (Opp. 29); Anal. of Prop. Consent Ord., 76 Fed. Reg. 71564-01 (Nov. 18, 2011). Yet, this consent agreement—in which ScanScout admits to no

[28] Despite an apparently misplaced heading on page 28 of their Opposition, Plaintiffs discuss their unlawful prong claim only in a single paragraph on page 13.

wrongdoing—fails to show how Facebook's actions violated any constitutional, statutory, or regulatory provisions, including Section 5. Facebook users consented to Facebook's use of cookies. (*See* § II(B).) Plaintiffs thus fail to satisfy the "unfair" prong of the UCL.

H. Plaintiffs Fail to State a Claim Under the CLRA (Count XI).

Plaintiffs fail to refute any of Facebook's four independent grounds for dismissing the CLRA claim (Mot. 32). *First*, Plaintiffs fail to show they have suffered "damages" within the meaning of the CLRA. (Mot. 30.) Plaintiffs cite *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102 (N.D. Cal. 2010) to argue that "the disclosure of plaintiffs' personal information [constitutes] damages under the CLRA." (Opp. 29.) But unlike the plaintiffs in *AOL*, Plaintiffs do not allege the public disclosure of highly-sensitive information like "credit card numbers, social security numbers, financial account numbers, user names and passwords." 719 F. Supp. 2d at 1111. *Second*, Plaintiffs are not "consumers" within the meaning of the CLRA (Mot. 30), which requires an individual who "seeks or acquires, by *purchase or lease*" goods or services. *See* Cal. Civ. Code § 1761(d) (emphasis added). Plaintiffs argue that their personal information was "consideration" that constituted a "payment" to Facebook. (Opp. 30.) But that argument was flatly rejected in *Facebook Privacy Litigation*, 791 F. Supp. 2d at 717 ("Plaintiffs' contention that their personal information constitutes a form of 'payment' to Defendant is unsupported by law."). Plaintiffs offer no response to this on-point precedent. *Third*, Plaintiffs challenge Facebook features, such as the Like button, that are or relate to software. (Mot. 30.) Plaintiffs do not dispute that software is not covered by the CLRA and concede that browsers are "software application[s]." (Opp. 5.)[29] *Finally*, Plaintiffs' CLRA claim fails because, independent of Rule 9(b), Plaintiffs fail to allege causation or reliance. (*See* Mot. 30; § II(B).)

I. Plaintiffs Fail to State a Claim for Conversion (Count VI).

Plaintiffs' claim for conversion should be dismissed because Plaintiffs fail to allege any injury or harm. (Mot. 30-31.) Plaintiffs' bare assertion that "personal information has value" (Opp. 31) is insufficient to establish injury. (*See* § III(A).) Plaintiffs also fail to allege a

[29] Plaintiffs assert that "Facebook sells a social networking service," but offer no case law or explanation in support of this statement. (Opp. 30 (emphasis omitted).)

convertible property right (Mot. 31), which only exists where plaintiffs establish an interest (1) that is "capable of precise definition" and (2) "exclusive possession or control" and (3) in which the owner has "established a legitimate claim to exclusivity." *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003). Plaintiffs offer no argument in response and fail to discuss, let alone distinguish, this case law. (*Compare* Opp. 31-32 *with* Mot. 31); *see also iPhone*, 844 F. Supp. 2d at 1074 (dismissing with prejudice claim for conversion of "personal information" under *Kremen*). Moreover, as explained in the Motion (Mot. 31) and above (§ (II(B)), Plaintiffs consented to Facebook's use of cookies and therefore cannot state a claim for conversion. *Bank of N.Y. v. Fremont Gen. Corp.*, 523 F.3d 902, 914 (9th Cir. 2008).

Plaintiffs claim there is a trend to apply the tort of conversion to intangible property interests and assert that "the modern trend recognizes that misuse of the [sic] confidential information becomes the gravamen of conversion . . . ." (Opp. 31-32.) Even if this were true, the Ninth Circuit test continues to govern. *See Kremen*, 337 F.3d at 1030-33. Moreover, Plaintiffs offer no support for this claim regarding the "modern trend." (Opp. 32.)[30] Indeed, the principal case they cite actually states that "[t]he gravamen of the tort of conversion is the *deprivation* of the possession or use of one's property." *FMC Corp. v. Capital Cities/ABC, Inc.*, 915 F.2d 300, 304 (7th Cir. 1990) (emphasis in original).

J. Plaintiffs Fail to State a Claim for Trespass to Chattels (Count VII).

Plaintiffs' trespass to chattels claim should be dismissed for four independent reasons: Plaintiffs fail to allege (1) damages, (2) a property right that may be trespassed upon, or (3) interference with their personal information or computers, and (4) Plaintiffs consented to the activity they allege to constitute a trespass. (Mot. 32.) Plaintiffs fail to rebut these arguments.

Plaintiffs assert that "California generally recognizes a trespass claim where the defendant exceeds the scope of the consent." (Opp. 32 (citing *eBay, Inc. v. Bidder's Edge*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000)).) Despite asserting their claim satisfies "California" law (Opp. 32),

[30] The cases Plaintiffs cite all involve confidential *business* information, often in a tangible form. *See, e.g., FMC Corp.*, 915 F.3d at 305 (documents reflecting business information); *Annis v. Tomberlin & Shelnutt Assocs., Inc.*, 195 Ga. App. 27, 32-33 (1990) (marketing strategy manual).

Plaintiffs ignore controlling California Supreme Court precedent, *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003). The *Hamidi* court held that, insofar as *eBay* could be read as stating that an "unauthorized use of another's chattel is actionable even without any showing of injury," that "would not be a correct statement of California" law. *Id.* at 1356-57. Moreover, Plaintiffs consented to Facebook's use of cookies. (*See* § II(B).)

Plaintiffs also fail to allege injury to computer systems or "personal information." *Hamidi* explains that "while a harmless use or touching of personal property may be a technical trespass, an interference . . . is not *actionable* without a showing of harm." 30 Cal. 4th at 1351 (citation omitted; emphasis in original). "[I]ntermeddling is actionable only if the chattel is impaired as to its condition, quality, or value, or . . . the possessor is deprived of the use of the chattel for a substantial time." *Id.* at 1357 (citation omitted). Plaintiffs cannot show "actual or threatened damage to [their] computer hardware or software [or] interference with its ordinary and intended operation" or that they have been dispossessed or deprived of the use of information about them. *Id.* at 1352-53, 1357; (Mot. 32-33.) Plaintiffs' trespass claim should, therefore, be dismissed.

K. Plaintiffs Fail to State a Claim for Intrusion upon Seclusion (Counts IV & V).

Plaintiffs' intrusion upon seclusion claim fails because the Complaint does not allege an intrusion into a place (1) in which Plaintiffs have a subjective expectation of privacy (2) that is objectively reasonable (3) in a manner highly offensive to a reasonable person.

1. Plaintiffs Fail to Allege a Subjective Expectation of Privacy that Is Objectively Reasonable.

The Opposition completely ignores Facebook's arguments regarding Plaintiffs' failure to allege any precautionary measures that would support a subjective expectation of privacy. (*See* Mot. § II(C).) Plaintiffs also ignore case law that states users do not have an objectively reasonable expectation of privacy in information provided to others as part of the normal operation of the Internet, as here. (*See* Mot. 34.) Instead of addressing these on-point authorities, Plaintiffs cite to inapposite cases that either dealt with information stored exclusively on one's computer, *see United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (information stored locally on one's hard drive); *United States v. Peden*, 2007 U.S. Dist. LEXIS 61354 (E.D.

Cal. Aug. 9, 2007) (same), or cases that do not even address information relating to computers at all, *see Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971) (no discussion of computers or a reasonable expectation of privacy); *Sanders v. Am. Broadcasting Cos.*, 20 Cal. 4th 907, 918 (1999) (discussing recorded conversations not privacy in one's computer). Plaintiffs' unsupported assertion that users have a reasonable expectation of privacy in their browsing information voluntarily shared with third parties should be rejected.

2. Plaintiffs Fail to Allege a "Highly Offensive" Intrusion.

Plaintiffs ignore case law defining a "highly offensive" intrusion. They contend that Facebook conflates how the information was obtained with what was done with the information (Opp. 33), but the California Court of Appeals addressed this question and "found no case which imposes liability based on the defendant obtaining unwanted access to the plaintiff's private information which did not also allege that the *use* of plaintiff's information was highly offensive." *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992-93 (2011). Like *Folgelstrom*, Plaintiffs fail to allege a highly offensive intrusion because the suggestion that Facebook might use Plaintiffs' information for ad targeting purposes (¶ 178) is routine commercial behavior. *Id.*

Even if the court were to ignore this precedent, as Plaintiffs do, the Complaint still does not allege a highly offensive intrusion. Plaintiffs allege that they gave Facebook permission to install cookies. (¶ 16.) Unlike the cases Plaintiffs cite, which deal with clandestine wiretapping of telephone conversations, Plaintiffs' allegations, even assuming them to be true, are not such an "egregious breach of social norms" as to constitute an actionable intrusion upon seclusion. *See iPhone*, 844 F. Supp. 2d at 1063 (obtaining personal data and geolocation information without one's knowledge and consent "does not constitute an egregious breach of social norms").

IV. CONCLUSION

For these reasons, the Court should grant Facebook's motion to dismiss with prejudice.

Dated: August 22, 2012

COOLEY LLP

/s/ Matthew D. Brown
Matthew D. Brown (196972)
Attorneys for Defendant FACEBOOK, INC.

1283200/SF