COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
MATTHEW D. BROWN (196972)
(brownmd@cooley.com)
KYLE C. WONG (224021)
(kwong@cooley.com)
ADAM C. TRIGG (261498)
(atrigg@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 MOTION TO DISMISS PLAINTIFFS' SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT (FED. R. CIV. P. 12(b)(1) & 12(b)(6))

Date:	April 28, 2016
Time:	9:00 a.m.
Courtroom:	4
Judge:	Hon. Edward J. Davila
Trial Date:	None Set

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)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

TABLE OF AUTHORITIES
(continued)

Page(s)

Other Authorities

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on April 28, 2016 at 9:00 a.m. or as soon thereafter as this Motion may be heard in the above-entitled court, located at 280 South First Street, San Jose, California, in Courtroom 4, 5th Floor, Defendant Facebook, Inc. ("Facebook") will, and hereby does, move to dismiss the Second Amended Consolidated Class Action Complaint ("SAC"). Facebook's Motion is made pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) and is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, and all pleadings and papers on file in this matter, and upon such matters as may be presented to the Court at the time of hearing or otherwise.

STATEMENT OF RELIEF SOUGHT

Facebook seeks an order pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) dismissing with prejudice Plaintiffs' SAC and each of the eleven claims alleged therein for lack of standing and failure to state a claim upon which relief can be granted.

STATEMENT OF ISSUES TO BE DECIDED

1. Whether Plaintiffs have established Article III standing.
2. Whether the SAC states a claim upon which relief can be granted.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs' SAC, although longer than their previous complaint, fails to meaningfully address the Court's October 23, 2015, Order ("Order") dismissing each of their 11 claims under Rules 12(b)(1) and 12(b)(6). The SAC does not, for instance, add any allegations of actual injury or damages Plaintiffs claim to have suffered. Nor does it assert new facts to connect their conclusory allegations of injury to Facebook's alleged conduct. In fact, the SAC again does not identify a single specific communication or URL Plaintiffs contend Facebook improperly obtained. In the end, Plaintiffs rely on the same core allegations that Facebook used browser cookies to track individual users who were logged out when those users visited webpages that integrated Facebook features. Although they have puffed up their pleading with new and largely

irrelevant details to suggest to the Court that they have filled the holes in their pleading, upon closer inspection, it is clear that these new allegations are little more than window dressing.

Specifically, in dismissing Plaintiffs' common law and statutory claims that require proof of injury, the Court determined that Plaintiffs failed to adequately allege, "for the purposes of Article III standing, that they personally lost the opportunity to sell their information or that the value of their information was somehow diminished after it was collected by Facebook." Order at 10. Yet, the SAC fails to add a single allegation to address, let alone satisfy, this threshold requirement. Instead, they simply reiterate conclusory allegations of theoretical harm, unconnected to Plaintiffs themselves, or to Facebook's conduct—allegations the Court has already determined are inadequate. Their claims again should be dismissed under Rule 12(b)(1).

Even if the SAC included allegations sufficient to establish Plaintiffs' Article III standing, each of their claims remain deficient under Rule 12(b)(6). For example, in dismissing Plaintiffs' Wiretap Act claim, this Court noted that "Plaintiffs may never be able to state" such a claim because the URL addresses they contend Facebook "intercepted" were not "contents" under the Ninth Circuit's binding precedent in *In re Zynga Privacy Litigation*, 750 F.3d 1098 (9th Cir. 2014) ("*Zynga*"). (Order at 15-16.) Ignoring this Court's ruling, the SAC reasserts a Wiretap Act claim without alleging any new facts to address this fatal flaw. The SAC continues to rely on URL information sent to Facebook when users view webpages with Facebook content as the basis for their claim. As this Court already held, however, this URL information is not "content" under the statute—it is simply record information that is transmitted as part of the normal operation of the Internet. Nor does the SAC adequately allege an "interception" through use of a "device" or address the fact that Facebook was necessarily a party to the communications, each of which is an independent basis for dismissing the Wiretap Act claim.

Likewise, the Court dismissed Plaintiffs' claim under the Stored Communications Act ("SCA") because Plaintiffs alleged that cookies were "persistent" and therefore could not demonstrate that they were accessed in "temporary" "electronic storage," as required by the statute. The SAC suffers from the same defect—it acknowledges that cookies are "persistent," and fails to allege that Facebook actually accessed a communication while in "electronic storage."

The addition of vague allegations about the operation of browsers does nothing to address this fatal defect. Nor does the SAC allege, as it must, that Facebook accessed a "facility" through which an electronic communications service is provided.

The Court also dismissed Plaintiffs' claim under the California Invasion of Privacy Act on two separate grounds: Plaintiffs failed to allege facts to demonstrate (1) that a passive cookie could act as a "machine, instrument, or contrivance" under the statute, and (2) that any of Plaintiffs' communications had been intercepted. Despite the Court's Order, the SAC does not assert new facts showing that a cookie takes any actions to make it a contrivance and does not identify a single communication of any named Plaintiff that Facebook allegedly intercepted.

And while Plaintiffs add several new claims (while declining to reassert several of their dismissed claims), they suffer from, *inter alia*, the same fatal defects that the Court addressed in its Order. Plaintiffs lack Article III standing to assert these claims because the SAC relies, just as the previous complaint did, on vague, generalized allegations that are not tethered to the named Plaintiffs and do not show any concrete harm suffered as a result of the complained-of conduct. The SAC also fails to plead facts to support the necessary elements of these claims. Instead, these claims are largely based on conclusory allegations that Facebook represented during the proposed class period that it would delete certain cookies when users logged out of their accounts. Critically, this statement is alleged to have appeared in a single entry in Facebook's extensive online Help Center, not in Facebook's Statement of Rights and Responsibilities. Plaintiffs do not allege when the statement was made, or that any of the Plaintiffs ever even saw it, much less relied on it. These deficiencies are fatal to Plaintiffs' contract and fraud claims.

For these and the reasons that follow, the Court should dismiss the SAC with prejudice.

II. STATEMENT OF FACTS[1]

A. The Operation of the Internet

To browse the Internet, individuals use a web browser, such as Microsoft Internet Explorer or Google Chrome. (SAC ¶ 28.) To view a webpage, an individual's browser sends a

[1] By discussing the SAC's factual allegations and documents incorporated by reference, Facebook does not thereby make any admissions.

"GET" request to the server that hosts that webpage. (*Id.* ¶ 31.) Webpages are "often an assembled collage of independent parts . . . [and] portions often exist on different servers, often operated by third parties . . . ." (*Id.* ¶ 36.) Thus, if an individual's browser sends a GET request to view a webpage that also contains third-party content, the webpage responds to the browser by sending back, among other things, code that causes the browser to send a separate and different GET request to the server hosting the third party content. (*Id.* ¶¶ 37, 60.) Thus, there are two distinct requests sent by the browser—one initially to the webpage's server to load the webpage, and one to the third-party's server to load its content onto that same webpage. (*Id.* ¶ 60.) The GET request sent by the browser typically contains the URL of the webpage being loaded, known as the "referer URL"[2] (sometimes described as a "referer header"), so the third-party server knows where to load the requested content. (*Id.* ¶¶ 38, 60); *see also Zynga*, 750 F.3d at 1101-03.

Like any web content provider, Facebook's servers receive GET requests, along with referer URLs, when an individual requests to view a webpage that contains Facebook content, such as the "Like" button.[3] (*Id.* ¶ 60.) This is true regardless of whether the individual sending the request to Facebook's server has a Facebook account, is logged into Facebook, or has never visited Facebook's website, because it is part of the "normal operation of the Internet." (*Id.* Ex. I at 3.) Thus, whenever any individual wishes to visit a webpage with Facebook content, Plaintiffs allege that that individual's browser sends a GET request to Facebook that includes the URL of that webpage. (*Id.* ¶¶ 37, 38.)

B. Facebook's Use of "Cookies"

A "cookie" is a "small text file[]" that a server creates and sends to a browser. (*Id.* ¶ 52.) It is "a piece of information . . . that the browser software is expected to save and to send back whenever the browser makes additional requests of the [same] server (such as when the user visits additional webpages at the same or related sites)." *In re Pharmatrak, Inc. Privacy Litig.*, 329

[2] "Referer," although a misspelling of "referrer," is the term of art in the industry.

[3] The Like button is a thumbs-up symbol next to the word "Like," that users may click to share their affinity for particular piece of content. To include the Like button on its webpage, a third-party website incorporates code for the Like button into the code for that webpage.

F.3d 9, 14 (1st Cir. 2003).[4] "Cookies are widely used on the internet by reputable websites to promote convenience and customization[,]" *id.*, including Facebook, which uses cookies to enable its users to share content with each other, including content on third-party websites (SAC Ex. E at FB_MDL_00000008). Facebook also uses cookies for security purposes. (*Id.*)

The SAC discusses several cookies that Facebook allegedly writes to the browsers of Internet users that visit Facebook's website. (*Id.* ¶ 58.) These cookies are stored in the user's browser, and, unless they are removed or expire, they are sent back to Facebook's server when a user sends a GET request to view a webpage with Facebook content. (*Id.*¶ 60.)

C. Facebook's Terms of Use and Privacy Policy

Every Facebook user during the alleged class period agreed to Facebook's terms of use, called the Statement of Rights and Responsibilities ("SRR"), which "govern[ed] [Facebook's] relationship with users . . . ." (SAC Ex. A at FB_MDL_00000012; *id.* Ex. B at FB_MDL_00000021; *id.* Ex. C at FB_MDL_00000024; *id.* Ex. D at FB_MDL_00000037.) The SRR imposed obligations on Facebook's users. For example, users were prohibited from, among other things, posting unauthorized commercial communications, accessing an account belonging to someone else, providing false personal information, creating multiple accounts, or creating more than one profile. (*Id.* Exs. A-D.) The SRR further included an integration clause, which provided that the SRR "makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements." (*Id.* Ex. A at § 18.1; *id.* Ex. B at § 18.2; *id.* Ex. C at § 18.2; *id.* Ex. D at § 18.2.) The SRRs applicable during the alleged class period made no representations regarding Facebook's use of cookies. (*Id.* Exs. A-D.)

Facebook also maintained a Privacy Policy (later called the Data Use or Data Policy). Since the start of the alleged class period, the Privacy Policy—which is linked at the bottom of virtually every page on Facebook—disclosed the following to users:

> **Cookie Information.** We use "cookies" (small pieces of data we store for an extended period of time on your computer…) to make Facebook easier to use, to make our advertising better, and to protect both you and Facebook. For example,

[4] Because cookies do not collect any information, the SAC incorrectly asserts that cookies "can record a person's Internet communications" and "track a person's communications." (*Id.* ¶ 55.)

> we use them to store your login ID (but never your password) to make it easier for you to login whenever you come back to Facebook. We also use them to confirm that you are logged into Facebook, and to know when you are interacting with Facebook Platform applications and websites, our widgets and Share buttons, and our advertisements. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use Facebook.

(*Id.* Exs. E-G.)[5] Plaintiffs allege (without citation) that Facebook informed users that "when you log out of Facebook, we remove the cookies that identify your particular account." (*Id.* ¶¶ 23, 63, 245.) This language is not included in any version of the SRR or Privacy Policy during the alleged class period. Plaintiffs appear to allege that the statement was included on one of Facebook's many Help Center pages (*Id.* ¶ 23), but Plaintiffs do not allege what page that was, when the page was live, or whether any of the Plaintiffs ever saw it (and if so, when).

D. The Plaintiffs and the Putative Class

The SAC includes nearly identical allegations for each of the four Plaintiffs. According to the SAC, Plaintiffs had active Facebook accounts and "visited websites after logging-out of [their] Facebook account[s] which Facebook tracked, intercepted, and, in relation to which, Facebook accessed [their] computing device[s] and web-browser[s]. URLs for many of these websites contain detailed file paths containing the content of GET and POST communications." (SAC ¶¶ 113-128.) Plaintiffs do not allege which websites they visited when logged out that were allegedly "tracked." The SAC also does not identify what, if any, communications or personal information Facebook supposedly collected from Plaintiffs, nor that Facebook actually used it or disclosed it to any third party. While the SAC opines on the theoretical value of users' referer URLs, these allegations are virtually unchanged from the Corrected First Amended Consolidated Class Action Complaint ("FAC"); they remain abstract and untethered to *anything* that Plaintiffs allege actually happened here. (*Id.* ¶¶ 129-143.) Nor do Plaintiffs allege that they suffered any actual harm from the alleged conduct, or that they ever sought to sell, were prevented from selling, or had the chance to sell this information.

[5] The September 2011 Data Use Policy included similar language. (*Id.* Ex. H at FB_MDL_00000048.)

III. LEGAL STANDARDS

Under Rule 12(b)(1), a court must dismiss claims where a plaintiff has failed to establish standing under Article III of the U.S. Constitution. *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000); *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 101-02 (1998). A court must also dismiss claims under Rule 12(b)(6) when "there is no cognizable legal theory or an absence of sufficient facts alleged to support a cognizable legal theory." *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). "[L]abels and conclusions, and a formulaic recitation of the elements of a cause of action" are not sufficient to save a complaint from dismissal. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

Rule 9(b) requires claims sounding in fraud to be pled with particularity. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (citations omitted). This heightened standard applies to all claims sounding in fraud, regardless of whether fraud is an enumerated element of the underlying cause of action. *Id.* at 1103. Here, Plaintiffs' claims for violation of § 502, civil fraud, and larceny must be pled with particularity because each claim sounds in fraud. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009).[6]

IV. ARGUMENT

A. Plaintiffs Lack Article III Standing

As this Court has already held as to most of the claims asserted, Plaintiffs lack Article III standing because they do not allege (1) they suffered an "injury in fact," (2) that is fairly traceable to the defendant's conduct and (3) will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000). A plaintiff who fails to show that she "personally ha[s] been injured" cannot seek relief for herself or any other putative class member. *Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F.3d 1018, 1022 (9th Cir. 2003).

[6] The civil fraud claim speaks for itself. As to the § 502 claim, Plaintiffs allege a "scheme to defraud" and that Facebook committed "fraud." (SAC ¶¶ 278, 285.) Similarly, Plaintiffs' larceny claim alleges that Facebook "deceived" Plaintiffs and acted "fraudulently." (*Id.* ¶¶ 290, 292.)

1. Plaintiffs Again Fail to Allege Injury in Fact

In the Order, the Court held that Plaintiffs did not "articulate[] a cognizable basis for standing pursuant to Article III" because they did "not demonstrate[] that Facebook's conduct resulted in some concrete and particularized harm." (Order at 11.) The Court determined that the FAC failed to connect whatever value there might be in the information allegedly collected by Facebook "to a realistic economic harm or loss that is attributable to Facebook's alleged conduct." (*Id.* at 10.) Put another way, "Plaintiffs [did] not show[], for the purposes of Article III standing, that they personally lost the opportunity to sell their information or that the value of their information was somehow diminished after it was collected by Facebook." (*Id.*) Despite the notice afforded by this Order, Plaintiffs' SAC still suffers from this same fatal defect.

The SAC leaves the allegations regarding the theoretical economic value of their referer URL information virtually unchanged from those in the FAC, and contains *no new allegations* demonstrating that any Plaintiff plausibly suffered any concrete and particularized harm. (*Compare* FAC ¶¶ 10-14, 111-125 *with* SAC ¶¶ 129-143.) The SAC now contains two paragraphs with opinion poll results suggesting that Americans value control over information about them. (SAC ¶¶ 142-43.) But that says nothing about any concrete and particularized loss Plaintiffs actually suffered. In fact, Plaintiffs do not plead a single instance where anyone was willing to pay them for their information, let alone where Facebook's alleged conduct lessened the value of their information or its purported marketability. This sort of generalized pleading fails to satisfy the injury-in-fact requirement that Plaintiffs must be harmed *personally*. (Order at 8-11 (citing *Low v. LinkedIn Corp.*, 2011 U.S. Dist. LEXIS 130840, at *12-15 (N.D. Cal. Nov. 11, 2011); *LaCourt v. Specific Media, Inc.*, 2011 U.S. Dist. LEXIS 50543, at *11-12 (C.D. Cal. Apr. 28, 2011)); *see also In re Zappos.com, Inc.*, 2015 U.S. Dist. LEXIS 71195, at *12 (D. Nev. June 1, 2015) (no injury-in-fact where "Plaintiffs do not allege any facts explaining how their personal information became less valuable . . . or that they attempted to sell their information and were rebuffed because of a lower price-point"); *In re iPhone App. Litig.*, 2011 WL 4403963, at *5-6 (N.D. Cal. Sept. 20, 2011) ("*iPhone App. Litig. I*") (dismissing claims for lack of standing). Thus, Plaintiffs lack standing under Article III to pursue their claims.

2. The Alleged Statutory Violations Do Not Confer Article III Standing

The mere allegation of a statutory violation does not create standing as to that claim without an allegation that the plaintiff suffered a resulting, non-speculative, actual injury, as the Supreme Court has repeatedly stated. *See, e.g.*, *Summers v. Earth Island Inst.*, 555 U.S. 488, 497 (2009) ("[I]njury in fact is a hard floor of Article III jurisdiction that cannot be removed by statute."); *Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997) ("It is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing."); *Gladstone, Realtors v. Village of Bellwood*, 441 U.S. 91, 100 (1979) ("In no event, however, may Congress abrogate the Art. III minima: A plaintiff must always have suffered 'a distinct and palpable injury to himself[.]'") (citation omitted). Because, in addition to the reasons discussed above (*supra* § IV.A.1), the alleged statutory violations in this case are not accompanied by allegations of concrete and particularized injury to Plaintiffs that resulted from the alleged violations, there is no standing as to these claims.[7]

Even under *Edwards*, Plaintiffs have no standing as to their statutory claims because the SAC fails to show that the alleged statutory violations affected *Plaintiffs themselves*. *Edwards*, 610 F.3d at 517 (Article III standing for violation of statutory right only where "the constitutional or statutory provision on which the claim rests properly can be understood as granting persons *in the plaintiff's position* a right to judicial relief" (emphasis added) (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975))). Courts find allegations of distinct and palpable injury only when, unlike here, the pleadings allege specific harm to the plaintiffs caused by the statutory violations. In *Gaos v. Google Inc.*, for example, 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 (N.D. Cal. Mar. 29, 2012). The Court dismissed six of the plaintiff's seven claims for failure to allege injury

[7] Facebook acknowledges that courts in this circuit have applied *Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), to find standing based on mere assertions of statutory violations. Facebook respectfully submits that *Edwards* was incorrectly decided, although currently precedential in this circuit. The Supreme Court soon will rule in a case that may bear on the issue, *Spokeo, Inc. v. Robins*, No. 13-1339 (*cert. granted* Apr. 27, 2015; argued Nov. 2, 2015).

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; *see also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021 (N.D. Cal. 2012) (alleged SCA violations sufficient to establish Article III injury in fact where plaintiff "[gave] specific examples of the information allegedly transmitted to third parties when he visited the LinkedIn website"). Here, in contrast, Plaintiffs fail to provide a single example of a third-party webpage they visited, a communication of theirs that was "tracked," or other injury "specific to them." Plaintiffs lack Article III standing for their statutory claims.

Further, Plaintiffs' failure to allege actual injury dooms three of their statutory claims that require injury by the statutes' own terms.[8] The Court, in its previous Order, dismissed Plaintiffs' claim under California Penal Code § 502 for lack of standing because that statute "require[s] a plausible economic injury for standing." (Order at 12-13.) Plaintiffs offer no basis for the Court to revisit that decision. Plaintiffs now assert new claims for civil fraud under California Civil Code §§ 1572 and 1573, and larceny under California Penal Code §§ 484 and 496. Like § 502, the civil fraud and larceny statutes also require injury. *Moncada v. W. Coast Quartz Corp.*, 221 Cal. App. 4th 768, 776 (2013) (damages must be alleged for fraud claims); *Jones v. Wagner*, 90 Cal. App. 4th 466, 471 (2001) (constructive fraud requires damages); Cal. Penal Code § 496(c)[9] (providing private right of action to someone "who has been injured by a violation" of the statute). Because Plaintiffs have not alleged any actual injury, these three claims must be dismissed for lack of standing for this independent reason.

B. Plaintiffs Fail to State a Claim under the Wiretap Act (Count I)

To establish a Wiretap Act violation, Plaintiffs must allege that Facebook (1) "intercepted" (2) the "contents" of an "electronic communication" (3) using a "device."

[8] As discussed below, this deficiency also means that Plaintiffs have failed to state a claim so, even if the Court had subject-matter jurisdiction over these three claims in the first instance, the claims would have to be dismissed under Rule 12(b)(6) as well. (*See infra* §§ IV.E, F, L.)

[9] As explained in § IV.L. *infra*, Penal Code § 484 does not provide for a private right of action.

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002). The SAC does not substantively change the allegations that this Court previously held were insufficient to state a claim. Even were the Court to determine that Plaintiffs had adequately pled these requirements, Facebook would fall within several exemptions provided under the law.

1. Plaintiffs Do Not Allege that Facebook's Conduct Dealt With the "Contents" of Their Communications, Let Alone that Facebook "Intercepted" Their Communications With a "Device"

No contents. In *Zynga*, the Ninth Circuit held that "contents" means "the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." 750 F.3d at 1106-07. The *Zynga* court then determined that a referer header, even when it includes the address of the webpage a user is viewing, is not "contents" but rather "record information" akin to an address. *Id.* Applying *Zynga*, this Court dismissed Plaintiffs' Wiretap Act claim, recognizing that the URL information Plaintiffs allege has been intercepted "is so similar to the referer headers addressed in *Zynga Privacy Litigation* [that] Plaintiffs may never be able to state [a] Wiretap Act claim . . . ." (Order at 16.) The Court was right. The SAC fails to distinguish the URL information Plaintiffs allege has been intercepted from the referer headers at issue in *Zynga*. Indeed, Plaintiffs' amendments repeatedly refer to the allegedly intercepted information as "referer URLs" and explain that such information is a combination of the name of the webpage and the file path. (SAC ¶¶ 185, 34.) This is the very same "record" information the Ninth Circuit and this Court held are not "contents" under the Wiretap Act. *Zynga*, 750 F.3d at 1106-07.

Moreover, the SAC concedes that the referer URL is part of a message "automatically sent" by Plaintiffs' computers. (SAC ¶ 60.) Under *Zynga*, such an automatically generated communication cannot be an "intended message" under the Wiretap Act, and the claim fails for this additional reason. *See Zynga*, 750 F.3d at 1106-07 (contents refers to the "intended message conveyed by the communication" not information that is "generated in the course of the communication"); *see also In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1061-62 (N.D. Cal. 2012) ("*iPhone App. Litig. II*") (geolocation data allegedly intercepted from mobile phones were not the "contents" of communications because they were "generated automatically").

Plaintiffs' vague allegation that the "referer URLs" on which their claim is based included "search queries which [P]laintiffs sent to [] websites [other than Facebook]" (SAC ¶ 185) does not compel a different result. Plaintiffs fail to specify any search query attributable to any Plaintiff. Nor do they specify any referer URL they allege contains the contents of a search query. Even if this theory had a basis in the law, which it does not, this passing reference in the SAC is too conclusory to support a claim and does not satisfy the standard of plausibility. *See, e.g., Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (A plaintiff must plead "more than a sheer possibility that a defendant has acted unlawfully.").

No interception. Plaintiffs' SAC again fails to show that Facebook "intercepted" a communication protected by the Wiretap Act.[10] *Konop*, 302 F.3d at 879 & n.6 (noting that interception must occur "during transmission," which is the "very short" period where an electronic communication "travels across the wires at the speed of light"). An interception does not occur where a defendant acquires a separate copy of a communication. *Bunnell v. Mot. Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1152-54 (C.D. Cal. 2007) (receiving forwarded emails did not constitute an interception of the original email); *Cobra Pipeline Co. v. Gas Nat., Inc.*, 2015 U.S. Dist. LEXIS 124236, at *19 (N.D. Ohio Sept. 17, 2015) (no interception where the defendant acquired the communication "at the expected end-point of the transmission"). Nor does the fact that multiple communications are sent or received within a short time of one another change their sequential nature. *Bunnell*, 567 F. Supp. 2d at 1154 (noting that once an email was received by an email server, it could no longer be intercepted during transmission, regardless of whether a subsequent copy of a message was sent or received within "milliseconds").

Plaintiffs vaguely allege Facebook intercepted communications between Plaintiffs and the first-party webpages they were attempting to view. However, the SAC does not allege that Facebook receives the actual communication sent to the first-party webpage. To the contrary, the SAC describes a sequential process where Plaintiffs' browser sends two *different* communications at two different times. First, a GET request is sent to a first-party server, such as Walmart.com,

[10] The Court previously dismissed this claim based on failure to allege "contents," so it did not reach Facebook's arguments that Plaintiffs had not alleged "interception" or use of a "device."

requesting the contents of a webpage. (SAC ¶ 60.) Only *after this GET request has been sent and received by the first-party website,* does the first-party website respond to the user's browser with some of the webpage content and the code that subsequently triggers the browser to send a *separate* and *different* GET request *to Facebook*. (*Id.*) Thus, Plaintiffs' own allegations establish that the communication between the Plaintiffs and the webpage they wish to view is not intercepted by Facebook. *See Bunnell*, 567 F. Supp. 2d at 1154 (once a communication is received at its destination, it can no longer be intercepted during transmission under the Wiretap Act).

No Device. Plaintiffs' claim also fails because Plaintiffs cannot establish that Facebook used any "device" covered by the Act. The statute defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5). Plaintiffs' conclusory allegations that every element involved in the process of requesting and displaying a webpage—including data, computer, computer program, or even Facebook's "plan"—qualifies as a "device" (SAC ¶ 187) are insufficient. *See Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (dismissing Wiretap Act where defendant "did not acquire [the communication] using a device other than the drive or server on which the e-mail was received"). Indeed, the SAC does not show how any of these items "can be used to intercept" the communication between Plaintiffs and first-party servers. A cookie is only "a small file[] that store[s] information." (SAC ¶ 23.) It is incapable of "intercepting" anything. Similarly, the SAC does not show how Facebook could have used Plaintiffs' own computers to intercept anything. And "Facebook's web servers" are not even mentioned in the body of the SAC, much less with sufficient factual allegations to show how they "intercepted" the contents of any communications. Plaintiffs' remaining allegations—that "computer code" or Facebook's "plan" can constitute a device—lack any legal support. *See Potter v. Havlicek*, 2008 U.S. Dist. LEXIS 122211, at *23 (S.D. Ohio June 23, 2008) (computer software not a "device" under Wiretap Act).

2. Section 2511(2)(d) Exempts Facebook From Liability Because Facebook Was a Party to the Communication and Also Because Facebook Had Consent

The Wiretap Act provides an exemption to liability where a person is "a party to the communication or one of the parties to the communication has given prior consent." 18 U.S.C. § 2511(2)(d). Plaintiffs concede that Facebook only received a copy of the referer URL because *their* browsers sent it *to Facebook*. (SAC ¶ 60.) *See Crowley*, 166 F. Supp. 2d at 1269 (dismissing Wiretap Act claim where alleged interceptor "merely received the information transferred to it by [Plaintiffs], an act without which there would be no transfer"). Plaintiffs' assertion that they were unaware that their computers were sending referer URLs to Facebook is irrelevant. Courts have routinely held that a party to a communication is exempt from the Wiretap Act, even if they were an unintended recipient of the communication. *See United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964) (that the caller intended to reach a different recipient did not negate application of the party exemption); *Ideal Aerosmith, Inc. v. Acutronic U.S., Inc.*, 2007 U.S. Dist. LEXIS 91644, at *13-14 (W.D. Pa. Dec. 13, 2007) (that defendant was unintended recipient of communication had no legal bearing on whether "party exemption" to Wiretap Act applied). Moreover, to hold that a third-party server that receives a GET request has somehow "intercepted" communications from an Internet user merely because the user was not aware that their computer sent the request would place a large majority of webpage content providers in violation of the Wiretap Act.

Even if the "party" exemption does not apply, there is no claim because the first-party website consented to Facebook's receipt of the alleged communication. 18 U.S.C. § 2511(2)(d) (providing exemption where "one of the parties to the communication has given prior consent"); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1029-30 (N.D. Cal. 2014) (dismissing Wiretap Act claim where one party to the communication consented). Plaintiffs concede that these first-party webpages have purposefully incorporated a code that by normal operation of the Internet would send a second GET request to Facebook to display Facebook content. (SAC ¶¶ 49, 60.) Thus, the first-party website consented to their communications being sent to Facebook by choosing to display Facebook's Like button. *See Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D.

Wash. 2001) (finding consent because "it is implicit in the web pages' code instructing the user's computer to contact Avenue A . . . that the web pages have consented to Avenue A's interception of the communication between them and the individual user").

3. Facebook's Alleged Conduct Is Not Subject to the Wiretap Act Because It Is Part of Facebook's Ordinary Course of Business

The Wiretap Act also creates an exception for interceptions conducted by an electronic communications service provider occurring in "the ordinary course of its business." *See In re Google Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *33 (N.D. Cal. Dec. 3, 2013). The ordinary course of business exception applies to "protect[] a provider's customary and routine business practices." *Id.* For example, in *In re Google Privacy Policy Litigation*, the court found that that Google's scanning of emails for targeting advertising purposes was "furthering its 'legitimate business purposes'—including advertising." *Id.* at *35. Similarly, in *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012), the Tenth Circuit held that where an ISP allowed another company to conduct a test collection of its customers' Internet browsing histories, the ISP was protected from liability because the test gave the ISP "access to no more of its users' electronic communications than it had in the ordinary course of its business as an ISP." *Id.* at 1250. While courts in this district have applied different standards for application of the exception,[11] the conduct complained of here is exempt under any formulation of the standard.

Plaintiffs acknowledge that the process by which Facebook receives referer URLs is not unique to Facebook. Rather, webpages often are assembled from information residing on third-party servers. (SAC ¶ 36.) Obtaining the information from such third parties requires a GET request through which "the detailed URL from the first domain is acquired by the third-party." (*Id.* ¶¶ 37-38.) Plaintiffs thus concede that Facebook acquires the referer URL through the

[11] *Compare In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *33 (exempting "a provider's customary and routine business practices"), *with Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 844 (N.D. Cal. 2014) (exempted activities must be "related or connected to an electronic communication provider's service"), and *with In re Google, Inc. Gmail Litig.*, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013) ("*Gmail*") (exempted activities must "facilitate[] . . . or [be] incidental to the transmission of [the communication]").

process that is normally employed to display Internet webpages. As such, Facebook's receipt of referer URLs falls under the ordinary course of business exception.

C. Plaintiffs Fail to State a Claim Under Penal Code §§ 631 and 632 (Count III)

The allegations in the SAC do not give rise to a cause of action under the California Invasion of Privacy Act ("CIPA"), Penal Code §§ 631 and 632. Not only do Plaintiffs fail to adequately allege the elements of §§ 631 and 632, they also fail to identify a single communication that Facebook allegedly "eavesdropped" upon.[12]

1. Plaintiffs Do Not Adequately Allege the Elements of a § 631 Violation

To state a claim for wiretapping under § 631, Plaintiffs must plead facts to show that Facebook used a "machine, instrument, or contrivance" to make an "unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument" and, through that connection, obtained the contents of communications. Cal. Penal Code § 631(a). The SAC fails to do so.

First, as in the FAC, Plaintiffs have not alleged that Facebook obtained the contents of any communication. (Order at 18); *see also People v. Suite*, 101 Cal. App. 3d 680, 686 (1980) (dismissing § 631 claim where no "contents" of the communications were obtained). As discussed above (*supra* § IV.B.1), URLs and cookies are not the contents of communications. *Zynga*, 750 F.3d at 1106-07; *see In re Nickelodeon Consumer Privacy Litig.*, 2014 U.S. Dist. LEXIS 91286, at *64 (D.N.J. July 2, 2014) (noting that "courts read CIPA's wiretapping provision and the federal Wiretap Act to preclude identical conduct" and dismissing both claims for failure to allege interception of "contents" of communications).

Second, Plaintiffs have again failed to allege any facts to support their conclusory assertion that Facebook used a "machine, instrument or contrivance." The Court previously held that Plaintiffs failed to satisfy this element. (Order at 18 ("[I]f a cookie is truly a 'contrivance' . . . Plaintiffs must include facts in their pleading to show why it is so. In its current form, the CCAC only defines a cookie as a small text file containing a limited amount of information which sits idly on a user's computer until contacted by a server.").) The SAC does

[12] As discussed in Facebook's prior Motion to Dismiss (Dkt. 44 at 17), CIPA does not apply to electronic communications. Facebook will not re-argue its position here, but preserves the issue.

not make any new allegations to overcome this deficiency but instead provides a laundry list of the elements regularly used in the provision of web content in hopes that the Court might find one to be a "machine, instrument or contrivance." (SAC ¶ 217 (listing, *inter alia*, Plaintiffs' browsers and computing devices, third-party webservers, and Facebook's "plan").) Such conclusory allegations are insufficient. *See Twombly*, 550 U.S. at 555 ("A plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions.").

Third, Plaintiffs have not adequately alleged that Facebook obtained communications "without [] consent," or in an "unauthorized manner." Cal. Penal Code § 631(a). The SAC is distinguishable from the FAC on this issue and thus the Court's previous holding is not dispositive.[13] Specifically, the SAC alleges that the "contents or meaning" that Facebook "attempt[ed] to learn" under § 631 were referer URLs (SAC ¶ 216), whereas Plaintiffs' FAC complained that Facebook accessed a cookie (FAC ¶ 200).

These revised allegations provide an independent basis to dismiss the § 631 claim. As the SAC alleges, Facebook, like any other third-party provider of webpage content, automatically receives the GET request containing referer URLs whenever a person seeks to load a page containing Facebook content. (SAC ¶¶ 36-39, 60.) Plaintiffs' contention that a potential violation of § 631 could turn on an Internet user's awareness of what requests the browser was sending when the individual visits a webpage with third-party content thus is untenable. First, this would potentially criminalize the provision of webpage content by third-party providers. Second, California courts have held that parties to communications cannot be liable under § 631. *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 898-99 (1975) (holding that § 631 does not apply to recordings made by a participants). A participant in a conversation "does not intercept the message while it is in transit." *Id.* Nor can a participant "eavesdrop" or "listen secretly to a private conversation." *Id.*; *accord Membrila v. Receivables Performance Mgmt., LLC*, 2010 WL 1407274, at *2 (S.D. Cal. Apr. 6, 2010) (dismissing claim because § 631 "applies only to

[13] The Order reasoned that Plaintiffs had adequately alleged that the "tracking of [Plaintiffs'] browsing activity" was unauthorized, even though Facebook was a party to the communication, because Plaintiffs allegedly were unaware that they were communicating with Facebook via cookies. (Order at 18.)

eavesdropping by a third party and not to recording by a participant to a conversation"). Moreover, as these mechanisms are "part of the normal operation of the internet" (SAC Ex. I at 3), Plaintiffs impliedly authorized Facebook to receive a communication from them, including a referer URL, when they visited a page containing Facebook content.

2. Plaintiffs Do Not Adequately Allege the Elements of a § 632 Violation

Plaintiffs fail to state a § 632 claim because they fail to allege that Facebook used an "electronic amplifying or recording device" to record a "confidential communication" as required under the statute. Cal. Penal Code § 632(a).

Plaintiffs do not allege that Facebook received any "confidential communications." *See Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002) (§ 632 applies only "if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded"); *Gmail*, 2013 WL 5423918, at *22 (dismissing § 632 claim because email communications are "recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else who has access to the internet"). But even if Plaintiffs had alleged a specific communication that Facebook received, they do not have "an objectively reasonable expectation" of "confidentiality" in the information at issue here, which was shared automatically by their browsers when they visited webpages with Facebook content. The Court concluded as much in its Order: "Plaintiffs could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable because 'Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit . . . .' Plaintiffs 'should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.'" (Order at 12 n.5 (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)).) California courts generally hold that Internet communications are not "confidential" under § 632 because such communications can easily be shared. *Gmail*, 2013 WL 5423918, at *22 (collecting cases).

The SAC also is devoid of any allegations that an "electronic amplifying or recording device" was used. Plaintiffs do not allege that Facebook amplified anything, nor is it apparent from their allegations how the process they describe involved a "recording device." Courts

generally have held § 632 to apply to traditional "recording devices" such as audio and video recorders. *E.g.*, *People v. Gibbons*, 215 Cal. App. 3d 1204, 1208 (1989).

3. Plaintiffs Fail to Identify a Single Specific Communication Allegedly Obtained and Therefore Do Not Plead a Plausible Violation of CIPA

Plaintiffs do not identify even a single communication attributable to any named Plaintiff that Facebook allegedly acquired. As the Court noted in its Order, "a list of the named plaintiffs coupled with the same set [of] generalized facts for each one . . . do not suffice to 'nudge' their CIPA claim 'across the line from conceivable to plausible.'" (Order at 18 (quoting *Iqbal*, 556 U.S. at 680).) The SAC does not remedy this problem. The SAC alleges virtually identical facts for each Plaintiff—that each "visited websites . . . which Facebook tracked" and the "URLs for many of these websites contain detailed file paths . . . ." (SAC ¶¶ 113-124.) These generalized facts do not identify a single communication Facebook allegedly acquired and thus fail to satisfy Plaintiffs' pleading burden. *Twombly*, 550 U.S. at 555 (pleadings must "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests").

D. Plaintiffs Fail to State a Claim under the SCA (Count II)

Plaintiffs also fail to remedy the deficiencies in their SCA claim identified by the Court—namely their failure to allege that any information was obtained "while it is in electronic storage." (Order at 15-17.) The SAC also does not allege that Facebook accessed "a facility through which an electronic communication service is provided," nor that any information obtained was without or exceeding "authorization." 18 U.S.C. § 2701(a).

No electronic storage. Plaintiffs fail to show that Facebook accessed any communications in "electronic storage." *Id.* § 2701(a). Electronic storage is "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission . . . ." and "storage of such communication by an electronic communication service for purposes of backup protection . . . ." *Id.* § 2510(17)(A)-(B). The Court previously dismissed the SCA claim because Plaintiffs' allegations of access to "persistent cookies" "cannot be reconciled with the temporary nature of storage contemplated by the statutory definition." (Order at 17.) *See In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001) ("The

cookies' long-term residence on plaintiffs' hard drives places them outside of [the SCA]'s definition of 'electronic storage' and, hence, [the SCA's] protection."). The SAC still acknowledges that cookies are "persistent," lasting "for months or years," (SAC ¶ 55) and therefore has not cured this fatal defect.

Plaintiffs cannot salvage their claim with allegations that copies of referer URL requests are stored in two browser-managed files: (1) the toolbar, which they claim is "temporary, intermediate, and incidental to" electronic transmission and (2) the browsing history, which they claim is for back-up protection. (*Id.* ¶¶ 204-207.) These new allegations are wholly insufficient. First, the SAC does not explain how the toolbar stores communications "in the middle of a transmission;" and thus cannot satisfy the requirements for electronic storage under § 2510(17)(A). *In re Toys R Us, Inc. Privacy Litig.*, 2001 U.S. Dist. LEXIS 16947, at *10-11 (N.D. Cal. Oct. 9, 2001) (the SCA "only protects electronic communications stored for a limited time in the middle of a transmission, i.e., when an electronic communication service temporarily stores a communication while waiting to deliver it." (citation omitted)). Plaintiffs claim that "a copy of the [] URL request" is no longer in the toolbar after a user leaves a webpage (SAC ¶ 206), but do not allege that it was delivered anywhere, as would be required for storage in the toolbar to be "in the middle of a transmission." Second, Plaintiffs allege that their own browsers are electronic communications services providing backup storage under § 2510(17)(B) (*Id.* ¶ 199), but this is contrary to law. *See Garcia v. City of Laredo*, 702 F.3d 788, 792 (5th Cir. 2012) ("electronic storage" does not include "information that an individual stores to his hard drive or cell phone"); *Doubleclick, Inc.*, 154 F. Supp. 2d at 511 ("cookies" resident on plaintiffs' computers do not fall into § 2510(17)(B) because plaintiffs are not "electronic communication service" providers); *Thompson v. Ross*, 2010 U.S. Dist. LEXIS 103507, at *18-19 (W.D. Pa. Sept. 30, 2010) (plaintiffs' computers are not electronic service providers and thus cannot provide backup protection under § 2510(17)(B)).

Finally, Plaintiffs' new allegations regarding storage locations are only relevant if these locations actually stored electronic communications and Facebook actually accessed these locations, but Plaintiffs make no such allegation. To the contrary, the SAC alleges that Plaintiffs'

browsers *sent* Facebook the information at issue in the form of a GET request. (SAC ¶ 60.) *See In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *11-14 (dismissing SCA claim where plaintiffs alleged that cookies were accessed in electronic storage because cookies were placed in random access memory ("RAM"), but failed to plead that the defendant's access occurred while the cookies were in RAM, rather than on the hard drive). Additionally, Plaintiffs' interpretation would lead to the absurd result that any third-party provider of webpage content that receives referer URL information—something that happens "often" according to Plaintiffs—has accessed information in "electronic storage" and may be liable for violating the SCA. (SAC ¶¶ 36-38.)

No facility. Plaintiffs do not allege that Facebook accessed "a facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1). Plaintiffs claim that "personal computing devices," "web-browsers," and "browser-managed files" constitute facilities (SAC ¶ 199), but this theory "runs contrary to the vast majority of published and non-published decisions that have considered the issue." *In re Nickelodeon*, 2014 U.S. Dist. LEXIS 91286, at *60; *iPhone App. Litig. II*, 844 F. Supp. 2d at 1057 (collecting cases and concluding that "an individual's computer, laptop, or mobile device" does not "fit[] the statutory definition of a facility") (internal quotations omitted). The computers covered by the SCA "are not computers that *enable* the use of an electronic communication service, but instead are facilities that are *operated by* electronic communication service providers . . . ." *Garcia*, 702 F.3d at 792 (internal quotations omitted). Indeed, interpreting "facilities" to include Plaintiffs' computers would lead to the absurd result that "electronic service providers" and "users" of Plaintiffs' computers would be permitted to authorize access to Plaintiffs' computers under exceptions to liability provided in § 2701(c)(1) and (c)(2). *See Crowley*, 166 F. Supp. 2d at 1271 (if plaintiff's personal computer could be a facility, that would lead to the nonsensical result that "the provider of a communication service could grant access to one's home computer to third parties" under § 2701(c)(1)); *iPhone App. Litig. II*, 844 F. Supp. 2d at 1063 (if plaintiff's personal computer was a facility, websites would become "users" of the electronic service provided by the personal computer, and could therefore authorize access to any communication intended for that website under § 2701(c)(2)). The SCA therefore requires that communications were accessed "while those communications

[were] stored on someone else's computer." *In re Nickelodeon*, 2014 U.S. Dist. LEXIS 91286, at *59. The SAC alleges that Facebook received information stored in cookies on Plaintiffs' own browsers, not any third-party location. Other courts have considered and rejected such claims. *See id.* at *61. ("[T]he SCA is not concerned with access of an individual's personal computer.").

E. Plaintiffs Fail to State a Claim for Fraud (Count VIII)

Plaintiffs allege actual and constructive fraud under California Civil Code §§ 1572 and 1573, respectively. (SAC ¶¶ 263, 264.) Plaintiffs appear to allege two species of actual fraud—false representations and suppression. (*Id.* ¶¶ 265, 266.) Specifically, Plaintiffs allege that Facebook falsely represented that it would delete certain cookies when users logged out, and suppressed knowledge that this was not occurring. Allegations for claims under both §§ 1572 and 1573 must meet Rule 9(b)'s heightened pleading standard by alleging "'the who, what, when, where, and how' of the misconduct charged." *Vess*, 317 F.3d at 1106 (citations omitted). Plaintiffs fail to do so.

1. Plaintiffs Fail to State a Claim for Actual Fraud (§ 1572)

To plead actual fraud under a theory of false representations (§ 1572(1)) or suppression (§ 1572(3)), Plaintiffs must allege that (1) Facebook made a false representation or suppressed a material fact, (2) Facebook had knowledge of the falsity or was without sufficient knowledge to warrant a representation, (3) Facebook intended to induce Plaintiffs into using Facebook, (4) Plaintiffs acted in reliance upon the material false representation or would have acted differently had Facebook not misrepresented or suppressed the alleged facts, and (5) Plaintiffs suffered damages as a result. *S. Tahoe Gas Co. v. Hofmann Land Improv. Co.*, 25 Cal. App. 3d 750, 765 (1972). Additionally, to plead suppression under Civ. Code § 1572(3), Plaintiffs must allege that Facebook was under a duty to disclose the facts allegedly suppressed. *Moncada*, 221 Cal. App. 4th at 775. Plaintiffs fail to plead multiple elements with specificity under Rule 9(b) and make no allegations at all regarding other required elements.

a. Plaintiffs Fail to Allege that Facebook Acted With Intent

Fraud requires intent to induce, not just knowledge of falsity. *Engalla v. Permanente Med. Grp., Inc.*, 15 Cal. 4th 951, 976 (1997). Specifically, liability under § 1572 requires intent

to induce conduct or reliance of the *plaintiff*. *Blickman Turkus, LP v. MF Downtown Sunnyvale, LLC*, 162 Cal. App. 4th 858, 869 (2008) (stating that both suppression and false representation require intent to induce). In *Levin v. Citibank, N.A.*, plaintiff alleged "fraudulent concealment" and claimed that defendant's actions were "deceptive." 2009 WL 3008378, at *5 (N.D. Cal. Sept. 17, 2009). The court dismissed plaintiff's fraud claim because plaintiff's allegations were "conclusory," and because plaintiff failed to allege that defendant had acted with intent to induce any specific conduct on the part of the plaintiff. *Id*.

Here as well, the SAC fails to allege that Facebook intended to induce reliance or conduct. Remarkably absent is any allegation that Facebook made false statements, or suppressed material facts, to induce Plaintiffs to do anything. *See Senah, Inc v. Xi'an Forstar S & T Co.*, 2014 WL 3044367, at *4 (N.D. Cal. July 3, 2014) (plaintiff's "bare allegation" that defendant concealed material facts was not enough to infer defendant intended reliance). Plaintiffs quote from emails between Facebook personnel (SAC ¶¶ 66, 68, 69, 73-78), but none of these quotes demonstrate any intent to defraud Plaintiffs, nor are they ever connected to any alleged misrepresentation supposedly made to Plaintiffs. *See DeLeon v. Wells Fargo Bank, N.A.*, 2011 WL 311376, at *8 (N.D. Cal. Jan. 28, 2011) (dismissing in part because "knowing, intentional fraud" requires more than mistakes stemming from "one department not talking to another"). To the contrary, many of the emails discuss Facebook's efforts to ensure user privacy. (SAC ¶¶ 66, 72, 73, 74, 76.) For example, in several emails a Facebook employee notes potential privacy concerns and requests that certain aspects of cookies be adjusted immediately in response. (*Id.* ¶¶ 66, 72-74.) These emails do not suggest intent to defraud; instead, they demonstrate that Facebook acted quickly to remedy potential or perceived privacy concerns regarding its use of cookies.

b. Plaintiffs Fail to Allege that they Relied on the Alleged Misrepresentation

Plaintiffs must allege facts sufficient to show that they relied on an allegedly fraudulent statement. *Great Am. Ins. Co. v. Wexler Ins. Agency, Inc.*, 2000 WL 290380, at *22 (C.D. Cal. Feb. 18, 2000). Failure to allege reliance with specificity as required by Rule 9(b) is grounds for dismissal. *See Kearns*, 567 F.3d at 1126. Plaintiffs make no such allegations. As an initial

matter, the only statement that Plaintiffs have conceivably identified as misleading is the alleged Help Center entry regarding deletion of certain cookies on logout, but they do not identify when that statement was made, that the statement was false at the time it was made, or that they actually read it. *See Smith v. Allstate Ins. Co.*, 160 F. Supp. 2d 1150, 1152 (S.D. Cal. 2001) (dismissing fraud claim for failure to allege the time, place, and content of the alleged misrepresentation and that it was false at the time it was made); *Patterson v. Bayer Healthcare Pharm., Inc.*, 2015 WL 778997, at *13 (E.D. Cal. Feb. 24, 2015) ("Absent . . . is where or when [plaintiff] was exposed to the [fraudulent] materials."). Moreover, Plaintiffs do not plead factual allegations showing that any specific misrepresentation was "an immediate cause" of Plaintiffs' actions and that absent the misrepresentation, Plaintiffs "would not, in all reasonable probability, have entered into the contract[.]" *Engalla*, 15 Cal. 4th at 976 (internal quotations omitted). Conclusory statements of reliance are insufficient under Rule 9(b). *Mazur v. eBay Inc.*, 2008 WL 618988, at *13 (N.D. Cal. Mar. 4, 2008) ("Plaintiff pleads reliance in a conclusory manner and merely regurgitates the statements that allegedly induced reliance."). Again, this is fatal to their fraud claim.

Likewise, Plaintiffs' suppression theory fails as they must allege that they were unaware of the allegedly suppressed information and that they would have acted differently otherwise. *Moncada*, 221 Cal. App. 4th at 775. They have not done so.

c. Plaintiffs Fail to Allege Damages

To state a claim for fraud, Plaintiffs must allege that they suffered damages as a direct result of the fraud. *Moncada*, 221 Cal. App. 4th at 776 ("'Whatever form it takes, the injury or damage must not only be distinctly alleged but its causal connection with the reliance on the representations must be shown.'") (citation omitted). Plaintiffs nowhere allege damages arising from the alleged fraud and thus their claim should be dismissed. *Marble Bridge Funding Grp. v. Euler Hermes Am. Credit Indem. Co.*, 2015 WL 971761, at *5 (N.D. Cal. Mar. 2, 2015) ("Even at the pleading stage, the complaint must show a cause and effect relationship between the fraud and damages sought; otherwise no cause of action is stated.") (internal quotations omitted).

d. Plaintiffs Fail to Allege Facebook Had a Duty to Disclose

Plaintiffs offer conclusory allegations of suppression, but fail to allege that Facebook had a duty to disclose. This alone is grounds for dismissal of their suppression claim. *Monreal v. GMAC Mortg., LLC*, 948 F. Supp. 2d 1069, 1078 (S.D. Cal. 2013) (dismissing an action for fraudulent concealment where plaintiff failed to allege how defendants had a duty to disclose); *Goodman v. Kennedy*, 18 Cal. 3d 335, 346 (1976) (sustaining dismissal where there was no allegation of a duty to disclose). The allegation of a duty to disclose must further be accompanied by specific factual allegations showing the existence of such a duty. *Gerawan Farming, Inc. v. Rehrig Pac. Co.*, 2012 WL 691758, at *9 (E.D. Cal. Mar. 2, 2012) *aff'd*, 587 F. App'x 654 (Fed. Cir. 2014). Plaintiffs fail to allege a duty, let alone specific facts in support.

2. Plaintiffs Fail to State a Claim for Constructive Fraud (§ 1573)

Constructive fraud under § 1573 requires that the plaintiff allege facts to show "(1) a fiduciary or confidential relationship; (2) an act, omission or concealment involving a breach of that duty; (3) reliance; and (4) resulting damage." *Dealertrack, Inc. v. Huber*, 460 F. Supp. 2d 1177, 1183 (C.D. Cal. 2006).[14] Plaintiffs' allegation that Facebook breached its duty "not to track, intercept, or access its users' Internet communications, computers, or web-browsers while they were logged-off of Facebook" is insufficient. (SAC ¶ 268.)

This claimed "duty" is just the contractual obligation that Plaintiffs allege, not the kind of confidential or fiduciary duty that "distinguishes constructive fraud." *Byrum v. Brand*, 219 Cal. App. 3d 926, 937-38 (1990). No such confidential or fiduciary relationship is alleged here, nor does one plausibly exist. *Portney v. CIBA Vision Corp.*, 2008 WL 5505517, at *5 (C.D. Cal. July 17, 2008) (holding that the exchange of confidential information does not by itself create a confidential relationship). "'A confidential relation exists between two persons when one has gained the confidence of the other and purports to act or advise with the other's interest in mind.'" *Patriot Sci. Corp. v. Korodi*, 504 F. Supp. 2d 952, 966 (S.D. Cal. 2007) (dismissing constructive fraud claim) (quoting *Davies v. Krasna*, 14 Cal. 3d 502, 510 (1975)). As Plaintiffs

[14] Section 1573 also applies where a law specifically states a particular act or omission is fraudulent, but Plaintiffs cite no particular acts. *Id.*

have failed to allege a fiduciary or confidential relationship, their claim fails as a matter of law. *Gilmore v. Am. Mortg. Network*, 2012 WL 6193843, at *12 (C.D. Cal. Dec. 10, 2012) (dismissing a constructive fraud claim for failing to allege a fiduciary or confidential relationship).

A claim for constructive fraud also must allege damages resulting from the alleged fraud. *See Jones*, 90 Cal. App. 4th at 471. As explained above in § IV.A.1., Plaintiffs fail to allege specific damages that were directly caused by the alleged fraud. For this independent reason, Plaintiffs' constructive fraud claim should be dismissed.

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

Plaintiffs allege that Facebook accessed Plaintiffs' computers in a manner that violates Penal Code §§ 502(c)(1), (2), and (6)-(8). Among other requirements for stating a claim under § 502(c), Plaintiffs must allege that (1) Facebook acted "without permission" and (2) they "suffer[ed] damage or loss by reason of [the] violation." *Id.* § 502(c)(1), (2), (6)-(8), (10); *id.* § 502(e)(1). And for claims under § 502(c)(8), Plaintiffs must also allege that Facebook introduced a "computer contaminant" into Plaintiffs' computers. *Id.* § 502(c)(8). The SAC fails to allege any of these requirements.

No Damages. In its previous Order, the Court dismissed Plaintiffs' § 502 claim for lack of standing, explaining that the statute "require[s] a plausible economic injury for standing." (Order at 13 (citing Cal. Penal Code § 502(e)(1)).) The SAC does nothing to change this outcome. As described above, none of the revisions to the SAC establishes any plausible economic injury, and their § 502 claims should be dismissed. *See In re Apple & ATTM Antitrust Litig.*, 2010 U.S. Dist. LEXIS 98270, at *23-24 (N.D. Cal. July 8, 2010) (loss of access to smartphone is not damage or loss under § 502).

Not Without Permission. Facebook's alleged use of cookies was not "without permission." Section 502 is a criminal "anti-hacking" statute, and courts interpret "without permission" narrowly. *Custom Packaging Supply, Inc. v. Phillips*, 2015 WL 8334793, at *3 (C.D. Cal. Dec. 7, 2015). Liability generally requires allegations that the defendant circumvented a technical or code-based barrier. *See, e.g.*, *Facebook, Inc. v. Power Ventures, Inc.*, 2010 U.S.

Dist. LEXIS 93517, at *24 (N.D. Cal. July 20, 2010); *Enki Corp. v. Freedman*, 2014 WL 261798, at *3 (N.D. Cal. Jan. 23, 2014) (dismissing for failure to allege circumvention of technical or code based barrier). Writing cookies does not require any circumvention of technical or code-based barriers; it is a widely used feature and Plaintiffs do not allege otherwise.[15]

No Contaminant. Plaintiffs' claim under § 502(c)(8) fails because they do not adequately allege that Facebook introduced a "computer contaminant" into Plaintiffs' computers. Cal. Penal Code § 502(c)(8).[16] A "contaminant" must "modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network." Cal. Penal Code § 502(b)(10). But Plaintiffs do not allege that Facebook's cookies have any effect on the information held in a user's computer memory. Rather, browsers automatically send copies of information stored in cookies when users access certain URLs. Also, § 502(c)(8) "appears to be aimed at 'viruses or worms,' and other malware that usurps the normal operation of the computer or computer system." *iPhone App. Litig. I*, 2011 WL 4403963, at *13 (stating that "it is not clear to the Court how [§] 502(c)(8) applies to" voluntarily downloaded applications that secretly copied and shared plaintiffs' personal information). Plaintiffs do not allege that Facebook's cookies operate as viruses or worms or that they usurp the normal operation of a user's computer. In fact, Plaintiffs admit that cookies have a range of functions and information is regularly sent and received by browsers when they interact with web servers. (SAC ¶ 52.) As such, cookies are "standard web browser function[s]," which are not contaminants under the statute. *See In re*

[15] The SAC also alleges that (1) Facebook employees filed a patent application that contemplates a cookie that "bypasses security settings" (SAC ¶¶ 79-84) and (2) Facebook circumvented the Privacy Preferences Project system ("P3P")—a protocol developed by Microsoft for certain versions of its Internet Explorer browser to, among other things, help manage what information websites obtain from visitors' browsers based on the websites' privacy policies (*id.* ¶¶ 85-101). But Plaintiffs do not allege that Facebook practiced this patent, that Facebook ever circumvented Plaintiffs' browser settings, that Facebook's collection of information was inconsistent with its Privacy Policy, or that any Plaintiffs even used the versions of Internet Explorer that used P3P. Moreover, the Privacy Policy informed users that Facebook used these cookies. Facebook did not circumvent any technical barriers, and Plaintiffs have not alleged otherwise.

[16] "Computer contaminants" include "viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer . . . ." Cal. Penal Code § 502(b)(10).

Facebook Privacy Litig., 2011 U.S. Dist. LEXIS 147345, at *14 (N.D. Cal. Nov. 22, 2011), *aff'd in part and rev'd in part on other grounds*, 572 F. App'x 494 (9th Cir. 2014).

G. Plaintiffs Fail to State a Claim for Trespass to Chattels (Count IX)

Plaintiffs claim that Facebook's alleged failure to delete certain cookies is a trespass to Plaintiffs' computers, but this claim fails for several reasons. As an initial matter, Plaintiffs do not allege actual injury, as discussed in § IV.A.1. above. *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1351 (2003) (holding "that some actual injury must have occurred in order for a trespass to chattels to be actionable"). This pleading defect is fatal. *iPhone App. Litig. I*, 2011 WL 4403963, at *14 (dismissing trespass claim for failing to allege identifiable injury).

Additionally, a claim for trespass to chattels requires either degradation of the value or condition of personal property or deprivation of the use of that property for a substantial time. *Hamidi*, 30 Cal. at 1351. Even unauthorized access to a computer system without degradation or deprivation does not constitute a trespass. *See Id*. at 1347. Plaintiffs' conclusory claim that Facebook interfered with their "personally identifiable information" and personal computers is insufficient. (SAC ¶ 273.) First, although Plaintiffs refer to "personally identifiable information," the only information at issue is referer URLs in which Plaintiffs do not have a property interest. (*See infra* § IV.L.) Moreover, Plaintiffs do not allege that they lost any value in this information or were deprived of its use. (*See supra* § IV.A.1.) Likewise, regarding their personal computers, Plaintiffs do not allege either "actual or threatened damage to [their] computer hardware or software [or] interference with its ordinary and intended operation." *Hamidi*, 30 Cal. 4th at 1352-53. In fact, Plaintiffs concede that cookies facilitate rather than impair their use of web browsers. (SAC ¶¶ 52, 56.) Because Plaintiffs have not alleged damage to their hardware or software, and have not alleged interference with the use or function of their computers, Plaintiffs' claim should be dismissed. *See LaCourt*, 2011 U.S. Dist. LEXIS 50543, at *20 (dismissing claim for trespass to chattels where defendant wrote persistent cookies to plaintiffs' browsers because plaintiffs failed to allege interference with their computers' functioning beyond "trivial" presence of the cookies themselves).

H. Plaintiffs Fail to State a Claim for Intrusion upon Seclusion (Count V)

Plaintiffs fail to adequately allege that Facebook "(1) intru[ded] into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998).

No Intrusion. To show the first element, Plaintiffs must allege that Facebook "penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff" and that Plaintiffs "had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source." *Id.* at 231-32. Plaintiffs do not allege either.

First, Plaintiffs' claimed expectation of privacy in the information at issue is not objectively reasonable. As this Court stated in its Order, "Plaintiffs could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable because 'Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit . . . .'" (Order at 12 n.5 (quoting *Forrester*, 512 F.3d at 510)); *see also People v. Stipo*, 195 Cal. App. 4th 664, 669 (2011) (no expectation of privacy in routine information that is "voluntarily turned over in order to direct the third party's servers") (citation omitted); *Zynga*, 750 F.3d at 1107 ("[R]eferer header information . . . includ[ing] the user's Facebook ID and the address of the webpage from which the user's HTTP request to view another webpage was sent . . . functions as a 'name' . . . [and] an 'address.'") (citation omitted). None of Plaintiffs' new allegations overcome the Court's prior reasoning.[17]

Second, Plaintiffs do not allege that Facebook obtained any information attributable to any particular Plaintiff. Courts require sensitive and confidential information to be specifically alleged, and have held this requirement is not satisfied where a plaintiff alleges only a generalized privacy interest. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1040 (plaintiffs' allegation that they have a "legally protected privacy interest and reasonable expectation of privacy in email

[17] Plaintiffs' claim that an expectation of privacy was reasonable because Facebook allegedly "promised users it would not track their communications or access their computing devices or web-browsers while they were logged-off of Facebook" (SAC ¶ 226) fails because (1) the Help Center page quoted does not say anything about tracking communications or accessing computer devices, but rather just discusses "cookies that identify your particular account" (*Id.* ¶¶ 23, 63) and (2) Plaintiffs do not allege when that representation was made or that they ever saw it.

generally . . . regardless of the specific *content* in the emails . . . fails as a matter of law"). As Plaintiffs have not identified any of their specific, private information that was allegedly obtained, their claim must be dismissed. *Id.* at 1040-42.

Not Highly Offensive. Plaintiffs cannot show that the alleged invasion of privacy was "*highly offensive to a reasonable person.*" The common law "set[s] a high bar" for this claim. *Low*, 900 F. Supp. 2d at 1025. An intrusion is only highly offensive if it is so serious and unwarranted as to constitute an egregious breach of social norms. *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 295 (2009). To determine whether an alleged intrusion is highly offensive, courts consider "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." *Wilkins v. Nat'l Broad. Co.*, 71 Cal. App. 4th 1066, 1076 (1999) (citation omitted); *see Hernandez*, 47 Cal. 4th at 295 (dismissing intrusion claim where surveillance was limited in scope and was beneficially motivated by legitimate business concerns). Plaintiffs' conclusory allegations are insufficient.

In re Google, Inc. Privacy Policy Litigation, 58 F. Supp. 3d 968 (N.D. Cal. 2014), is instructive. There, the Plaintiffs alleged that Google comingled information collected during the plaintiffs' use of Google products, such as Google search queries, address lookups, and YouTube history, with information tied to plaintiffs' Gmail accounts, such as name and identity, private contact list, and the contents of email communications. *Id.* at 973-74. The court held that this conduct did not constitute a highly offensive conduct, noting that "[c]ourts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms." *Id.* at 985.

Here, Plaintiffs allege that Facebook's routine receipt of referer URLs was highly offensive because Facebook failed to delete certain cookies when users logged out. The conduct Plaintiffs identify is no different than the "disclosure of common, basic digital information" that courts have held insufficient to state an invasion of privacy claim. *See Low*, 900 F. Supp. 2d at 1025 (no serious invasion of privacy where defendant allegedly disclosed user browsing history coupled with digital identification information to third parties in violation of its policies);

Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 992 (2011) (sharing plaintiffs' ZIP codes, names, and credit card numbers with marketing agency was not highly offensive but rather "routine commercial behavior"); *cf. iPhone App. Litig. II*, 844 F. Supp. 2d at 1063 (disclosure to third parties of unique device identifier number, personal data, and geolocation information did not constitute an egregious breach of privacy under the California Constitution). That Facebook allegedly misled Plaintiffs into believing such information would not be collected does not make the alleged conduct egregious. *See Low*, 900 F. Supp. 2d at 1025 (disclosure of unique identifiers and browsing history was not highly offensive even though defendant allegedly had promised that information it shared would not be personally identifiable). Plaintiffs' intrusion upon seclusion claim should be dismissed.

I. Plaintiffs Fail to State a Claim for Invasion of Privacy (Count IV)

Plaintiffs' invasion of privacy claim fails for similar reasons. The elements of an invasion of privacy claim under Article 1, section 1, of the California Constitution are similar to those for intrusion upon seclusion. *See Heidorn v. BDD Mktg. & Mgmt. Co.*, 2013 U.S. Dist. LEXIS 177166, at *45 (N.D. Cal. Aug. 19, 2013) (the California Supreme Court "looks to the common law governing invasion of privacy to define the contours of the state constitutional right to privacy") (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 15, 26 (1994)). To assert an actionable invasion, a plaintiff must show "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of the privacy interest." *Int'l Fed'n of Prof'l & Tech. Eng'rs, Local 21, AFL-CIO v. Super. Ct.*, 42 Cal. 4th 319, 338 (2007).

As discussed above, Plaintiffs' claims fail because they have not identified any reasonable expectation of privacy that would constitute an egregious breach of social norms. *See Low*, 900 F. Supp. 2d at 1025 (dismissing both constitutional and common law invasion of privacy claims as plaintiffs had failed to allege a sufficiently serious violation of privacy under either standard); *Folgelstrom*, 195 Cal. App. 4th at 993 (same); *iPhone App. Litig. II*, 844 F. Supp. 2d at 1063. Plaintiffs also do not allege that Facebook obtained any particular information attributable to any particular Plaintiff. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1040; *Zbitnoff v. Nationstar Mortg.*,

LLC, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014) (dismissing constitutional privacy claim for failure to plead "with the required specificity" where she did "not identify exactly what private information defendants are alleged to have disclosed").

Nor does Plaintiffs' claim identify any legally protected privacy interest. *Hill*, 7 Cal. 4th at 35 (plaintiff asserting violation of constitutional right to privacy must identify specific, legally protected privacy interest). Courts have construed this claim narrowly to find protected interests in only certain types of particularly sensitive personal information. *See, e.g.*, *Susan S. v. Israels*, 55 Cal. App. 4th 1290, 1295-98 (1997) (confidential mental health records); *Urbaniak v. Newton*, 226 Cal. App. 3d 1128, 1140-41 (1991) (HIV status). Moreover, the SAC fails to specify a single webpage that any Plaintiff visited, let alone that their visit to that webpage was "tracked" by Facebook and that such visit involved any sensitive personal information. Without such allegations, any supposed privacy interest is merely hypothetical, not plausible, as required under federal pleading standards. *Iqbal*, 556 U.S. at 680; *Zbitnoff*, 2014 WL 1101161, at *4 (dismissing privacy claim where plaintiff "merely state[d] that she had a 'reasonable expectation that defendants would preserve the privacy of [p]laintiff's private information'") (citation omitted).[18]

Plaintiffs try to overcome this pleading defect by listing a number of statutes that they assert give rise to legally protected privacy interests. Plaintiffs allege, without further detail, that the Fourth Amendment, the Pen Register Act, and Facebook's own privacy policies create privacy rights that are implicated by Facebook's conduct. (SAC ¶ 225.) None of these statutes or policies establish that the privacy of referer URLs is a legally recognized privacy right.

First, even if the question of a protectable privacy interest for purposes of a civil claim is coextensive with Fourth Amendment jurisprudence (which Facebook does not concede), the Fourth Amendment does not embody a social norm that referer URLs should be legally protected information. (Order at 12 n.5 (quoting *Forrester*, 512 F.3d at 510).) The SAC cites *Riley v.*

[18] While the SAC cites *Ung v. Facebook* (SAC ¶¶ 161-64; *id.* Ex. HH), the Superior Court's demurrer ruling did not take into account the binding precedent and other case law that this Court discussed in its previous Order (Order at 12 n.5 (citing, among others, *Forrester*)) or the other arguments and case law discussed above in this section and in the previous section H. For these reasons, the *Ung* decision on this issue is inapposite here, in addition to being incorrectly decided.

California, but *Riley* is inapposite. The Supreme Court in *Riley* held that the "search incident to arrest" exception for a warrant did not extend to a cell phone because the rationales for the exception—officer safety and evidence destruction—were not present, and search of a cell phone implicated far different privacy concerns than the traditional pocket-sized items at issue in prior cases. 134 S. Ct. 2473 (2014). While the Court noted in dicta that Internet browsing history might reveal private interests, it did not consider whether the information was protected by the Fourth Amendment. *Riley* had no cause to consider exceptions to Fourth Amendment protection, such as for information voluntarily disclosed. Thus, it cannot stand for the proposition that the Fourth Amendment creates legal protection for referer URLs that are transmitted to Internet content providers to fulfill browsing requests. *Id.* at 2489-91.

The Pen Register Act applies to information obtained with a "pen register" or a "trap and trace device . . . ." 18 U.S.C. § 3121(a). Since neither device is used to obtain referer URLs, it is not apparent how this statute could embody a social norm that referer URLs should be legally protected information. Furthermore, even the Pen Register Act acknowledges that electronic service providers may use such devices in relation to the operation of an electronic communication service. 18 U.S.C. § 3121(b)(1).

Finally, as described below, Facebook did not violate its terms, and even if it had done so, the right to privacy provided by the California Constitution was not designed to protect against mere alleged contractual breaches. *See Hernandez*, 47 Cal. 4th at 287 (legally protectable privacy interests must be "based on breaches of established social norms, derived from such sources as the common law and statutory enactment").

J. Plaintiffs Fail to State a Claim for Breach of Contract (Count VI)

Plaintiffs allege that Facebook's failure to delete certain cookies upon logout breached a contract between Facebook and users. To plead a claim for breach of contract, a plaintiff must allege (1) there was a contract, (2) plaintiff performed or was excused from performance under the contract, (3) defendant breached the contract, and (4) plaintiff suffered damages from the breach. *Oasis W. Realty, LLC v. Goldman*, 51 Cal. 4th 811, 821 (2011). Plaintiffs' multiple pleading failures mandate dismissal.

1. Plaintiffs Fail to Allege that Facebook Violated any of the Terms Governing its Relationship with Users

The SRR governs Facebook's relationship with its users. Plaintiffs fail to point to any provision in the SRR during the Class Period that Facebook allegedly breached. Instead, Plaintiffs base their breach of contract claim solely on Facebook's alleged statement in its Help Center: "When you log out of Facebook, we remove the cookies that identify your particular account." (SAC ¶ 245.) But Plaintiffs never identify where in their integrated contract with Facebook this statement appears—because it appears nowhere in the SRR. The statement does not appear anywhere in the 367 pages of exhibits they attached. This failure to point to a provision of the contract that was breached is alone grounds for dismissal. *Woods v. Google Inc.*, 2011 WL 3501403, at *3 (N.D. Cal. Aug. 10, 2011) ("In an action for breach of a written contract, a plaintiff must allege the specific provisions in the contract creating the obligation the defendant is said to have breached.").

Plaintiffs neglect to mention that the above-quoted statement appears only on a Facebook Help Center webpage, which Plaintiffs did not attach or even allege was active *during the alleged class period*. Tellingly, Plaintiffs never expressly allege that this Help Center page is part of Facebook's terms. They instead imply that the SRR linked to the Privacy Policy, which linked to various pages in the Help Center as part of a "layered approach." (SAC ¶ 23.) But Plaintiffs' quote regarding a "layered approach" was made by Facebook in 2012, two years *after* the class period, and the quote refers to how the Data Use Policy in particular was structured in 2012: "we use a layered approach, summarizing our practices on the front page and then allowing people to click through *the Policy* for more details." (*Id.* ¶ 22; Ex. I at 9 (emphasis added)). It was the Data Use Policy itself that used this approach, not the SRR or the Help Center.

Even if Plaintiffs' disingenuous description of a layered approach were accurate, the SAC never identifies any section in the SRR that contained hyperlinks to the *specific* Help Center page

with this specific statement.[19] Without that connection, Plaintiffs cannot argue that this statement was somehow incorporated into the SRR. *See Chan v. Drexel Burnham Lambert, Inc.*, 178 Cal. App. 3d 632, 643-44 (1986) (effective incorporation "requires the incorporating document to refer to the incorporated document with particularity").[20] As such, Plaintiffs cannot rely on the Help Center as the basis of their breach of contract claim. *Dunkel v. eBay Inc.*, 2014 WL 1117886, at *4 (N.D. Cal. Mar. 19, 2014) ("As Plaintiffs have not adequately alleged that the "Help" articles are included in the contract between themselves and Defendant, their allegations that Defendant acted contrary to these articles do not suffice to state a breach."); *Woods*, 2011 WL 3501403, at *3-4 (finding Help Center pages not incorporated into agreement). As a result, they cannot identify any contractual term that was even arguably breached, and as such their claim fails as a matter of law. *Id.*; *see also Frances T. v. Vill. Green Owners Ass'n*, 42 Cal. 3d 490, 512-13 (1986) (affirming demurrer where the Plaintiff alleged a contract breach but provided no contract provision that had been violated).

2. Plaintiffs Fail to Plead Damages

In a breach of contract claim, damages must be "clearly ascertainable in both their nature and origin." Cal. Civ. Code § 3301. Additionally, a defendant's breach must be the direct and proximate cause of the damages. *Troyk v. Farmers Grp., Inc.*, 171 Cal. App. 4th 1305, 1352 (2009). Plaintiffs' allegations do not satisfy these requirements. Plaintiffs claim they did not receive the benefit of the bargain for which they supposedly paid "valuable consideration . . . ." (SAC ¶ 252.) But Plaintiffs do not specify *what* benefit they were denied or damages that

[19] The Privacy Policy does not link to this Help Center page either. It linked only to the following Help Center pages: "help page for complaints about our privacy policies or practices;" "help page to report use by a child under age 13;" "help page with info to help parents talk to children about safe internet use." (SAC Exs. E-G.)

[20] Additionally, the Help Center pages are not easily available to the parties in the necessary way. In *Woods v. Google*, the court dismissed a breach of contract claim that was premised on the incorporation of pages from Google AdSense's Help Center. 2011 WL 3501403, at *4. The court found that it was too "difficult to identify the terms of any actual and unambiguous contractual obligations" if the contract was construed as including not just discrete documents but also webpages in various formats and locations. As such, the court concluded that the Help Center pages were not "'known or easily available'" for purposes of incorporation. *Id.*

resulted from the alleged breach. (*Id.*) Instead, Plaintiffs allege that Facebook was "unjustly enriched" and that the breach resulted in "non-monetary privacy damages." (*Id.* ¶¶ 251, 252.)

But, under California law, unjust enrichment is a quasi-contract principle, not a form of contract damages. *See Jogani v. Super. Ct.*, 165 Cal. App. 4th 901, 911 (2008); *McKell v. Wash. Mut., Inc.*, 142 Cal. App. 4th 1457, 1490 (2006). Plaintiffs' invocation of unjust enrichment in their damages allegation is incoherent, as a claim based in quasi-contract is mutually exclusive to one for breach of contract. *See Lance Camper Mfg. Corp. v. Republic Indem. Co.*, 44 Cal. App. 4th 194, 203 (1996) ("[A]n action based on an implied-in-fact or quasi-contract cannot lie where there exists between the parties a valid express contract covering the same subject matter."). And non-monetary damages, such as for mental suffering or emotional distress, are generally prohibited in breach of contract cases. *E.g.*, *Erlich v. Menezes*, 21 Cal. 4th 543, 558 (1999).

In a separate section of the SAC, Plaintiffs allege that their referer URLs have great value. (SAC ¶¶ 129-143.) But, as detailed in § IV(A)(1), Plaintiffs fail to allege *any* damages to that information, let alone "clearly ascertainable" damages.

3. Plaintiffs Fail to Allege that They Performed Under the Contract

Plaintiffs' SAC does not make a single allegation of performance or excuse (and does not even identify Plaintiffs' many obligations under the SRR). This complete failure is fatal to Plaintiff's breach of contract claim. *Bennett-wofford v. Bayview Loan Servicing, LLC*, 2015 WL 8527333, at *6 (N.D. Cal. Dec. 11, 2015). Even where the court suspects a plaintiff performed, express allegations of performance are required to overcome a motion to dismiss. *Id.* (dismissing, in part, because "it is improper for a court to assume the [plaintiff] can prove facts that [it] has not alleged" and plaintiff failed to allege performance) (internal quotations and citation omitted). The SRR requires, among other things, that users must not post unauthorized commercial communications, access an account belonging to someone else, provide false personal information, create multiple accounts, or create more than one profile. (*See* Exs. A-D at 2-3.) Plaintiffs have not alleged they performed these, or any of the obligations in the SRR. The failure is not a mere technicality. For instance, if Plaintiffs did not provide accurate personal information when creating their accounts, the cookies at issue would not actually identify them.

K. Plaintiffs Fail to State a Claim for Breach of the Implied Covenant of Good Faith and Fair Dealing (Count VII)

To succeed in an action for breach of the implied covenant of good faith and fair dealing, Plaintiffs must show (1) a valid contract; (2) that Plaintiffs performed or were excused from performing under the contract; (3) that Facebook unfairly interfered with Plaintiffs' rights to receive the benefits of the contract; and (4) that Plaintiffs were harmed as a result. *Avila v. Countrywide Home Loans*, 2010 WL 5071714, at *5 (N.D. Cal. Dec. 7, 2010). Additionally, Plaintiffs must plead more than a breach of the contract terms themselves. *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1394-95 (1990); *Partti v. Palo Alto Med. Found. for Health Care, Research & Educ., Inc.*, 2015 WL 6664477, at *10 (N.D. Cal. Nov. 2, 2015) (dismissing "cause of action [that] relies on the same allegations as the breach of contract claims") (internal quotations and citation omitted). Plaintiffs simply duplicate the breach of contract claim, offer a conclusory allegation of damages, and fail to plead Plaintiffs' own performance.

Mere Recitation of a Breach of Contract Claim. Count VII of Plaintiffs' SAC alleges little more than a breach of contract under a different heading. Plaintiffs assert: "Despite its *contractual* privacy promises not to track users while they were logged-off of Facebook, in fact, Facebook took actions outside those *contractual* promises[.]" (SAC ¶¶ 257 (emphasis added).) This is identical to the breach of contract claim discussed above. The court in *Careau* proscribed this very style of pleading: "If the allegations do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action, they may be disregarded as superfluous as no additional claim is actually stated." 222 Cal. App. at 1395 (affirming the lower court's sustaining of a demurrer); *see also Croshal v. Aurora Bank, F.S.B.*, 2014 WL 2796529, at *6 (N.D. Cal. June 19, 2014) (dismissing for the same reason).

Moreover, as Count VII is essentially a restatement of Count VI, the same dispositive arguments raised above apply. The implied covenant of good faith and fair dealing cannot fix a defective breach of contract claim by creating new substantive obligations not found in the

contract. *See Rosenfeld v. JPMorgan Chase Bank N.A.*, 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010) ("[T]he implied covenant of good faith and fair dealing cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement.") (internal quotations and citation omitted). Plaintiffs cannot accomplish in Count VII, under the guise of the implied covenant, what they failed to accomplish in Count VI—the invention of a new contract term.

No Damages. A claim for breach of the implied covenant requires that the plaintiff suffered damages as a result. *Avila*, 2010 WL 5071714, at *5. Plaintiffs offer nothing more than a parroting of the generic pleading requirement (SAC ¶ 261) that fails for the same reasons that Plaintiffs' breach of contract allegations fail to allege damages.

No Performance. For the same reasons Plaintiffs' failure to plead performance is fatal to their breach of contract claim, that failure similarly dooms their implied covenant claim. *See Berkeley v. Wells Fargo Bank*, 2015 WL 6126815, at *4 (N.D. Cal. Oct. 19, 2015); *Rosenfeld*, 732 F. Supp. 2d at 969.

L. Plaintiffs Fail to State a Claim for Larceny (Count XI)

The SAC does not state a claim for larceny under California Penal Code §§ 484 or 496.

Penal Code § 484. Plaintiffs allege theft of their "personally identifiable information" by false pretenses under § 484. (SAC ¶¶ 289, 291, 292.) But a violation of § 484 does not give rise to a private right of action.[21] *Windham v. Davies*, 2015 WL 461628, at *6 (E.D. Cal. Feb. 3, 2015) ("Nor does the Court finds [sic] any authority that a violation of Penal Code section 484 provides a private right of action.") (citation omitted). Even if this were not the case, theft by false pretense requires a misrepresentation, fraudulent intent, and reliance. *Harris v. Garcia*, 734 F. Supp. 2d 973, 989 (N.D. Cal. 2010) (listing elements for the criminal prosecution of theft by false pretense). Plaintiffs have not adequately alleged any of these elements. (*See supra* § IV.E.1.)

[21] The legislature made express a private right of action for other sections of this chapter. *E.g.*, Cal. Penal Code § 496(c). Where the legislature uses terms in one section of a statute, but omits them in another, such an omission should be found purposeful. *See Briggs v. Eden Council for Hope & Opportunity*, 19 Cal. 4th 1106, 1117 (1999).

Penal Code § 496. To plead a violation of § 496, Plaintiffs must allege that Facebook either (1) bought or received property, knowing the property had been obtained by theft or extortion; or (2) concealed, sold, or withheld property from the owner, or aided in the same, knowing the property had been obtained by theft or extortion. Cal. Penal Code § 496(a). Plaintiffs must plead the elements of their § 496 claim under the stringent pleading requirements of Rule 9(b). *See Boulton v. Am. Transfer Servs., Inc.*, 2015 WL 2097807, at *3 (S.D. Cal. May 5, 2015) (finding that Rule 9(b) applied to the § 496 claim because it was "based on the same course of fraudulent conduct" as the other actions sounding in fraud). Plaintiffs' claims fail to satisfy Rule 8, let alone Rule 9(b)'s heightened pleading standard.

First, the information plaintiffs allege Facebook collected is not "property" under § 496. *Cf., e.g., In re Zynga Privacy Litig.*, 2011 WL 7479170, at *1 (N.D. Cal. June 15, 2011), *aff'd*, 750 F.3d 1098 (9th Cir. 2014) ("personally identifiable information does not constitute property for purposes of a UCL claim"); *Low*, 900 F. Supp. 2d at 1026 (same).

Second, Plaintiffs' § 496 claim requires the alleged property to have been stolen, and Facebook to have known as much. As noted, Facebook received the information directly from Plaintiffs. Facebook had no reason to believe the information was stolen, nor was it. Moreover, Plaintiffs allege not only that the information was stolen, but that it was a theft by false pretense, as defined by § 484. (SAC ¶¶ 289, 291.) As mentioned, that crime requires a false representation, fraudulent intent, and reliance. *Harris*, 734 F. Supp. 2d at 989. Again, Plaintiffs have not properly pled any of these elements. (*See supra* § IV.E.1.) Where a plaintiff fails to allege the specific facts necessary to plead fraud, a § 496 claim that is based on the same allegedly fraudulent conduct is also properly dismissed. *See Boulton*, 2015 WL 2097807 at *3.

Third, Facebook never bought Plaintiffs' property or received it from a third party. Instead, Plaintiffs' own browsers sent "GET" requests *to Facebook* as part of the Internet's normal operation. (*See supra* § II.A.) Likewise, Facebook never concealed or withheld property from Plaintiffs. Plaintiffs retained their own browsing history information at all times. None of the alleged conduct interfered with that access or concealed browsing information from Plaintiffs.

For each of these reasons independently, Plaintiffs fail to state a claim under § 496.

M. Plaintiffs' Claims Should Be Dismissed With Prejudice

Plaintiffs have not established that they have standing to pursue these claims and have not alleged facts sufficient to state any claim. Plaintiffs have had ample opportunity to cure the deficiencies this Court identified in its previous Order, but they have not. Thus, their claims should be dismissed with prejudice. *See Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1007 (9th Cir. 2009) ("[W]here the plaintiff has previously been granted leave to amend and has subsequently failed to add the requisite particularity to its claims, '[t]he district court's discretion to deny leave to amend is particularly broad.'" (citations omitted)).

V. CONCLUSION

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

Dated: January 14, 2016

COOLEY LLP

/s/ Matthew D. Brown
Matthew D. Brown

Attorneys for Defendant FACEBOOK, INC.

126465553