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 REPLY IN SUPPORT OF 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)

Statutes

I. INTRODUCTION

Plaintiffs' Opposition ("Opposition" or "Opp.") to Facebook's Motion to Dismiss fails to demonstrate why Plaintiffs' Second Amended Consolidated Class Action Complaint ("SAC") should not meet the same fate as their first consolidated complaint. The SAC does not include any allegations of particularized and concrete harm required to establish standing, and Plaintiffs' theory that standing is established when any violation of state law is asserted has been explicitly rejected by the Ninth Circuit.

The SAC also fails to allege facts sufficient to state any of its eleven claims. Many of the arguments in the Opposition directly contradict the actual facts pled in the SAC. As the SAC explains, when an individual visits a webpage with Facebook content, the individual sends to Facebook a ***separate and different*** GET request containing the "referer URL" of the webpage being loaded so that Facebook knows where to load its content. (SAC ¶¶ 37, 38, 60.) Facebook receives a referer URL when an individual requests to view a webpage that contains Facebook content, in the same manner as any other third-party provider of Internet content. (*Id.*) When a Facebook cookie is present, that cookie is also sent as part of the GET request, but it is simply a "small text file[]" that includes only the data Facebook itself included. (*Id.* ¶ 52.)

These same factual allegations have serious—indeed fatal—implications for many of Plaintiffs' claims. Because Plaintiffs sent referer URLs to Facebook whenever Plaintiffs visited a webpage that contained Facebook content, Facebook's receipt of this information cannot be (i) an "interception" under the Wiretap Act, (ii) improper "access" of information in "electronic storage" under the SCA, (iii) "without permission" under Penal Code § 502, (iv) "unlawful access," as required for trespass, or (v) "theft," as required for larceny. Nor does a user have a reasonable expectation of privacy in such information, as numerous courts have held. Moreover, Facebook is a party to the GET request, precluding liability under the Wiretap Act and California Invasion of Privacy Act ("CIPA"). Finally, as an idle "text file," a cookie is not a "device" under the Wiretap Act, a "contrivance" under CIPA, or a "contaminant" under Penal Code § 502.

But that's not all. Plaintiffs also fail to rebut Facebook's numerous challenges to the other necessary elements of their claims. And they ignore Ninth Circuit precedent holding that referer

URLs are not "contents" of any communications. A number of Plaintiffs' common law claims are based on Facebook's alleged statement that certain cookies would be deleted on logout, but the Opposition offers no justification for the SAC's failure to plead when the alleged statement was made, that any named Plaintiffs ever saw or relied on it, that Facebook intended the statement to induce reliance, or that it was part of any contract between Plaintiffs and Facebook.

For these reasons and those that follow, the SAC should be dismissed with prejudice.

II. ARGUMENT

A. Plaintiffs Lack Article III Standing As to All Claims

1. Plaintiffs Fail to Point to Any Allegations Establishing Injury in Fact

In its Order dismissing the FAC, this Court dismissed Plaintiffs' state law claims, holding that because the FAC did not "demonstrate[] that Facebook's conduct resulted in some concrete and particularized harm" Plaintiffs failed to "articulate[] a cognizable basis for standing pursuant to Article III[.]" (Order at 11.) The SAC fails to cure this fatal defect. As demonstrated in Facebook's Motion, Plaintiffs' SAC contains no new allegations of "a realistic economic harm or loss that is attributable to Facebook's alleged conduct." (*Id.* at 10.) Nor have Plaintiffs even attempted to respond to Facebook's cited authority. Given these failures, the Court should dismiss the SAC. (Mot. at 8 (collecting cases).)

Plaintiffs also have not pled they *themselves* were harmed by Facebook's alleged conduct. Specifically, they have not alleged a single example of a third-party webpage *they* visited or a communication of *theirs* that was supposedly "tracked." (Mot. at 9-10.) Instead, their Opposition argues that the SAC is sufficient because it includes allegations that the "intercepted URLs contain detailed file paths containing the content of GET and POST communications." (Opp. at 8 (internal quotation marks omitted).) But this conclusory assertion about the alleged contents of the URLs says nothing about any concrete or particular harm suffered *by Plaintiffs*. (Mot. at 9-10 (citing cases).) Likewise, Plaintiffs do not address their failure to allege an actual economic injury, as required by their California Penal Code § 502, civil fraud, and larceny claims. (Mot. at 10 (citing cases).) Without these allegations, Plaintiffs cannot establish Article III standing.

2. The Ninth Circuit Has Explicitly Rejected Plaintiffs' Theory that Pleading a State Law Claim Establishes Article III Standing

Recognizing the weaknesses in their standing argument, Plaintiffs incorrectly rely on *FMC Corp. v. Boesky*, 852 F.2d 981 (7th Cir. 1988), and *Cantrell v. City of Long Beach*, 241 F.3d 674 (9th Cir. 2001),[1] for the proposition that pleading a state law claim is sufficient to invoke Article III standing, regardless of any particularized injury, because "if a claim is cognizable under state common law it is Constitutionally cognizable in federal court." (Opp. at 7.) This argument is meritless. As an initial matter, the language from the cases that Plaintiffs rely on for this sweeping proposition is dicta. *FMC*, 852 F.2d at 990-91 (concluding facts alleged established Article III injury regardless of state law claims);[2] *Cantrell*, 241 F.3d at 683 (holding no standing to bring state taxpayer claim in federal court regardless of *FMC*). More importantly, the Ninth Circuit has squarely rejected Plaintiffs' theory. *Cantrell* itself stated: "[A]lthough the [plaintiffs] may well have standing under California law to bring their suit in state court, that does not help them here. ***A party seeking to commence suit in federal court must meet the stricter federal standing requirements of Article III***." 241 F.3d at 683 (emphasis added).

The Ninth Circuit reaffirmed this holding in *Lee v. American National Insurance Company*, 260 F.3d 997 (9th Cir. 2001), where the plaintiff brought a class action against two out-of-state insurance companies alleging a violation of California's Unfair Business Practices Act. *Id.* at 999. Although California law would have permitted the plaintiff to sue without having purchased the insurance policy being challenged, the Ninth Circuit agreed that state law

---

[1] Plaintiffs' reliance on *In re Google Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015) (Opp. at 6-7), is unavailing since there the court did not even address the argument that pleading a state law claim establishes Article III standing. Rather, the court reasoned that plaintiffs had standing simply because the "events that the complaint describes are concrete, particularized and actual as to the plaintiffs." *Id.* at 135. The opinion does not explain how such allegations amount to an ***injury*** under Article III when case law is replete with examples of plaintiffs who alleged "events" that were particular to them, but nonetheless had no standing because the allegations failed to demonstrate a concrete *injury*. (Mot. at 8 (collecting cases).)

[2] *FMC* is also inapposite. In that case, the defendant allegedly stole confidential business information, which has value only if it remains secret. *Id.* at 991. Plaintiffs' logged out browsing information is decidedly different from the information in *FMC*, the misappropriation of which the Seventh Circuit held "destroyed whatever value it had in FMC's hands." *Id.* at 991 n.21.

did not trump Article III's standing requirements: "***[A] plaintiff whose cause of action is perfectly viable in state court under state law may nonetheless be foreclosed from litigating the same cause of action in federal court, if he cannot demonstrate the requisite injury***." *Id.* at 1001-02 (emphasis added); *accord Fiedler v. Clark*, 714 F.2d 77, 79-80 (9th Cir. 1983) ("In determining jurisdiction, district courts of the United States must look to the sources of their power . . . not to the acts of state legislatures. However extensive their power to create and define substantive rights, the states have no power directly to enlarge or contract federal jurisdiction.").

Plaintiffs fare no better with their arguments that the *Erie* doctrine and the Class Action Fairness Act ("CAFA") support standing here. As to *Erie*, federal courts *must first have Article III jurisdiction* before considering the doctrine, as the Ninth Circuit has long recognized:

> The *Erie* doctrine does not extend to matters of jurisdiction . . . . ***It does not require relegation of the diversity jurisdiction to the mercies of the legislatures of fifty separate states***. Indeed, the *Erie* doctrine rests upon the premise that the jurisdiction of the federal diversity court is satisfied . . . .

Begay v. Kerr-McGee Corp., 682 F.2d 1311, 1316 (9th Cir. 1982) (emphasis added) (citation omitted).[3] As to CAFA, Plaintiffs argue that this Court should retain jurisdiction over state claims absent Article III injury because to do otherwise would be "contrary to CAFA's nonsubstantive purpose." (Opp. at 6.) Plaintiffs cite no case law in support. Nor could they, as several cases have held the exact opposite.[4] *E.g.*, *Wallace v. ConAgra Foods, Inc.*, 747 F.3d 1025, 1033 (8th Cir. 2014) ("CAFA does not purport to extend federal jurisdiction to state claims—if any exist—permitting recovery for bare statutory violations without any evidence the

[3] *Lee* and its progeny expressly apply to claims under state statutes in addition to common law claims. *E.g.*, *In re Capacitors Antitrust Litig.*, 2015 U.S. Dist. LEXIS 173404, at *28-29 (N.D. Cal. Dec. 30, 2015) ("It is of no moment that a state statute might purport to expressly give the plaintiff a right to sue; a plaintiff who clearly has standing under a state statute but not under the requirements of Article III cannot proceed with that claim in federal court."). Therefore, Plaintiffs do not have standing to maintain their California statutory claims based merely on alleged violations of the statutes separate from some Article III injury, including CIPA claims. This is not affected by *Edwards v. First American Corporation*, 610 F.3d 514 (9th Cir. 2010), which addressed a federal, not state, statute.

[4] In *Lee*, the Ninth Circuit recognized that dismissing state law claims for lack of standing would require two separate class actions to proceed in state and federal court and concluded that it was a necessary outcome of Article III's injury in fact requirement. 260 F.3d at 1006.

plaintiffs personally suffered a real, non-speculative injury in fact.").[5]

As Plaintiffs have not pled injury, the Court should dismiss the SAC for lack of standing.[6]

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

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

Addressing Plaintiffs' FAC, the Court held that the information allegedly 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 (citing *In re Zynga Privacy Litig.*, 750 F.3d 1098 (9th Cir. 2014).) *Zynga* specifically held that referer headers—the same information that Plaintiffs allege was intercepted here—do not qualify as "contents" of communications under the Wiretap Act. 750 F.3d at 1108. Nothing in the SAC or Opposition alters this conclusion.

The Opposition first contends that *Zynga* is distinguishable because the referer headers in *Zynga* allegedly included the name of a person or a group, rather than the title of an article such as "How Do I Reduce Herpes Breakouts." (Opp. at 11.) But this is a distinction without a difference. *Zynga*, in fact, contemplated that referer headers could disclose that a person viewed "the Facebook page of a gay support group." *Id.* at 1108. *Zynga* nevertheless held that referer headers are record information—not "contents" under the Wiretap Act. *Id.* As this Court has already recognized, it is bound by that ruling and should dismiss this claim.

---

[5] Plaintiffs ask the Court to reconsider its Order distinguishing this case from *In re Facebook Privacy Litigation*, 572 F. App'x 494 (2014), but provide no reason to do so. That decision is not precedential, did not even address the issue of standing, and certainly did not "extend[] *Cantrell*" as Plaintiffs argue. (Opp. at 7.) Moreover, as this Court explained in its Order, the unpublished decision is "inapplicable to this case" (Order at 11 n.3) because, unlike here, the plaintiffs alleged the "dissemination of their personal information" and "[loss of] sales value of that information." 572 F. App'x at 494. *In re Anthem Data Breach Litigation*, 2016 U.S. Dist. LEXIS 18135 (N.D. Cal. Feb. 14, 2016), is also inapplicable because there the court specifically held that "the ***loss*** of value of PII represents a cognizable form of ***economic*** injury." *Id.* at 170 (emphasis added). As this Court previously concluded, Plaintiffs did not allege a loss of value in any of their information. The SAC is also devoid of any such allegations.

[6] The Court should reject Plaintiffs' request to wait to resolve the standing issue until some unspecified "later stage" (Opp. at 9) because "[t]he Supreme Court has been very clear that Article III standing is a threshold inquiry that must be undertaken at the outset of a case before the Court proceeds any further." *In re Capacitors Antitrust Litig.*, 2015 U.S. Dist. LEXIS 173404 at *23 (rejecting request to delay standing question) (citing *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94-95 (1998)). Even the cases from this district that Plaintiffs cite ruled on standing on the pleadings. *In re Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1065-69 (N.D. Cal. 2015); *Anthem Data Breach Litig.*, 2016 U.S. Dist. LEXIS 18135 at *98-109.

Plaintiffs also cite two out-of-circuit cases, but neither is availing. *Google Cookie Placement* stated that the "post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user," but ultimately concluded that it did not need to decide whether all such information was "content" under the Wiretap Act. 806 F.3d at 139. Moreover, the defendants in that case *conceded* that some queried URLs may qualify as "content." *Id.* Similarly, *Declassified Opinion from the FISC* (ECF No. 78) held that dialing, routing, addressing, or signaling information can be content, observing that "if a user runs a search using an Internet search engine [and] the search phrase [] appear[s] in the URL," the URL includes the "contents" of communications. *Id.* at 31-32. Neither case, however, supports the conclusion that Plaintiffs advocate here—that *all* referer URLs are content. (Opp. at 11-12.) Rather, these two courts determined that certain referer URLs *could* be content if they included a search query. Plaintiffs here, however, do not allege a single URL that was collected, let alone that Facebook collected a URL containing a search query by Plaintiffs.[7] (*See* SAC ¶¶ 113-124.) And to the extent that either of these cases conflicts with *Zynga*, they are incorrectly decided and, in any event, irrelevant, as this Court must follow binding Ninth Circuit precedent.

2. Plaintiffs' Own Allegations Show That There Was No "Interception"

Plaintiffs ignore the clear case law establishing that there can be no "interception" where, as the SAC acknowledges is true here, Facebook receives *separate and different* communications *after* Plaintiffs' communications to first-party servers are complete. (Mot. at 12-13.) Plaintiffs' arguments in opposition are meritless. First, Plaintiffs dismiss *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), as factually distinguishable because the communications in *Konop* had been stored for "far longer than the milliseconds" at issue here. (Opp. at 13.) That argument has been squarely rejected, *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (citing *Konop*) (whether a defendant "received the [] messages in milliseconds or days . . . makes no difference"), because the key inquiry under *Konop* is whether the

[7] Plaintiffs' continued failure to provide the referer headers allegedly intercepted is no mere technicality. While the SAC speculates that some allegedly intercepted referer headers included search queries, Plaintiffs point to no search engines that utilize the Facebook social media plugin.

interception occurs before the communication reaches its destination. *Konop*, 302 F.3d at 878 (requiring interception during transmission "is consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course *before arrival*'" (emphasis added)). Because the SAC concedes that the allegedly "intercepted" communication has already arrived at the first-party website before that website instructs the user's browser to send a separate communication to Facebook (SAC ¶¶ 37, 61), there can be no interception as a matter of law.[8]

Second, courts have squarely rejected Plaintiffs' suggestion that an interception is shown so long as some derivative of the communication is obtained. *E.g.*, *Bunnell*, 567 F. Supp. 2d at 1154 (holding that even a scheme to immediately forward exact copies of communications did not "intercept" them while in transit). Plaintiffs offer no explanation (or case law) to support their illogical argument that two different messages, sent at different times to different parties, but containing some of the same information, can amount to an "interception" under the statute.

Finally, Plaintiffs deny that acceptance of their theory could impose liability on all third-party providers of webpage content because other third-party providers can rely on users' implied consent. (Opp. at 22.) Plaintiffs cite *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) in support, but that case held that Doubleclick had consent from *first-party websites* that integrated code instructing Internet users' browsers to contact Doubleclick; it did not consider whether Doubleclick had obtained the consent of Internet *users*. *Id.* at 510-11.[9] Plaintiffs' interpretation would lead to an absurd result that is wholly unsupported by the statutory text or case law.

3. Plaintiffs Fail to Identify Any "Device"

The Opposition fails to explain how any one of the seven possible "devices" listed in the

[8] *United States v. Szymuszkiewicz* held that a communication was "intercepted" where it was obtained before it had reached its destination, and thus is consistent with the standard articulated here. 622 F.3d 701, 704 (7th Cir. 2010) (noting that the evidence at trial showed "[t]he copying *at the server* was the unlawful interception, catching the message 'in flight' (to use Szymuszkiewicz' preferred analogy)"). To the extent that dicta in *Szymuszkiewicz* provides an alternate definition of "interception," it is at odds with the Ninth Circuit and therefore irrelevant.

[9] Indeed, applying the theory of consent articulated in *In re Doubleclick*, Facebook would be exempt from liability under the Wiretap Act because first-party web sites impliedly consented to the alleged interception. (*See infra* § II.B.4.)

SAC "can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5). Instead, Plaintiffs argue that under certain circumstances, computers, computer code, cookies, and "a plan" *can* function as devices.[10] But Plaintiffs have not alleged how Facebook intercepted "through the use of" any alleged "devices," thus they have not met this element of the claim. For example, Plaintiffs claim that their computers are "devices" under the Act, but fail to explain how Facebook "use[d]" their computers to intercept communications. 18 U.S.C. § 2510(4); *see Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (dismissing Wiretap Act claim where defendant "did not acquire [the communication] using a device other than the drive or server on which the e-mail was received").[11]

4. Facebook Was a Party to the Alleged Communication and Had Consent to Receive the URL Referers

The SAC concedes that Facebook only acquired communications that Plaintiffs sent directly to Facebook. (SAC ¶ 61.) Because Facebook was a party to those transmissions, they cannot form the basis of a Wiretap Act violation. (Mot. at 14 (collecting cases).) Facebook's "admission" that it is a third-party provider of content does not alter this conclusion. (Opp. at 15.) First, Facebook's Motion "admits" nothing; it simply referred to one of Plaintiffs' *allegations*: that websites that incorporate third-party content (such as the Facebook Like button) require the users' browsers to communicate directly with "third-party" providers to display the site accurately. (Mot. at 17 (citing SAC ¶¶ 36-39).) Assuming that allegation is true, Facebook, when acting as a third-party provider of webpage content, communicates ***directly*** with the user and is therefore a party to those communications. *See Crowley*, 166 F. Supp. 2d at 1269 (dismissing Wiretap Act claim where alleged interceptor "merely received the information

[10] Facebook disputes that computer code, cookies, or "a plan" constitute "devices." Notwithstanding Plaintiffs' Random House reference (Opp. at 14), applying the canon of construction *ejusdem generis*, "other devices," in the phrase "electrical, mechanical, or any other device," must be physical devices and cannot be computer software, cookies, or a "plan." *Yates v. United States*, 135 S. Ct. 1074, 1086-87 (2015) (*ejusdem generis* applies to limit "tangible object" in context of "any record, document, or tangible object" to things used to record or preserve information, and does not include fish).

[11] Plaintiffs attempt to distinguish *Crowley* because there Amazon was a second party to the communication (Opp. at 15), but that is irrelevant to *Crowley*'s holding on what constitutes a "device." Similarly, Plaintiffs cite to *In re Carrier IQ*, but there the court did not consider the argument made here – that software is not a "device." 78 F. Supp. 3d at 1084.

transferred to it by [Plaintiffs], an act without which there would be no transfer").

Plaintiffs argue that *Crowley* is distinguishable because Plaintiffs here had "no intention of sending any information to Facebook" and "Facebook [had] explicitly promised it would not acquire user communications." (Opp. at 15.)[12] But Plaintiffs cannot reconcile this argument with their allegations that, as part of the normal operation of the Internet, when a person seeks to visit a webpage with third-party content, her browser must communicate with those third-party content providers. (SAC ¶¶ 37-40.) Plaintiffs also ignore precedent that their subjective belief about Facebook's status as a party to the communication is irrelevant. (Mot. at 14 (collecting cases).) Even *Google Cookie Placement*, upon which Plaintiffs heavily rely, ultimately dismissed the Wiretap Act claims because, like Facebook here, Google was a party to those communications. 806 F.3d at 143-45.[13]

As to consent, Plaintiffs fundamentally misconstrue Facebook's argument. The *first-party websites* consented to Facebook's receipt of URL referrers by voluntarily integrating the Facebook code to place Facebook content on their webpages. *See e.g., Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) (consent "is implicit in the web pages' code instructing the user's computer to contact Avenue A"). Plaintiffs' attempt to manufacture a factual dispute here is unavailing; there is no dispute that first-party websites voluntarily installed Facebook's social plugin. (*See* SAC ¶¶ 2, 60.) Courts have not hesitated to dismiss Wiretap Act claims where, as here, consent was evident on the face of the complaint. *E.g.*, *Chance*, 165 F. Supp. 2d at 1162; *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1029-30 (N.D. Cal. 2014).

5. Facebook Is Exempt from the Wiretap Act as an Electronic Communication Service Provider in the Ordinary Course of Business

Plaintiffs assert that Facebook is an ECS provider "only for communications made on Facebook.com" (Opp. at 17), but Facebook plugins enable users to send electronic

[12] As discussed below, Facebook did not promise that it would not acquire referer URLs, and Plaintiffs' SAC contains no such allegation. And the SAC admits that third-party providers of Internet content receive such information so they can render such content. (SAC ¶¶ 36-40.)

[13] Neither of the cases Plaintiffs cite—*In re Pharmatrak*, 329 F.3d 9 (1st Cir. 2003) and *Szymuszkiewicz* (Opp. at 16)—even considered whether the party exemption applied to the recipient of the communication.

communications when, for example, a user "clicks on the Like or Share button" on a "webpage with Facebook functionality." (SAC ¶ 3.) Thus, Facebook "provides to users . . . the ability to send . . . electronic communications." 18 U.S.C. § 2510(15); Mot. at 15-16. And it does so in the ordinary course of its business. Plaintiffs' own allegations demonstrate that users necessarily send referer URLs to third-party providers of website content to enable display of such content. (SAC ¶¶ 36-41.)

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

CIPA § 631. Plaintiffs' Opposition merely recycles their argument on their deficient Wiretap Act claim—asserting without factual or legal support that referer URLs are "contents" of communications (Opp. at 22 n.9), ignoring binding Ninth Circuit authority to the contrary. (*See* § § II.B.1; Mot. at 16.) But the Court previously rejected this argument and dismissed Plaintiffs' CIPA claim for failure to adequately plead that Facebook obtained the "contents of communications." (Order at 18.) It should do so again on this ground alone.

The Opposition also fails to demonstrate that the SAC remedied the deficiencies this Court identified when it dismissed the FAC for not adequately alleging the use of a "machine, instrument, or contrivance." (*Id.*) Plaintiffs cannot meet this element by simply providing a laundry list of things that may fulfill this requirement; they must "include facts in their pleading to show why it is so." (Mot. at 16-17; Order at 18.) Unable to point to any such factual allegations, the Opposition argues, without any legal support, that because the statute proscribes certain conduct "by means of any machine, instrument, or contrivance, *or in any other manner*" they need not explain how the objects listed in their SAC acted to satisfy this requirement. (Opp. at 22-23.) But their argument does not relieve them of their pleading burden.

The Opposition also fails to rebut that Facebook was a party and had consent.[14] Plaintiffs rely on their arguments under the Wiretap Act (Opp. at 22 n.9), which fail for the reasons articulated in § II.B.4 above. Moreover, courts have rejected Plaintiffs' argument that Facebook, as a party to the communication, required *Plaintiffs'* consent to avoid liability under § 631. (Mot.

[14] Plaintiffs' Opposition does not dispute that the Court's prior holding on this issue is inapplicable because the SAC made material changes to its allegations regarding what supposed "content" was obtained. (Mot. at 17.)

at 17 (collecting cases).)

CIPA § 632. Plaintiffs attempt to manufacture the "confidential communication" missing from their SAC by claiming that Facebook "promised" their communications would be confidential. (Opp. at 23.) But this argument has no basis in the SAC and Plaintiffs provide no authority to support it. First, Facebook's alleged promise to "remove the cookies that identify [a user's] particular account" is not a "promise[] not to record the communications at issue" as Plaintiffs claim. (*Id.*) The referer URLs at issue would have been sent, *regardless of whether these cookies were present.* Second, even if Facebook had promised not to receive referer URLs, such a promise would not create a reasonable expectation of privacy in such communications. *See, e.g., People v. Maury*, 30 Cal. 4th 342, 385 (2003) (promise of anonymity did not create reasonable expectation of privacy where circumstances suggested that such expectation was unreasonable). Section 632 applies only "if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002). But this Court, like many others, has concluded that the alleged information that was communicated here is not private. (Order at 12 n.5 ("Internet users have no expectation of privacy in the. . . IP addresses of the websites they visit . . . ." (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008).) And such decisions are not limited to IP addresses. *Forrester*'s reasoning extends to all "information [that] is provided to and used by Internet service providers for the specific purpose of directing the routing of information." 512 F.3d at 510. As Plaintiffs' SAC acknowledges, that is precisely the purpose of the GET requests that Plaintiffs send. (SAC ¶ 31.) *See also In re Google, Inc. Gmail Litig.*, 2013 WL 5423918, at *22 (N.D. Cal. Sept. 26, 2013) (applying § 632 and finding no confidentiality in communications that can be "recorded [by] . . . the recipient, who may then easily transmit the communication to anyone else").

Plaintiffs also contend that that they have satisfied the "recording device" requirement. But Plaintiffs merely rely on the list of things they claim constitute a "machine, instrument, or contrivance" under § 631. Plaintiffs have not described how any of these things are capable of "recording" or "amplifying" communications. For example, Plaintiffs allege that "cookies [are]

designed to track and record . . . communications" (Opp. at 24), but they do not explain how an idle "text file" can record anything or qualifies as a "recording device" under § 632.[15]

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

1. Plaintiffs Fail to Allege Facebook Accessed Information While in "Electronic Storage"

Plaintiffs fail to rebut Facebook's showing that neither "the toolbar" nor "browsing history" satisfy the definition of "electronic storage" under §§ 2510(17)(A) and (B). First, the toolbar does not store referer URLs "in the middle of a transmission" and therefore is not "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" under § 2510(17)(A). (Mot. at 19-20.) Plaintiffs' Opposition distorts the allegations in the SAC to suggest that storage in the toolbar is part of the transmission process. (Opp. at 21.) But the SAC alleges only that "a copy of the Plaintiffs' URL requests" appears in the toolbar while "the communication is in the process of being sent and received between the user and the first-party webpage." (SAC ¶ 206.) Because Plaintiffs do not (and cannot) allege that "a copy of the Plaintiffs' URL request" in the toolbar is the actual communication or that this copy is delivered anywhere, Plaintiffs have not alleged that the toolbar stores a communication "in the middle of a transmission" as required 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).

Second, § 2510(17)(B) only encompasses storage "by an electronic communication service for purposes of backup protection," and thus cannot include storage of "browsing history" on Plaintiffs' personal computers. (Mot. at 19-20 (collecting cases).) Plaintiffs fail to address any of Facebook's cited authorities (*Id*. at 19-21), instead claiming only that "the definitions of storage are 'extraordinary – indeed, almost breathtakingly – broad'" (Opp. at 20-21 (citing *United States v. Councilman*, 418 F.3d 67, 73 (1st Cir. 2005)), and that backup protection includes storage "for the user's benefit" (Opp. at 21 (citing *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075

[15] *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010), is not to the contrary. There, the court *assumed* that all requirements of § 632, including the use of a recording device, had been met, before determining there was no "confidential communication." *Id.*

(9th Cir. 2004)). But *Councilman* and *Theofel* involved electronic storage on an email server and thus are not an answer to the authority offered by Facebook demonstrating that storage on a personal computer does not qualify as "electronic storage" for backup protection under the Act.[16]

Lastly, even if storage in the toolbar or in browsing history could constitute "electronic storage," Plaintiffs have not alleged that Facebook accessed information "while it is in" these locations, as required by the statute. Instead, Plaintiffs have alleged that Facebook receives referer URLs because they are sent to Facebook so that Facebook can deliver requested website content. (SAC ¶¶ 35-40, 61.) Plaintiffs' Opposition suggests that it does not matter whether Facebook "access[es] . . . [an] electronic communication while it is in electronic storage" (18 U.S.C. § 2701(a)(2)) so long as Facebook obtained or even just used the information somehow. (Opp. at 21-22.) This absurd argument ignores the plain language of the statute, and if accepted, would impose liability for obtaining or using any communication that had ever, at any point, been in temporary "electronic storage." Moreover, courts have not interpreted "access" under § 2701(a)(2) to be synonymous with "obtain" or "use," nor has plaintiff identified any authority to the contrary. *See In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *11-14 (dismissing SCA claim where plaintiffs alleged that cookies were in "electronic storage" while in random access memory ("RAM"), but failed to plead that the defendant procured the cookies from RAM).

2. Plaintiffs Fail to Establish that Facebook Accessed a "Facility"

Facebook established in its Motion that personal computers are not "facilities" under the SCA. (Mot. at 21 (collecting cases).) Plaintiffs' efforts to carve out web browsers and browser-managed files from these authorities (Opp. at 18) is unavailing, as web browsers and browser-managed files are installed *on their own personal computers*. *See Crowley*, 166 F. Supp. 2d at 1270-71 (plaintiff's personal computer is not a facility under the SCA); *In re Nickelodeon Consumer Privacy Litig.*, 2014 U.S. Dist. LEXIS 91286, at *61 (D.N.J. July 2, 2014) ("[T]he SCA is not concerned with access of an individual's personal computer."). Plaintiffs' inability to distinguish those cases cited in Facebook's Motion mandates dismissal.

[16] *Councilman* involved the Wiretap Act, not the SCA, and explicitly departs from Ninth Circuit precedent. 418 F.3d at 69; *id*. at 87 (Torruella, J., dissenting) (citing *Konop*).

Plaintiffs attempt to salvage their SCA claim by citing a number of irrelevant and inapposite authorities, several of which do not even discuss the meaning of "facility" under the SCA. (Opp. at 18-19.) Plaintiffs cite a series of Microsoft cases, but they all involve default judgments entered against parties who had not appeared, let alone contested whether browsers are "facilities." *See, e.g.*, *Microsoft v. Does, 1-8*, No. 14-cv-00811-LO-IDD (E.D. Va. July 20, 2015) (court accepts without question Microsoft's contention that browsers were "facilities" under the SCA).[17] Likewise, Plaintiffs' remaining citation is to a case in which a court did not hold that personal computers were "facilities" under the SCA, but rather considered the plaintiffs' interpretation for the sake of argument and then explained why "the subsequent implications of this rather strained interpretation of a 'facility through which an electronic communication service is provided' are fatal to [plaintiffs'] cause of action." *Chance*, 165 F. Supp. 2d at 1161.

Plaintiffs fare no better with their policy argument that excluding personal computers from the SCA's purview would enable the government to access an Internet user's web-browsing history without a warrant, and would enable a third party to disclose a user's web-browsing history without consent. The SCA already specifies what information can and cannot be lawfully disclosed to a governmental entity, *see* 18 U.S.C. § 2703, and Plaintiffs ignore the numerous cases addressing (and rejecting) similar attempts to depart from the plain interpretation of the statute. (Mot. at 21 (citing § 2701(c)).)

Finally, Plaintiffs are incorrect to argue that the SCA should apply to every alleged unwanted access to electronic communications (Opp. at 20). *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1022 (N.D. Cal. 2012) ("[T]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications" as "there are many problems of Internet privacy that the SCA does not address.") (citation omitted).[18]

[17]While Plaintiffs list other cases involving Microsoft and unnamed defendants, they fail to identify any decision in those cases holding that browsers or browser-managed files are facilities.

[18] Plaintiffs also claim that exempting access to web browsers from the SCA's purview would undermine *Riley v. California*. But even if the SCA question presented here were somehow coextensive with Fourth Amendment jurisprudence (which Facebook does not concede), *Riley* only stands for the limited proposition that law enforcement must obtain a warrant before searching a cell phone seized incident to arrest. *Riley* did not eliminate the principle that there is no reasonable expectation of privacy in information voluntarily disclosed to a third party. *See*

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

1. Plaintiffs Fail to Allege With the Specificity Required by Rule 9(b) Any False Statements Upon Which Plaintiffs Relied

Nowhere in either Plaintiffs' Complaint or Opposition does any Plaintiff allege that she both read and relied on a specific fraudulent statement. In fact, only one paragraph in the SAC even mentions reliance at all, stating in boilerplate fashion: "Plaintiffs relied on Facebook's false assertions in contracting with and using Facebook." (SAC ¶ 267.) Not only is this conclusory allegation of reliance itself insufficient, *see Mazur v. eBay Inc.*, 2008 WL 618988, at *13 (N.D. Cal. Mar. 4, 2008), but Facebook and the Court are also left to guess *which* allegedly false assertions Plaintiffs supposedly read and relied on.[19]

The Opposition, in an attempt to cure this defect, points to seven paragraphs Plaintiffs claim "specifically" identify the otherwise elusive false promises. (Opp. at 36 (citing SAC ¶¶ 4, 23, 24, 27, 74, 78).) But a review of each of these paragraphs reveals the fatal flaw of the SAC—Plaintiffs have utterly failed to point to a statement by Facebook that was false, that was read by any of the named Plaintiffs, and that was relied upon:

- Paragraph 4 of the SAC asserts: "When a subscriber logs out of Facebook, however, Facebook promises to delete those cookies that contain subscriber's identifying information, such as user ID." (SAC ¶ 4.) But Plaintiffs offer no specifics of when, where, or by whom this "promise" was made, and give no citation.
- Paragraph 27 claims that in November of 2011, *after the proposed class period*, Facebook told USA Today that it did not track users post-logout. (SAC ¶ 27.)
- Paragraphs 74 and 78 quote from *internal* Facebook communications, so Plaintiffs cannot have read and relied on any of these statements. (SAC ¶¶ 74, 78.)

United States v. Guerrero, 768 F.3d 351, 358–60 n.7 (5th Cir. 2014).

[19] Plaintiffs cite *In re Clorox Consumer Litig.*, 894 F. Supp. 2d 1224 (N.D. Cal. 2012), and *Anthony v. Yahoo!, Inc.*, 421 F. Supp. 2d 1257 (N.D. Cal. 2006), for the claim that they can allege reliance in general terms. (Opp. at 36.) But, in both cases, the plaintiffs alleged (1) specific false statements that they were exposed to and (2) which statements they relied on. *Clorox*, 894 F. Supp. 2d at 1234 (plaintiffs alleged seeing and relying on specific statements in commercials when purchasing the product); *Anthony*, 421 F. Supp. 2d at 1264 (plaintiffs pointed to specific "false profiles" and alleged exposure to and reliance on them). Here, Plaintiffs do neither.

The two remaining allegations also fail. Paragraph 23 alleges that a Facebook Help Center page said "when you log out of Facebook, we remove the cookies that identify your particular account." But critically, Plaintiffs do not explain *when* this Help Center page was live, nor do they clarify where it could be found. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1126 (9th Cir. 2009) ("Nor did [plaintiff] specify when he was exposed to [the allegedly fraudulent statements] or which ones he found material."). Equally important, the SAC is silent on whether any of the Plaintiffs ever visited the alleged Help Center page, when they did so, or if they relied on that alleged representation. *See 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.").

Finally, paragraph 24 alleges that 19 days before the end of the class period, Facebook added a "promise" to its Data Use Policy by stating: "[Data received] may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID." (SAC Ex. H, § I.) Whether this wording is a promise not to collect URLs post-logout (it is not) is irrelevant because no named Plaintiff alleges she actually read this language let alone relied on it. Nonetheless, Plaintiffs contend (with no factual support in the SAC) that but for statements like this, they would not have contracted with Facebook—a requirement of reliance. (Opp. at 36.) Plaintiffs cannot claim that they relied on the updated language of the Data Use Policy when deciding whether to use Facebook, given that all four Plaintiffs used Facebook for at least 16 months before the language was added and none allege that they even read and relied on the language added in the last 19 days of the class period. (SAC ¶¶ 12, 13, 14, 15.)

2. Plaintiffs Fail to Plead that Facebook Intended to Induce Reliance on the Alleged False Statements

Plaintiffs do not deny that fraud requires proof of falsity *and* intent to induce reliance, stating only that "Fraud's elements are not at issue. The facts are." (Opp. at 35.) Precisely. The question is whether the facts alleged in the SAC adequately plead the element of fraudulent intent. *See Levin v. Citibank, N.A.*, 2009 WL 3008378, at *5 (N.D. Cal. Sept. 17, 2009) (finding

conclusory allegations of intent to induce insufficient to plead fraud); *Senah, Inc. v. Xi'an Forstar S & T Co.*, 2014 WL 3044367, at *4 (N.D. Cal. July 3, 2014) (dismissing fraud claim due to "bare allegations" of intent). The SAC's failure to allege any intent to defraud on the part of Facebook, in conclusory fashion or otherwise, is fatal to Plaintiffs' claim.

The Opposition's citation to various quotes from Facebook employees does not demonstrate intent. As an initial matter, a quote showing that some engineers at Facebook discussed post-logout cookie functions would not alone suffice to allege intent to induce reliance. *See Engalla v. Permanente Med. Grp., Inc.*, 15 Cal. 4th 951, 976 (1997) ("A fraudulent state of mind includes not only knowledge of falsity of the misrepresentation but also an intent to . . . induce reliance on it.") (citation omitted); *DeLeon v. Wells Fargo Bank, N.A.*, 2011 WL 311376, at *8 (N.D. Cal. Jan. 28, 2011) ("[K]nowing, intentional fraud" requires more than mistakes stemming from "one department not talking to another"). Instead, Plaintiffs must set forth factual allegations demonstrating that Facebook made false statements, and did so with the specific intent, at the time, to trick Plaintiffs into using Facebook. The referenced statements do nothing of the sort.

For instance, the Opposition offers part of a sentence from SAC ¶ 74, from an internal email thread, that has been taken far out of context. (Opp. at 35 (citing SAC ¶ 74).) The quote in context does not show intent to trick Plaintiffs, but instead it demonstrates intent to ensure that Facebook's public statements were true. (SAC ¶ 74.) Plaintiffs point to no fact that suggests any person at Facebook made a statement to *users*, while that person knew the statement was false, let alone made it with intent to induce reliance. Plaintiffs' failure to plead intent requires dismissal.[20]

3. Plaintiffs Fail to Plead Constructive Fraud

The Opposition also does not cure the SAC's failure to plead a "confidential relationship," as required to make out a claim for constructive fraud. (Opp. at 38.) Rather than point to supporting allegations in the SAC, Plaintiffs grossly misquote two cases. Plaintiffs quote *Portney v. CIBA Vision Corp.*, 2008 WL 5505517, at *5 (C.D. Cal. July 17, 2008), for the proposition that

[20] Plaintiffs improperly argue for the first time that Facebook had a duty to disclose (Opp. at 37). *See Monreal v. GMAC Mortg., LLC*, 948 F. Supp. 2d 1069, 1078 (S.D. Cal. 2013).

a confidential relationship existed because Facebook's "sophistication and bargaining power," and Plaintiffs' "substantial" reliance on Facebook's claims, "give rise to equitable concerns." (Opp. at 38.) But this comes from *Portney*'s discussion of *fiduciary* relationships—a type of relationship not alleged in the SAC. 2008 WL 5505517, at *5. When discussing confidential relationships, the court made clear: "As a general rule, the [confidential] relationship is not created simply by the receipt of confidential information." *Id*. (citation omitted). Likewise, the Opposition cites *Patriot Scientific Corp. v. Korodi*, 504 F. Supp. 2d 952, 966 (S.D. Cal. 2007), for the proposition that the existence of a confidential relationship is "generally a fact question," but omits the rest of the sentence, which clarifies that "where the allegations of fact, if true, would be legally insufficient to establish a confidential relationship, dismissal is appropriate." *Id*. at 966.[21]

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

No Damages. The SAC and Opposition (*see* Opp. at 33-34) ignore this Court's earlier ruling that Plaintiffs failed to allege damages sufficient to plead a § 502 claim (Order at 13). Plaintiffs offer no reason for the Court to reach a different conclusion now. Indeed, they do not address any of Facebook's case law, but instead offer a single misleading excerpt from *In re Google Android Consumer Privacy Litig*., 2013 WL 1283236, at *11 (N.D. Cal. Mar. 26, 2013). There, however, plaintiffs alleged that the value of their user data was diminished when it was improperly collected. Even then, the court found the allegations were "not sufficient to allege damage" for purposes of § 502. *Id*. Plaintiffs have also made much of the Third Circuit's decision in *Google Cookie Placement*, but that court also affirmed dismissal of the § 502 claims for failure to allege cognizable damages. 806 F.3d at 152. Finally, Plaintiffs seem to suggest, for the first time, that the volume of data transmitted to Facebook somehow caused damage to Plaintiffs, but never explain how that purported fact satisfies the damages element here, or point

[21] Plaintiffs' failure to plead any damages caused by the alleged fraud is also an independent basis to dismiss this claim. (Mot. at 24.) Plaintiffs' claim that the *In re Facebook Privacy Litigation* memorandum opinion (Opp. at 37) is preclusive on this issue is incorrect because the distinguishable facts alleged there (*see supra* at 5 n.5) means the cases are not "identical," preventing any issue preclusion. *Hydranautics v. FilmTec Corp.*, 204 F.3d 880, 885 (9th Cir. 2000) (prior case must have considered the *identical* issue to be preclusive).

to where in the SAC such an allegation is made. (Opp. at 33.)[22]

Not Without Permission. The Opposition concedes that to state a § 502 claim the SAC must allege facts establishing that Facebook circumvented a technical barrier. (Opp. at 34.) Plaintiffs argue that Facebook supposedly circumvented the "cookie blocking technology" used by the Internet Explorer ("IE") subclass, but do not explain how. (Opp. at 34:9-12.) Nor could they. IE gives users the *option* to reject cookies, so if Facebook wrote cookies onto Plaintiffs' IE browsers, then Plaintiffs' privacy settings *allowed* for cookies. (SAC Ex. Z at 2.)

Plaintiffs do not even attempt to explain how their Privacy Policy Project Platform ("P3P") allegations support the claim that Facebook circumvented a technical barrier. As Plaintiffs' own exhibit makes clear, IE does *not* require that websites use more tokens than were sent by Facebook, and IE erects no technical barrier to two-token sets like Facebook's. (*Id.* at 6 ("[IE cookie filters] do not check to make sure the minimum required tokens are present.").) Neither Facebook, nor the over 6,000 other websites that were found to have missing tokens, "tricked" IE, as Microsoft was well aware of the common practice of using less than five tokens, and never took any technical steps to prevent it. (*Id.* at 4, 6.)[23]

No Contaminant. Plaintiffs argue that cookies are contaminants under the statute because they are "viruses or worms." (Opp. at 34.) But Plaintiffs offer no factual support for this claim, or for their conclusory assertions that cookies "self-replicate" and "contaminate" URLs. In fact, the SAC contradicts these characterizations. Cookies do not self-replicate; they are set when a user visits a website and send information only when the browser directs them. (SAC ¶¶ 56, 57, 60.) Likewise, the SAC never alleges that cookies contaminate URLs or alter them in any way.

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

Plaintiffs' Opposition advances two unpersuasive arguments to support their trespass claim. First, Plaintiffs attempt to distinguish *Intel Corp. v. Hamidi* in which the California

[22] Plaintiffs also assert that the alleged intrusion into their privacy is enough to establish damages under § 502. But Plaintiffs cite no support for this proposition.

[23] Plaintiffs cite *Google Cookie Placement* for their claim that Facebook acted without permission. But that case did not rule on § 502 permission, made no mention of P3P, and concerned fundamentally different allegations: namely that Google "used code to command users' web browsers to automatically submit a hidden form to Google." 806 F.3d at 132.

Supreme Court held that trespass to chattels "does not encompass . . . an electronic communication that neither damages the recipient computer system nor impairs its functioning." 30 Cal. 4th 1342, 1347 (2003). The SAC fails to plead around this standard. Plaintiffs' Opposition argues that Facebook's cookies interfered with the operation of their computers by circumventing privacy protections. (Opp. at 39.) But almost identical arguments were rejected in *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *7 (C.D. Cal. Apr. 28, 2011) (dismissing § 502 claim based on installation of cookies and interception of private information because plaintiffs had not alleged any interference with the *functioning of their computers* except in a "trivial sense"). Plaintiffs make no attempt to distinguish *LaCourt*, despite its clear applicability. (Opp. at 39.) Nor can they.

Second, the Opposition argues that the issue should not be decided on a motion to dismiss. (Opp. at 39.) But unlike the case Plaintiffs cite, *Coupons, Inc. v. Stottlemire*, 2008 WL 3245006 (N.D. Cal. July 2, 2008), here there is no factual dispute. The question is whether, as a matter of law, the alleged damages comport with the holding in *Hamidi*. Here, they do not. When such is the case, the claim should be dismissed. *LaCourt*, 2011 WL 1661532, at *7-8; *In re iPhone App. Litig.*, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) (dismissing trespass claim for failing to allege identifiable injury).

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

The Opposition fails to address this Court's prior order, binding Ninth Circuit law, or any of the cases cited in Facebook's Motion establishing that the elements of invasion of privacy cannot be met. Plaintiffs also ignore their continued failure to allege that any of their specific, private information was actually sent to Facebook. (Mot. at 29-30.) Plaintiffs instead rely principally on two cases (Opp. at 25), but both cases are distinguishable and erroneously decided.

Google Cookie Placement does not support Plaintiffs' arguments here. There, the court distinguished Google's conduct from mere "tracking and disclosure" and held that the plaintiffs' allegations were sufficient to state a claim largely because Google overrode "the plaintiffs' cookie blockers" while assuring users that they would be effective. 806 F.3d at 150. In contrast, Plaintiffs allegations do not show that Facebook subverted their attempts to block cookies (*see*

supra § II.F), nor that Facebook collected information about them despite an "express, clearly communicated denial of consent." *Id.* at 151. Thus, even under *Google Cookie Placement*'s standard, Plaintiffs fail to sufficiently allege a reasonable expectation of privacy and an egregious breach of social norms. *Id.* at 151. More importantly, *Google Cookie Placement* was wrongly decided. First, in concluding that plaintiffs had established a legally protected privacy interest, the court erroneously relied on dicta in a case involving a different privacy tort, which does not require the showing of such a legally protected interest. *Id.* at 151. Second, the court ignored the California Supreme Court's directive in *Hill* that individual circumstances limit the reasonable expectation of privacy. *Compare id.* at 150 ("It is no matter whether or not a given plaintiff had actual, subjective knowledge of her browser settings and the impact of those settings on the defendants' tracking practices") *with Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 36-37 (1994) (observing that "a privacy interest is not independent of the circumstances" and reasoning that "notice," "consent," and "awareness" affect the expectations of the individual).[24] Finally, the court failed to address case law holding that collection of consumer data is not an egregious breach of social norms.[25] (*See* Mot. at 30.)

Plaintiffs also cite the Superior Court's demurrer ruling in *Ung v. Facebook, Inc.*, No. 12-CV-217244 (Cal. Super. Ct. Santa Clara Cnty. July 2, 2012).[26] But in its decision, the *Ung* court relied on *United States v. Maynard*, 615 F.3d 544, 551 (D.C. Cir 2010), which concerned tracking a person's physical location, and was affirmed (*sub nom U.S. v. Jones*) on a theory of physical trespass. *Jones*, 132 S. Ct. 945, 955 (2012). *Maynard* thus has little application to whether browsing history is a legally protected privacy interest. Also, the *Ung* court failed to acknowledge case law finding a lack of a reasonable expectation of privacy in the type of information at issue here. Moreover, the *Ung* court did not consider case law binding on *this*

[24] Under the correct standard, Plaintiffs' claims fail, as described in the Motion. (Mot. at 31-32.)

[25] Moreover, to the extent that *Google Cookie Placement* conflicts with *Forrester*'s holding that "Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit," it must be disregarded. *Forrester*, 512 F.3d at 510.

[26] Plaintiffs halfheartedly argue that *Ung* "may" be preclusive here (Opp. at 24 n.12), but *Ung* did not consider Ninth Circuit case law, as well as other relevant case law and arguments, and, as a denial of a demurrer, was not a final decision on the merits. *See Arduini v. Hart*, 774 F.3d 622, 632 (9th Cir. 2014) ("[T]he denial of the motion to dismiss was not a final order.").

court, including cases raised in Facebook's Motion (Mot. at 31-33) and this Court's prior Order. (Order at 12 n.5 (citing, among others, *Forrester*).)

Finally, Plaintiffs selectively rely on Fourth Amendment jurisprudence, but fail to mention *Forrester* and other case law holding that there is no reasonable expectation of privacy in the type of information at issue here. Neither *Riley v. California*, 134 S. Ct. 2473 (2014), nor *United States v. Jones*, 132 S. Ct. 945 (2012), is to the contrary. *Riley* concluded that the search-incident-to-arrest exception was inapplicable to a cell phone. It did not overturn Supreme Court precedent finding no reasonable expectation of privacy in information voluntarily shared with a third party. *United States v. Guerrero*, 768 F.3d 351, 358–60 n.7 (5th Cir. 2014). Similarly, *Jones* merely held that placing a tracking device on a vehicle is a seizure, requiring a warrant. 132 S. Ct. at 955. Plaintiffs also cite *In re Application for Telephone Information*, 2015 WL 4594558, at *8 (N.D. Cal. July 29, 2015), but that case shows exactly why Plaintiffs cannot plead a reasonable expectation of privacy here.[27] There, the court considered whether a warrant was required to obtain cell phone location information. The court reaffirmed that information "voluntarily conveyed" to third parties is not protected by the Fourth Amendment, but reasoned that this principle is inapplicable with respect to cell phone location information not "voluntarily conveyed," such as information generated by continuously operating apps or automatic pinging. Plaintiffs here voluntarily conveyed referer URLs. *See Forrester*, 512 F.3d at 510 (holding that the Fourth Amendment does not protect information like IP addresses and to/from addresses that are voluntarily disclosed to direct the routing of information on the Internet).

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

As with their invasion of privacy claim, Plaintiffs cannot overcome this Court's prior Order dismissing this claim for lack of a reasonable expectation of privacy. (Order at 12 n.5.) Instead of rebutting Facebook's authority regarding actionable intrusions and reasonable expectations of privacy (Mot. at 29-30; *supra* § II.H), Plaintiffs' Opposition merely repeats the insufficient allegations in the SAC. Plaintiffs also fail to address controlling case law holding

[27] *In re Application for Telephone Information* is also distinguishable as it concerns location information, which implicates well-established privacy concerns different from those implicated here, including invasion of the right to privacy in one's home. 2015 WL 4594558, at *11.

that conduct of the sort alleged here is not "highly offensive." *E.g., Low*, 900 F. Supp. 2d at 1025 (no highly offensive invasion of privacy where defendant allegedly disclosed user browsing history coupled with digital identification information to third parties in violation of its policies). Plaintiffs' citation to *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014), fails because the court there sustained an intrusion claim based on allegations of unauthorized access to personal contact list information on a cell phone. *Id.* at 1061. *Opperman* does not suggest that collection of voluntarily disclosed information, as alleged here, could be highly offensive.

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

No Reliance on a Contractual Provision. The Opposition, like the SAC, fails to point to a specific contractual provision that Plaintiffs allege has been violated. As this Court has stated: "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." *Woods v. Google Inc.*, 2011 WL 3501403, at *3 (N.D. Cal. Aug. 10, 2011) (emphasis added).

The SAC quotes only one so-called "promise" in connection with its breach of contract claim: "When you log out of Facebook, we remove the cookies that identify your particular account." (SAC ¶ 245.) Such language, Plaintiffs note, was included in Facebook's "social plug-in discussion" in "one Help Page entry." (*Id*. ¶ 23.) The SAC, however, never alleges the URL address where this entry can be found, how one would navigate to it from the SRR, or whether Plaintiffs read this alleged representation before agreeing to the SRR.

Plaintiffs seek to overcome these defects by asserting that the Help Center is incorporated into the Privacy Policy which is, in turn, incorporated into the SRR. (Opp. at 31.) But this is at odds with the facts and the law. Only three specific Help Center pages are linked to the Privacy Policy, and none contain the statement Plaintiffs claim was breached, nor concern cookies or social plugins. (Mot. at 35 fn. 19; SAC Exs. E, F, G at 6.) Rather, Plaintiffs ask the Court to incorporate the *entire* Help Center into the SRR without demonstrating how the page containing the alleged "promise" is even linked to the SRR (if at all). Just because the Help Center appears on Facebook's website does not make it part of a contract (the SRR) that also happens to appear on the same website. This Court has, in fact, rejected such an attenuated theory of incorporation.

Woods, 2011 WL 3501403, at *4 (rejecting incorporation of webpages into contract as being too "difficult to identify the terms of any actual and unambiguous contractual obligations").[28]

No Performance. Plaintiffs claim that they were not required to plead performance of the contractual obligations identified in Facebook's Motion based on a distinction between positive and negative contractual obligations, but provide no supporting authority. (Opp. at 32-33.) Regardless, the SRR includes "positive" obligations as well, e.g., the obligation to use a real name. (SAC Exs. A-D at 2.) Unable to identify any allegations of performance in the SAC, Plaintiffs argue that allegations that they "accepted the terms of the contract with Facebook" and "had active Facebook accounts during the entire class period" are sufficient. (Opp. at 32.) But simply agreeing to a contract cannot satisfy the performance element of a breach of contract claim, lest the performance element be entirely eviscerated.[29]

K. Plaintiffs Fail to State a Claim for Breach of Implied Covenant (Count VII)

Plaintiffs concede that their claim for breach of the implied covenant is duplicative of their breach of contract claim (Opp. at 33), but argue that the Court should still consider the implied-covenant claim if "the promises made in the Help Pages or Privacy Policy are deemed not to be contractually binding on Facebook." (*Id*.) Plaintiffs provide no authority for using the implied covenant as a mechanism to create obligations that are not present in a contract. Indeed, case law holds precisely the opposite: "the 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." *Rosenfeld v. JPMorgan Chase Bank N.A.*, 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010) (citation omitted). Plaintiffs' claim should be dismissed.

---

[28] Plaintiffs' citation to *Chan v. Drexel Burnham Lambert, Inc.*, 178 Cal. App. 3d 632 (1986), is unavailing. *Chan* did not endorse multiple layers of incorporation, and instead required "the incorporating document to refer to the incorporated document *with particularity*." *Id.* at 643-44 (emphasis added). The SRR does not refer to this alleged help page with particularity (nor does the SAC).

[29] Plaintiffs' failure to plead any damages caused by the alleged breach is also an independent basis to dismiss their breach of contract and implied-covenant claims. (Mot. at 35-36, 38.) Plaintiffs' reliance on the *In re Facebook Privacy Litigation* memorandum opinion (Opp. at 32) is unavailing because of the distinguishable facts alleged there. (*See supra* at 5 n.5.)

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

Plaintiffs' larceny claim fails for several reasons. First, cookies and referers are not "property" under the statute. Plaintiffs also argue that alleged "personally identifiable information" can be property for purposes of this claim (Opp. at 28-29), but ignore that several courts have held the opposite. *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) ("[P]ersonally identifiable information does not constitute property for purposes of a UCL claim"); *Low*, 900 F. Supp. 2d at 1026 (same). Moreover, the case Plaintiffs cite, *CTC Real Estate Services v. Lepe*, 140 Cal. App. 4th 856 (2006), dealt with Cal. Penal Code § 530.5, which does *not* define property, but proscribes obtaining personal information with intent to defraud. *Id*. at 859-60. And the statute's definition of personal information includes items like credit card numbers and health care records, *not* browsing history. Cal. Penal Code § 530.55(b). Second, any cookies and referer URLs (the only things Facebook allegedly received that Plaintiffs object to) were not "stolen," despite Plaintiffs' conclusory assertions. (Opp. at 29-30). Referers are sent to Facebook when someone visits a page with Facebook content, *i.e.*, they are created for the very purpose of sending them to Facebook. Similarly, the cookies at issue here were set by Facebook. Plaintiffs rely on a theory of false pretense to turn this standard operation of the Internet into theft (Opp. at 29-30), but that theory fails for the same reasons Plaintiffs' other fraud theories fail. Third, Facebook did not sell any cookies or referers. Plaintiffs speculate that Facebook charged more to advertisers based on use of this information (Opp. 30), but cites to no such allegation in the SAC. Nor do Plaintiffs cite any case law to support the novel idea that Facebook's sale of advertising somehow amounts to a sale of the supposed *property* they allege was stolen.

III. CONCLUSION

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

Dated: March 10, 2016

COOLEY LLP

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