COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
MATTHEW D. BROWN (196972)
(brownmd@cooley.com)
JEFFREY M. GUTKIN (216083)
(jgutkin@cooley.com)
KYLE C. WONG (224021)
(kwong@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

DECLARATION OF NATALIE NAUGLE IN SUPPORT OF DEFENDANT FACEBOOK, INC.'S RESPONSE TO PLAINTIFFS' ADMINISTRATIVE MOTION TO FILE UNDER SEAL

DATE: April 28, 2016
TIME: 9:00 a.m.
JUDGE: Hon. Edward J. Davila
COURTROOM: 4
TRIAL DATE: Not Yet Set

[PUBLIC REDACTED VERSION]

Exhibit 2

to Declaration of David A. Straite Motion

[Re: ECF No.104-3]

REDACTED VERSION OF DOCUMENTS SOUGHT TO BE SEALED

EXHIBIT 2
TO
DECLARATION OF DAVID A. STRAITE

FILED UNDER SEAL

Stephen G. Grygiel (*admitted pro hac vice*)
SILVERMAN THOMPSON SLUTKIN WHITE LLC
201 N. Charles Street, 26TH Floor
Baltimore, MD 21201
Tel.: (410) 385-2225
Fax: (410) 547-2432
sgrygiel@mdattorney.com

Frederic S. Fox (admitted *pro hac vice*)
David A. Straite (admitted *pro hac vice*)
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue, 14th Floor
New York, NY 10022
Tel.: (212) 687-1980
Fax: (212) 687-7714
dstraite@kaplanfox.com

Laurence D. King (206423)
Mario Choi (243409)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, 4th Floor
San Francisco, CA 94104
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: FACEBOOK, INC. INTERNET TRACKING LITIGATION

No. 5:12-md-02314-EJD

PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO FACEBOOK'S MOTION TO DISMISS

Date: April 28, 2016
Time: 9:00am
Place: Courtroom 4
Judge: Hon. Edward J. Davila

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

I. INTRODUCTION

Defendant Facebook, Inc.'s ("Facebook") Motion to Dismiss (the "Motion") the Second Amended Complaint (the "SAC"), asks this Court to deny recourse for millions of Americans whose privacy Facebook repeatedly and profoundly violated through the unauthorized and secret tracking of their web browsing. Ignoring recent case law and new facts in the SAC, Facebook's motion is primarily built on two false premises. First, Facebook argues its misappropriation of billions of URLs and other personal data is not "injury in fact" for Article III standing. Second, Facebook argues URLs categorically do not contain "contents," the interception of which violates federal and state wiretap laws.

Remarkably, Facebook's Motion ignores the recent landmark opinion in *In re Google Inc. Cookie Placement Consumer Privacy Litig*., 806 F.3d 125 (3d Cir. Nov. 10, 2015 as amended Nov. 12, 2015) ("Google Cookie Placement"). This Court's order dismissing plaintiffs' First Amended Complaint relied on the lower court decision in *Google Cookie Placement*, and described the facts as "virtually indistinguishable." *In re Facebook Internet Tracking Litigation*, 2015 WL 6438744 at *6 (N.D. Cal. Oct. 23, 2015) (the "Order"). Facebook brought the district court's original opinion in *Google Cookie Placement* to this Court's attention in a Statement of Recent Decisions dated October 10, 2013 [ECF No. 69]. Three weeks after the Order, however, the Third Circuit *reversed* the district court on the standing and contents issues on which Facebook relies.

Facebook also argues that users have no reasonable expectation of privacy in a URL. But Facebook ignores the SAC's focus on the *aggregation* of web browsing history, and then brushes aside as "dicta" a recent unanimous Supreme Court decision finding a privacy interest in aggregated URLs. Facebook also relegates to a footnote a California state court decision against Facebook on identical facts (Exhibit HH to SAC), finding a privacy interest in aggregate web browsing history.

Finally Facebook complains that the SAC does not identify precisely which websites were visited. Facebook does not mention, however, that Facebook has that information for each plaintiff but has refused to produce it.

II. FACTUAL AND PROCEDURAL BACKGROUND

Plaintiffs filed the first amended complaint on May 23, 2012 [ECF No. 35] (the "FAC"). This Court granted Facebook's motion to dismiss all counts on October 23, 2015 with leave to re-plead. *See*

Order, 2015 WL 6438744. Plaintiffs filed the SAC on November 30, 2015. Defendants moved to dismiss on January 14, 2016 [ECF No. 94] (the "Motion"). Accompanying this opposition is the Declaration of Stephen Grygiel dated Feb. 18, 2016 ("Grygiel Decl.") providing referenced exhibits. Other documents accompanying the SAC as exhibits are designated "SAC Ex. – ".

The SAC differs from the FAC in several ways. First, four counts have been dropped and four have been added:

Claim	First Amended Complaint	Second Amended Complaint
Violation of the Federal Wiretap Act	Count I	Count I
Violation of the Federal Stored Communications Act	Count II	Count II
Violation of the Federal Computer Fraud and Abuse Act	Count III	[dropped]
Invasion of Privacy	Count IV	Count IV
Intrusion upon Seclusion	Count V	Count V
Conversion	Count VI	[dropped]
Trespass to Chattels	Count VII	Count IX
California Unfair Competition Law ("UCL")	Count VIII	[dropped]
California Penal Code § 502 (computer crime law)	Count IX	Count X
California Invasion of Privacy Act ("CIPA")	Count X	Count III
California Consumer Legal Remedies Act	Count XI	[dropped]
Breach of Contract	[not asserted]	Count VI
Breach of Duty of Good Faith and Fair Dealing	[not asserted]	Count VII
Civil Fraud	[not asserted]	Count VIII
California Statutory Larceny	[not asserted]	Count XI

Second, the SAC outlines litigation in the United States and Europe regarding privacy claims arising from Facebook's tracking of internet search histories. SAC ¶¶ 146-71. Third, the SAC adds facts supporting a serious invasion of privacy resulting from Facebook's internet tracking, with a focus on the aggregation of internet communications and personal data. Fourth, the SAC discusses a greater number of cookies Facebook used to track users post-logout, including the *a_user, c_user, datr, lu, fr* and [redacted] cookies. Fifth, the SAC cites discovery documents confirming [redacted] and [redacted] Sixth, the SAC specifically pleads that each named plaintiff actually visited websites with Facebook "Like" buttons while logged out during the class period, that intercepted URLs containing detailed file-paths beyond simple IP addresses, and more fully pleads Facebook's business practice of

tracking all visits to such pages. Finally, the SAC asserts claims specifically on behalf of a subclass of users of Microsoft Internet Explorer (the "IE Subclass").

III. LEGAL STANDARDS

A. Pleading Standards

Facebook agrees that all but three (fraud, statutory larceny and § 502) of the SAC's counts are governed by the notice pleading standards of Fed. R. Civ. P. 8(a). Motion at 7. Plaintiffs' factual allegations need only be detailed enough to "raise a reasonable expectation that discovery will reveal evidence" of the illegality alleged. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007). Dismissal at the pleading stage is only appropriate "where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Center*, 521 F.3d 1097, 1104 (9th Cir. 2008).

For Rule 12(b)(6) purposes, the Court must accept as true all the SAC's well-pleaded factual allegations. *Ashcoft v. Iqbal*, 556 U.S. 662, 664 (2009). The Court must construe those facts and draw all inferences in the manner most favorable to the plaintiff. *Love v. United States*, 915 F.2d 1242, 1245 (9th Cir. 1988). Nevertheless, Facebook improperly bases several of its arguments on facts materially differing from those in the SAC, and these are noted below where appropriate.[1]

B. Collateral Estoppel

Under 28 U.S.C. § 1738, federal courts give full faith and credit to state court judgments. *San Remo Hotel v. San Francisco*, 545 U.S. 323, 336 (2005); *Brodheim v. Cry*, 584 F.3d 1262, 1268 (9th Cir. 2009). To determine the preclusive effect of a state court judgment, federal courts look to state law. *Heinrichs v. Valley View Development*, 474 F.3d 609, 615 (9th Cir. 2007). In California, the preclusive effect of a final judgment can be either "issue preclusion" (i.e., collateral estoppel) or full "claim preclusion." *Mycogen Corp. v. Monsanto Co.*, 28 Cal. 4th 888, 896–97 (2002). Claim preclusion bars claims/issues actually litigated, or that could have been litigated, in a prior proceeding. *See Palomar Mobilehome v. San Marcos*, 989 F.2d 362, 364 (9th Cir. 1993). Issue preclusion, on the other hand,

[1] *Cf.* Memo. at 5, fn. 4 ("[b]ecause cookies do not collect any information") *with* SAC ¶ 23 (cookies are "small files that store information").

only bars re-litigation of individual issues. As explained below, Facebook is attempting to re-litigate two issues decided in previous cases and which should be precluded.

IV. ARGUMENT

A. Plaintiffs Have Article III Standing

1. Standing May Exist Solely by Virtue of Statutes

Facebook concedes that under current Ninth Circuit law, Art. III standing may exist solely by virtue of statutes creating legal rights. *See Warth v. Seldin*, 422 U.S. 490, 500 (1975); *Edwards v. First American Corp.*, 610 F.3d 514, 516-17 (9th Cir. 2010); Motion, fn. 7; Order, 2015 WL 6438744 at *7-8. Plaintiffs satisfy the injury-in-fact requirement for standing by alleging an invasion of a statutory legal right. Economic loss is not required. Facebook baselessly argues that plaintiffs' allegations are insufficiently detailed to establish statutory standing and that economic harm is a statutory prerequisite for three of the California claims (Cal. Penal Code § 502, fraud, and statutory larceny).[2]

2. Viable State-Law Claims are a Basis for Standing

a. Plaintiffs Have Viable State-Law Causes of Action

Plaintiffs have alleged several concrete harms that establish Article III harm: First, Facebook failed to expire personally identifying tracking cookies from their browsers at logout, and plaintiffs recently learned in discovery that [redacted]. *See, e.g.*, SAC ¶ 76. This concrete and systematic invasion of class members' computers exceeded the authorized use of plaintiffs' resources for both the Class and the IE Subclass. Second, Facebook misappropriated billions third-party private communications to which Facebook was not a party, associated them with user-identifying data in real time, and collected them without authorization. This is economic harm sufficient for standing. Third, the unauthorized collection and aggregation of plaintiffs' and class members' web browsing is a serious invasion of privacy under California law.

Facebook argues that plaintiffs have no standing to pursue valid state law claims to address the injuries above because plaintiffs' ability to monetize the misappropriated data remained undiminished. Such diminution is not Constitutionally required and the argument is factual anyway. More broadly,

[2] Facebook does not deny that economic harm is not a prerequisite specifically for claims under the CIPA. *See* Cal. Penal Code § 637.2(c) ("It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.").

"concrete harm" need not be economic. *Sierra Club v. Morton*, 405 U.S. 727, 734 (1972). Even in cases involving economic harm, where data is misappropriated and used for financial gain by another, the victim suffers injury even absent the victim's intent to monetize the data himself.

FMC Corp. v. Boesky, 852 F.2d 981 (7th Cir. 1988), an insider trading case, illustrates Plaintiffs' standing. In the FMC's civil case for disgorgement, Mr. Boesky argued that FMC had no standing because FMC was not denied the use of its own data, which Boesky had misappropriated. The Seventh Circuit disagreed: "We hold that this misappropriation constitutes a distinct and palpable injury that is legally cognizable under Article III's case or controversy requirement." *Id.*

First, the court held that "[c]onfidential business information, even though intangible in nature, is corporate property . . . to which the corporation has the exclusive right and benefit." *Id.* If the information is misappropriated, it harms the victim. "***Although FMC was not actually deprived of the information itself***, FMC, as a result of this wrongful conduct, was denied the right to use exclusively its confidential information. And that is injury." *Id*. (emphasis added).

Boesky teaches that if the claim is cognizable under state common law, it is Constitutionally cognizable in federal court. The court reasoned:

> *For example, the actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.* ***The same must also be true of legal rights growing out of state law****…. Properly pleaded violations of state-created legal rights, therefore, must suffice to satisfy Article III's injury requirement. Thus,* **even in the absence of a specific finding that FMC was injured by the misappropriation of its confidential business information, FMC sufficiently alleged the violation of a state-law right that in itself would suffice to satisfy Article III's injury requirement**.

Id. at 993 (citations omitted) (emphasis added); *accord, Veleron Holding, B.V. v. Morgan Stanley*, 2015 WL 4503580 at *15 (S.D.N.Y. July 23, 2015) (citing *Boesky*). More recently, the Ninth Circuit explicitly agreed with *Boesky* and held that requiring out-of-pocket damages might actually run afoul of the *Erie* doctrine. *Cantrell v. City of Long Beach*, 241 F.3d 674, 683 (9th Cir. 2001) (citing *Boesky*); *Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938) (federal courts apply state laws when sitting in diversity); *Guaranty Trust Co. v. York*, 326 U.S. 99, 105 (1945) (for diversity jurisdiction "Congress

never gave, nor did the federal courts ever claim, the power to deny substantive rights created by State law or to create substantive rights denied by State law").

Cantrell's focus on diversity cases merits attention here. For example, some states recognize claims for privacy intrusions even absent economic damages. *See, e.g., Rhodes v. Graham*, 37 S.W.2d 46, 47 (Ky. App. 1931) ("The fact that the damages cannot be measured by a pecuniary standard is not a bar to his recovery."). If a plaintiff were required to pursue his Kentucky tort claim in federal court, *Erie* says the claim ought to proceed substantively unaltered. Facebook's standing argument, however, requires the federal court to violate *Erie* by dismissing a viable state law claim because the privacy invasion did not cause any out-of-pocket damages.

Facebook's view of standing creates further problems in the Class Action Fairness Act ("CAFA") context. Say a plaintiff pursues a California state court case with a class limited to California members without out of pocket losses. Say also a parallel nationwide class asserts an identical California claim. That latter case must proceed in federal court under the CAFA. Facebook's Article III theory would result in the broader class having its state common-law causes of action extinguished while the state case proceeds. Such a result is contrary to CAFA's non-substantive purpose. *See* Senate Report 109-14 at p. 61 (Feb. 28, 2005), attached as Ex. 1 to Grygiel Decl.

The CAFA issue above is not merely academic in this case. Approximately one-seventh of the class here is covered by a state-law class action in Santa Clara County Superior Court asserting only state law claims against Facebook related to identical conduct. *See Ung v. Facebook, Inc*., Case No. 1-12-cv-217244 (Santa Clara Cty). The state court rejected Facebook's standing argument, finding that "Facebook's alleged conduct constitutes a serious invasion of a privacy interest." *See* SAC, Ex. HH. The Court's Order, that plaintiffs lack standing for the unauthorized collection and use of their personal data absent a showing that plaintiffs' ability to monetize the data was diminished as a result (Order, 2015 WL 6438744 at *6) is inconsistent with *Erie* and *Cantrell*.

Furthermore, the law changed significantly after the Order. This Court cited three opinions for its standing ruling. One was *Google Cookie Placement.* *See* Order, 2015 WL 6438744 at *6. Less than three weeks after the Order, however, the Third Circuit reversed the district court's ruling on standing:

> *For purposes of injury in fact, the defendants' emphasis on economic loss is misplaced…. a plaintiff need not show actual monetary loss for purposes of injury in fact.*
>
> * * * * * *
>
> *The plaintiffs here base their claims on highly specific allegations that the defendants, in the course of serving advertisements to their personal web browsers, implanted tracking cookies on their personal computers. Irrespective of whether these allegations state a claim, the events that the complaint describes are concrete, particularized, and actual as to the plaintiffs. To the extent that the defendants believe that the alleged conduct implicates interests that are not legally protected, this is an issue of the merits rather than of standing.*

Google Cookie Placement, 806 F.3d at 134-35 (citations omitted). The court allowed claims for invasion of privacy and intrusion upon seclusion to proceed, and remanded. *Id*. at 153.

This Court found the district court's opinion in *Google Cookie Placement* "instructive mainly because Plaintiffs' allegations are virtually indistinguishable." *Id*. at *6. Plaintiffs agree. *Google Cookie Placement* is perfectly consistent with the simple formulations of *Boesky* and *Cantrell*: if a claim is cognizable under state common law it is Constitutionally cognizable in federal court.

Finally, plaintiffs submit that the Ninth Circuit extended *Cantrell* specifically into data privacy cases. *See In re Facebook Privacy Litig.*, 572 Fed. Appx. 494 (9th Cir. 2014) (reversing district court and holding plaintiffs' allegations of misappropriation of their PII "sufficient to show the element of damages" for contract and fraud claims). This Court's Order limiting *In re Facebook Privacy Litigation* to cases where a defendant shared personal data with advertisers (*see* Order, 2015 WL 6438744 at *6, fn. 3) respectfully is inconsistent with the Ninth Circuit's standing ruling *In re Facebook Privacy Litig.* *See also In re Anthem, Inc. Data Breach Litig*., 5:15-MD-2617-LHK, Order on Motion to Dismiss, Slip Op. at 45-48 (N.D. Cal. Feb. 14, 2016) (citing *In re Facebook Privacy Litigation* as basis to conclude that loss of value of personal information "represents a cognizable form of economic injury").

3. Plaintiffs Have Pled Actual Injury to Them

Facebook argues that plaintiffs must allege specific third-party webpages visited during the class period or specific communications (URLs) that were intercepted. Motion at 10. Facebook misstates the allegations in the SAC and also misstates the applicable law. Pleading standing is no different than

pleading anything else: a short and plain statement putting the defendant on notice suffices. *See, e.g.*, *Nat'l Council of La Raza v. Cegavske*, 800 F. 3d 1032, 1039 (9th Cir. 2015). Notice pleading, buttressed by *general* facts sufficing to show "plausibility" – the "reasonable expectation that discovery will reveal evidence" supporting the claim – is the rule. *See, e.g., Starr v. Baca*, 652 F. 3d 1202, 1212, 1214 (9th Cir. 2011). The facts alleged need only establish the plausibility of standing. *See Landers v. Quality Communications, Inc.*, 771 F. 3d 638, 645 (9th Cir. 2015).

Plaintiffs' FAC alleged that Facebook installed tracking and session cookies on their computers without consent, that they visited websites with Facebook functionality while logged out, and that Facebook intercepted their electronic communications were intercepted. *See, e.g.*, FAC ¶ 103. The Order only identified one insufficiency: Plaintiffs failed to allege that Facebook obtained the "contents of a communication attributable to them" making the allegation too general to "nudge" a CIPA claim "across the line from conceivable to plausible." Order, 2015 WL 6438744 at *10 (citing *Iqbal*, 556 U.S. at 680). The FAC only alleged that communications were intercepted, but never alleged that the communications contain contents. For the SAC, plaintiffs reviewed the URLs of websites visited while logged out of Facebook, and specifically alleged that many of the intercepted URLs "contain detailed file paths containing the content of GET and POST communications." *See, e.g.*, SAC ¶ 113. These communications were more than IP addresses. The SAC also identifies the specific browser used by each plaintiff and alleges whether the computer was shared. These extra allegations provide the "nudge" the Court required. *See Erickson v. Pardus*, 551 U.S. 89, 94 (2007) (under Rule 8(a), "[s]pecific facts are not necessary…the statement need only 'give the defendant fair notice of what the …claim is and the grounds upon which it rests.'").

Furthermore, plaintiffs alleged with summary-judgment-like detail a business practice through which Facebook gathered billions of URLs during the class period and associated them with actual subscribers. SAC ¶¶ 68-78. Independent researchers (*see* SAC ¶ 58) support these allegations. So do Facebook's own documents. Such detailed allegations of a general business practice suffice to allege that plaintiffs were harmed. *See, e.g., Obama v. Klayman*, 800 F.3d 559, 563-64 (D.C. Cir. 2015) (standing established to assert claim against the NSA to proceed even though the plaintiff had not

alleged the particular phone calls at issue because the plaintiff "offer[ed] an inference derived from known facts.").

4. In the Alternative, Standing Should Be Resolved at a Later Stage

Although standing is normally a threshold issue to be resolved at the outset of a case, courts considering class actions may defer resolution until a later stage, even until class certification. *See Amchem Prods., Inc. v. Windsor*, 521 U.S. 591 (1997). In situations like this one prudential concerns favor deferral (*see In re Target Corp. Data Sec. Breach Litig*., 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014)), and "there is no rigid rule that precludes class certification from being addressed before standing issues." *In re Carrier IQ, Inc., Consumer Privacy Litig*., 78 F. Supp. 3d 1051 (N.D. Cal. 2015); *accord, In re Anthem, Inc. Data Breach Litig*., Slip Op. at 10 ("the Court finds that it has discretion to decide . . . when to consider issues of standing').

If the Court requires allegations of actual websites visited by the named plaintiffs, or actual URLs intercepted, plaintiffs request deferral of the standing issue pending resolution of an upcoming motion to compel. Facebook has refused to produce documents related to the named plaintiffs. Facebook has records of all data collected on the named plaintiffs, which might resolve this issue once and for all.

B. Plaintiffs Have Adequately Pled Federal Claims Under the ECPA

1. Specificity of Pleadings

Full of merits-based factual arguments about the Internet's functioning and, in particular, the functioning of Facebook's surreptitiously planted cookies,[3] Facebook's brief wishes away plaintiffs' many detailed factual allegations, from defendant's own documents, showing defendant's knowledge of its illicit post-log out tracking. Facebook assumes a requirement of proof in the pleadings that neither Fed. R. Civ. P. 8(a), nor 9(b), nor Ninth Circuit precedent imposes. Facebook's arguments nowhere recognize that any "ambiguities" in this highly technical setting – such as whether a personal computer, server, software or cookie can function as a "device" for Wiretap Act purposes, a "facility" for Stored

[3] *See, e.g.,* Memo at 2 ("proof of injury; "record information…transmitted as part of the normal operation of the Internet;"); at 4 ("[l]ike any web content provider, Facebook's servers…."); at 17 ("Facebook, like any other third-party provider of webpage content…").

Communications Act purposes, or as a "machine, instrument or contrivance" for CIPA purposes – "must be resolved in favor of the pleadings." *Heldt v. Tata Consultancy Servs., Ltd.*, 2015 WL 5542303, at *3 (N. D. Cal. Sep. 18, 2015) (citing *Walling v. Beverly Enters.*, 476 F. 2d 393, 396 (9th Cir. 1973)).

Alleging long-established, legally cognizable claims, the SAC does much more than simply "recite the elements of" those claims. *Starr,* 652 F. 3d at 1216. Plaintiffs do not, for example, merely allege "labels," that Facebook used a "device" to "intercept" the "content" of confidential communications. Plaintiffs factually plead the identity of such devices, the means and method of the interceptions, and the contents of the communications. Facebook's factual disagreement with those contentions is for discovery and summary judgment or trial. *See Walker v. B&G Foods, Inc.*, 2016 WL 463253, at * 2 (N.D. Cal. Feb. 8, 2016) ("In the Ninth Circuit, '[i]f there are two alternative explanations, one advanced by the defendant and the other advanced by the plaintiff, both of which are plausible, plaintiff's complaint survives a motion to dismiss.").

2. The Wiretap Act

a. Plaintiffs Adequately Allege Content.

Content "includes *any* information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The Order held that plaintiffs' failed to allege Wiretap content because of similarity to "the referrer headers addressed in *Zynga Privacy Litigation*." *Order* at 16. Plaintiffs' SAC shows that the information Facebook acquired differs from that in *Zynga.* The *Google Cookie Placement* ruling and recently declassified cases from the Foreign Intelligence Surveillance Court explain why detailed URLs do contain "content," i.e. "any information relating to the substance purport, or meaning" of a communication.

Plaintiffs' SAC alleges Defendant acquired "detailed URL requests and search queries" and explains that URLs are composed of several different parts. SAC at ¶185. For example, the URL http://progressivehealth.hubpages.com/hub/How-Do-I-Reduce-Herpes-Breakouts contains four parts: (1) "http" establishes the basic computer language of the communication; (2) "progressivehealth.hubpages.com" identifies the website to which the communications will be sent and received, i.e. the other party to the communication; (3) "How-Do-I-Reduce-Herpes-Breakouts" is the name of the precise file requested; and (4) "hub" plus "How-Do-I-Reduce-Herpes-Breakouts" is called

the "file path." SAC at ¶34. In this example, the phrase "How-Do-I-Reduce-Herpes Breakouts" is content because it contains information relating to the substance, purport, or meaning of a communication. Likewise, in the URL http://www.nytimes.com/2011/08/10/nyregion/post-traumatic-stress-disorder-from-911still-haunts.html, the phrase "[PTSD] from 911 still haunts" is content. *See* SAC at ¶ 35.

In *Zynga*, the URLs at issue were *Facebook* URLs that only included the name of a person or group. *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1109 (9th Cir. 2014). The URLs here are third-party communications, and include search terms or other detailed substance, purport and meaning, *e.g.*, like "How Do I Reduce Herpes Breakouts" and "[PTSD] from 911 still haunts." *See id.* (URLs contain content where include "a search term or similar communication."). Defendant's argument that computer-generated information can never contain content misstates *Zynga's* holding. The SAC-specified URLs were not computer spawned but were only generated after the user sent a 'GET' command to a non-Facebook website by either typing a URL into the navigation bar or clicking on a hyper-link. SAC at ¶31. The SAC is consistent with Internet users' everyday experience and the Supreme Court's explanation of the "relatively straightforward" manner of Internet communications. *See Reno v. ACLU*, 521 U.S. 844, 852-53 (1997) ("Users generally explore a given Web page, or move to another, by clicking a computer 'mouse' on one of the page's icons or links…".). Whether a detailed URL results from a user typing all of the information into their toolbar or clicking on a link, the underlying intentional communicative thought by the user is the same.

Affirmatively requesting information, and conveying personal thought, on how "PTSD from 9/11 still haunts," the user is sending a protected electronic communication under the Act. *See* 18 U.S.C. § 2510(12) ("Electronic communication" includes "any transfer of signs, signals, … data, or intelligence of any nature"). The browser sends a GET request directly to the NYT and populates the toolbar with the detailed URL includes the phrase "[PTSD] from 9/11 still haunts." That URL is contemporaneously acquired by Facebook without the user's knowledge or consent. The NYT responds with a 3,000 word essay on PTSD after 9/11 that is also protected by the Wiretap Act. SAC at ¶ 35.

Clicking on a mouse rather than typing the entire URL into their toolbar the user has still sent a protected communication. Another protected communication is about to be received. The ECPA's

primary purpose was to "effectively protect the privacy of electronic communications" by updating the law to "ke[ep] pace with the development of communications and computer technology … and the structure of the telecommunications industry" and "bring it in line with technological developments[.]" Senate Report 99-541 (Oct. 17, 1986) at 2-3, Grygiel Decl. Ex. 2 .

Consider email where the user forwards a message to another person without touching the subject line of the original email. Generated by the email providers' computer code, the forwarded email's subject line, is nearly identical to the subject line of the original email. Defendants' logic leads to the absurd result that such subject lines contain no content because the email providers' default rules "produced" them. So, too, with Defendant's argument about detailed URLs.

In *Declassified Opinion from the FISC*, provided to the Court on August 15, 2014 [ECF No. 78], the NSA argued it had authority under the Pen Register Act to track URLs because they are DRAS (dialing, routing, addressing, or signaling) information. The FISC, which routinely hears Wiretap cases, rejected this interpretation, holding "DRAS and content are not mutually exclusive categories." *Id*. at 31.

In *Google Cookie Placement*, the Third Circuit explained "everything before the .com instructs a centralized web-server to direct the user to a particular website, but post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user… between the information revealed by highly detailed URLs and their functional parallels to post-cut-through digits, we are persuaded that – *at a minimum* – some queried URLs qualify as content." 806 F.3d at 139 (emphasis added).

The *Google Cookie Placement* panel was persuaded by "post-cut-through-digit" cases holding that "numbers dialed from a telephone after a call is already set-up" are content. 806 F.3d at 138, citing *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000), *see also Brown v. Waddell*, 50 F.3d 285, 87-88 (4th Cir. 1995) (numbers sent to pager that are "more extensive … than those in telephone numbers" contain "content."). *Google Cookie Placement* also cited the PATRIOT Act's legislative history, in which a report of the House Judiciary Committee explained that a pen register order "could not be used to collect information other than [DRAS], such as the portion of a URL specifying Web search terms or the name of a requested file or article." *See* HR. Rep. 107-236 at 53 (Oct. 11, 2001), Grygiel Decl. Ex. 3; *see also In re Application for Pen Register*, 396 F.Supp.2d 45, 49-50 (D. Mass.

2005) ("Contents" included URL "subject lines, application commands, search queries, *requested file names*, and *file paths*."); *U.S. v. Forrester*, 512 F.3d 500, n. 6 (9th Cir. 2008) (URLs, unlike IP addresses, "reveal[] much more information" about user's Internet activity, including articles viewed.)

b. Plaintiffs Adequately Allege Interception, i.e. Contemporaneous Acquisition

Courts have interpreted the Wiretap Act to require the interception (18 U.S.C. § 2501(4)) to be contemporaneous to the sending or receipt of a communication. Plaintiffs know of no court that has accepted defendant's argument that simultaneous capture of referrer URLs appended to third-party cookies do not involve the acquisition of information contemporaneous to a communication. *Cf. U.S. v. Szymuskiewicz*, 622 F.3d 701, 706 (8th Cir. 2010) ("contemporaneous does not mean 'in flight' or 'in the middle' or any football metaphor;" is "contemporaneous by any standard" when the Wiretap defendant and the victims "receive[] each message with no more than an eyeblink in between"); *U.S. v. Councilman*, 418 F.3d 67, 76 (1st Cir. 2005) ("*Councilman I*") ("[B]road definition of … storage was to enlarge privacy protections for stored data … not to exclude email messages stored during transmission from these strong protections.").

Defendant acquired plaintiffs' communications with websites as in *Szymuskiewicz*. The re-direction of the URLs in this case functionally operated like an email forwarding rule and Facebook acquired users' communications to the websites in a time frame "contemporaneous by any standard." Defendant acquired information relating to the substance, purport, and meaning of communications that user received in return from the websites. SAC ¶ 184. Facebook's acquisition was completed "before the communication between the plaintiffs and the various websites were completed." SAC ¶ 184.

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) is inapposite. In *Konop*, the defendant gained unauthorized access to a "secure" website where the contents of the plaintiffs' communications had been stored on a server for an unspecified period of time, but far longer than the milliseconds at issue here. *Id*.

Facebook's argument that it must receive "the actual communication" misstates the law. Motion at 12.[4] An interception is defined as the "acquisition of the contents of any … electronic

[4] Facebook misstates the clear facts alleged in the SAC when it only discusses communications sent from the Internet users and ignores communications users received. SAC ¶ 184. ("In fact, Facebook

communication[.]" 18 U.S.C. § 2510(4). "Content" is defined as "any information concerning the substance, purport, or meaning" or the subject communication. 18 U.S.C. § 2510(8). The Wiretap Act prohibits the "acquisition of any information concerning the substance, purport, or meaning of any electronic communication." It is enough for a defendant to acquire post-cut-through dialed digits, the subject line of an email, or, in this case, the portion of a URL after the .com.

Finally, Facebook argues "Plaintiffs' browser sends two different communications at two different times." Motion at 12. The plaintiffs, however, are not browsers. The plaintiffs' are sentient human beings who made human decisions to send and receive personal communications from websites.

c. Plaintiffs Adequately Allege the Use of a Device.

The Wiretap defines an "electronic … or *other* device" as "*any* device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). Emphasis added. "*Other*" and "*any*" have meaning. They focus on function – i.e. whether something could be used to acquire communications. Congress chose these broad definitions to further its central purpose of effectively protecting the privacy of electronic communications. Random House defines device as, among other things: (1) "a thing made for a particular purpose; an invention or contrivance, especially a mechanical or electrical one;" (2) "a plan or scheme for effecting a purpose;" and (3) "a crafty scheme, trick."

The SAC alleges defendant used seven devices to acquire communications: (1) cookies; (2) web-browsers and their constituent files; (3) computing devices; (4) Facebook's web-servers; (5) the web-servers of the websites involved; (6) Facebook's computer code; and (7) the plan Facebook carried out to effectuate the acquisition of plaintiffs' communications. SAC ¶ 187.

Web-servers and computers are devices under the Wiretap Act. *Szymuszkiewicz*, 622 F.3d at 707 (discussing *Crowley v. Cybersource Corp.*, 166 F.Supp.2d 1263, 1269 (N.D. Cal. 2001)). Software and computer code are devices. *In re Carrier IQ*, 78 F. Supp. 3d at 1067 ("Plaintiffs have sufficiently alleged that the Carrier IQ Software is a 'device' for purposes of the Wiretap Act."). Facebook's cookies are devices under the act because they are an invention designed for the purposes of "track[ing] and record[ing] an individual Internet user's communications with and activities on websites across the

---

received the communications before the communication between the plaintiffs and the various websites were completed.")

Internet." SAC ¶ 52. Facebook's secret interception program is a "device" because it is a "plan or scheme" to carry out the purpose of acquiring the electronic communications of Internet users.

Crowley is inapposite. There the Court held that Amazon could not be liable under the Act because it "acted as no more than the second party to a communication" when it knowingly forwarded information to CyberSource to verify one of its users credit card information. *Id*. at 1266. Facebook is not a party to a communication between a plaintiff and a third-party website as Amazon was in *Crowley*.

Also inapposite, *Potter v. Havlicek*, 2008 WL 2556723 (S.D. Ohio June 23, 2008), arose out of a divorce. A jealous husband installed software on a family computer to surreptitiously record his wife's communications. The husband interpleaded the software company. The Court concluded that "computer software alone" is not a Wiretap Act "device" in the context of a software manufacturer who never received the alleged intercepted communications. *Id*. at *7 (Wiretap Act "does not contemplate imposing civil liability on software manufacturers and distributors for the activities of third parties"). Plaintiffs here allege seven devices, not *computer software alone*. Nor is Facebook a software manufacturer who received no communications and merely sold software to a third-party who subsequently used it to intercept another person's communications. Facebook used the software to acquire communications.

d. Facebook is Not a Party to the Communication.

Facebook tacitly concedes it is a "third-party" and not a party to the relevant communications between the users and the websites. MTD at 14, 21. Plaintiffs agree as the Court did. *Order* at 18-19. The SAC alleges Facebook intercepted communications that the logged-out plaintiffs sent and received from other websites. SAC ¶ 184. The SAC illustrates that communications between users and websites occur through a channel separate from the path through which Facebook acquires information. SAC ¶ 60. The SAC alleges interceptions while logged-out users were sending communications to non-Facebook websites, with no intention of sending any information to Facebook and when Facebook explicitly promised it would not acquire user communications.

Facebook's interpretation of the "party" exception obliterates the Wiretap Act. Suppose that, for "security purposes," the IRS places cookies on the web-browsers of every American who files taxes online. The IRS promises these Americans that it will not access the cookies except when the tax-filer is

actually on the IRS web-page attempting to file taxes. Suppose the IRS, for what it describes as "security purposes only" so the IRS is sure only approved vendors use the program, requires tax prep firms to place IRS computer code in the header of each web-page the firm controls if the firm wants its customers the option to file their taxes online. The code also places an IRS logo on the page. The IRS informs firms it will receive some information, but promises not to track individual tax-filers through cookies while they are not actively logged-in to the IRS site. Accordingly, tax filers permit the placement of cookies and tax preparation firms place the IRS code on every page of their websites for these limited "security purposes," including pages like: http://www.efile.com/what-are-the-penalties-for-not-filing-a-tax-return-or-not-to-pay-taxes-IRS-penalty-list/.

However, unbeknownst to the tax-filers and the tax preparation firms, suppose the IRS computer code tracks taxpayers and their communications (including the referrer URL above) so that the IRS acquires the content of every communication John Doe makes with his tax preparation firm through his web-browser – including, for example, whether he sent a communication seeking information on "what are the penalties for not filing or tax return or not to pay taxes?" The IRS then uses the information to determine whom to audit. Under Facebook's logic, directly contrary to Congressional intent, the IRS is a "party" to the intercepted communication between the tax-filer and their chosen tax preparation firm.

Similarly, *In re Pharmatrak*, 329 F.3d 9 (1st Cir. 2003) rejected an argument identical to Facebook's. *See also Szymuszkiewicz*, 622 F.3d 701 (rejecting similar argument where defendant used email forwarding rule to instruct victim's email service to automatically re-direct all emails to defendant); *but cf. Google Cookie Placement*, 806 F.3d at 143-45.

Crowley, cited repeatedly by defendant, illustrates why plaintiffs should prevail. Making an internet purchase, the *Crowley* plaintiff knowingly sent financial information to Amazon. Amazon transferred the data to CyberSource to verify payment details. The communication between the plaintiff and Amazon occurred on the Amazon web-page, a key fact Facebook omits. *Crowley* explains: "Amazon merely received the information transferred to it by Crowley, an act without which there would be no transfer. Amazon acted as no more than the second party to a communication. This is not an interception as defined by the Wiretap Act." *Id*. at 1269.

e. Consent is an Affirmative Defense

Defendant bears the burden of proving the affirmative defense of consent. *See Pharmatrak*, 329 F.3d at 19. No consent appears in the SAC so consent cannot be resolved on Facebook's Rule 12(b)(6) motion. *Scott v. Kuhlmann*, 746 F.2d 1377, 1378 (9th Cir. 1984) (citing Wright & Miller, Federal Practice and Procedure, § 1277 at 328-30) (affirmative defenses may not be raised in a motion to dismiss unless no disputed fact issues).

For Wiretap claims, "consent should not be casually inferred." *Pharmatrak* at 20. No constructive consent is permissible and "without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception." *Pharmatrak* at 19, 20. Facebook's interceptions broke its privacy promises and included the collection of personal data. No consent, actual or implied, exists. *Id*.

f. The Ordinary Course of Business Exception Does Not Apply

The Wiretap Act exception for interceptions "being used by" an ECS provider in the "ordinary course of its business (18 U.S.C. § 2510(5)(a)) only applies to actual ECS providers. *In re Google Inc. Gmail Litig*., 2013 WL 5423918 at *11 (N.D. Cal. Sep. 26, 2013) (exemption "designed only to protect [ECS] providers"); *Shefts v. Petrakis*, 2012 WL 4049484 at *5 (C.D. Ill. Sep. 13, 2012); cited with approval in *In re Carrier IQ* at 40. Facebook, however, fails to identify the relevant ECS provider, and does not say if it is making a vicarious claim. Facebook cites no case in which a defendant successfully invoked a vicarious "ordinary course of its business" exception. *Cf. Google Privacy Policy Litigation* (involved scanning of emails on defendant's own email service); *Kirch v. Embarq*, 702 F.3d 1245 (10th Cir. 2012) (ISP defendant invoked exception based on communications occurring through its own service).

Nor does Facebook claim it is the relevant ECS. Facebook is an ECS provider – but only for communications made on Facebook.com. Facebook nowhere identifies – a fact issue, anyway - the "instrument, equipment, or facility" or "component thereof" that it must show it used as an ECS in the ordinary course of business.

Even if Facebook identified the ECS and the facility necessary to invoke this exception, the non-consensual taking or tracking of electronic information is not within the "ordinary course of business

exception." *See Google Gmail Litigation*, 2013 WL 5423918 at *11 (adopting "narrow reading" of exception, requiring "some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good."). Facebook's interceptions and social-sharing tools are neither necessary for transmission of communications between users and websites nor "incidental" to them. *See Google Gmail Litigation*, 2013 WL 5423918 at *8 (exception limited to ECS provider interceptions that "facilitate[] the transmission of the communication at issue or is incidental to the transmission of such communication").

Facebook's argument fails under *In re Google Privacy Policy*. There the court held that the exception could apply to actions taken by an ECS provider to further its "legitimate business purpose." 2013 WL 6248499 at *11 (N.D. Cal., Dec. 3, 2013). Facebook's systematic violation of its privacy promises is not a "legitimate business purpose." *In re Carrier IQ* at 39 (exception inapplicable where device "has functionality" that was "expressly disclaimed"); *see also Opperman v. Path*, 87 F.Supp.3d 1018, 1061 (N.D. Cal. 2014) (common law intrusion claim; non-consensual taking of electronic information is not "routine commercial behavior.").

Disclosure of Facebook's behavior resulted in a Congressional inquiry (SAC ¶ 112) and an unprecedented 20 years of independent privacy audits. SAC at ¶111. False representations and misconduct punished by the FTC are not within the ordinary course of business exception.

3. The Stored Communications Act

a. Plaintiffs Adequately Alleged Access to a Facility

The Stored Communications Act defines "facility" as the conduits "through which an electronic communication service is provided." 18 U.S.C. 2701(a). An ECS is defined as "*any* service which provides to users thereof the ability to send or receive wire or electronic communications." To find a "facility," a court must first determine the ECS then determine the elements through which the service is provided.

The SAC alleges unauthorized access to three different types of facilities: (1) personal computing devices; (2) web-browsers; and (3) browser-managed files. SAC ¶ 199. Contrary to the Motion, every court to answer the question has found that web-browsers and browser-managed files are protected SCA "facilities."

For example, Microsoft has successfully used the SCA to challenge computer hackers who gain unauthorized access to Internet Explorer and its constituent files located on the personal computing devices of IE users. In *Microsoft v. Does 1-8*, the defendants circumvented IE's privacy settings to take information directly from IE users without consent. The court concluded, in unequivocal terms, "Microsoft's … Windows operating system and Internet Explorer software are facilities through which electronic communication services are provided." *Microsoft v. Does 1-8*, 14-cv-00811-LO-IDD (E.D. Va. July 20, 2015). Plaintiffs know of no SCA case involving web-browsers that Microsoft has lost. *See also Microsoft v. Does 1-27*, 10-cv-00156 (E.D. Va. 2010); *Microsoft v. Piatti*, 11-cv-01017 (E.D. Va. 2011); *Microsoft v. Does 1-39*, 12-cv-1335 (E.D. N.Y. 2012); *Microsoft v. Does 1-18*, 13-cv-139 (E.D. Va. 2013); *Microsoft v. Does 1-82*, 13-cv-00319 (W.D. N.C. 2013). These Microsoft cases get it right. *Accord, Chance v. Avenue A*, 165 F.Supp.2d 1153, 1160 (W.D. Wash. 2001); *Ehling v. Monmouth*, 961 F.Supp.2d 659, 667 (D. N.J. 2013); *Crispin v. Audigier*, 717 F.Supp.2d 965 (C.D. Cal. 2010); *Freedman v. AOL*, 325 F.Supp.2d 638 (E.D. Va. 2004); *Councilman I*, 418 F.3d at 77 ("Congress sought to ensure that the messages and by-product files that are left behind after transmission, as well as messages stored in a user's mailbox, are protected from unauthorized access. Email messages in the sender's and recipient's computers could be accessed by electronically 'breaking into' those computers and retrieving the files.").

Understanding the SCA's purpose is necessary to parse the distinction between the web-browser and email cases and the mixed case law on personal computing devices. Congress enacted the SCA "because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address." *Quon v. Arch Wireless*, 529 F.3d 892, 900 (9th Cir. 2008). Congress wished to protect electronic communications "subject to control by a third-party computer operator[.]" *See* Senate Report 99-541 at 3, Grygiel Dec. Ex. 2. Likewise, in *Riley v. California* (discussed in more detail below), the U.S. Supreme Court unanimously held that data contained on a personal computing device is protected by the Fourth Amendment, reasoning "[a]n Internet search and browsing history … could reveal an individual's private interests or concerns[.]" 134 S. Ct. 2473, 2490 (2014). *Riley* is a good step in the direction of privacy protection, as it closed the front door to secret seizure of such data. But the back door remains open unless the SCA applies.

Further, if web-browsers are not protected by the SCA, *Riley v. California* means nothing in the real world. First, rather than attempt to access communications directly through a person's computer or cell phone, the government need only serve a subpoena on the person's web-browsing company requiring the company to access the files to which it has access rights. Second, a web-browsing company could give government agents the authority to search a user's files contained within the browser to which the web-browsing company maintains the right to access. *See United States v. Matlock*, 415 U.S. 164, n. 7 (1974) ("Common authority" rest on "mutual use of the property by persons generally having joint access or control for most purposes[.]"). This is because a web-browser user does not "own" the browser or its files but only enjoys a "license" to use them subject to conditions which allow the web-browsing company to access the same files, under Facebook's argument. Finally, a web-browser licensor could disclose the contents of its user's Internet communications to any third-party without user consent. Viewed in its proper context, therefore, Facebook's position violates the basic rule of avoiding statutory interpretations that lead to absurd results. *See Los Coyotes Band of Cahuilla and Cupeno Indians v. Jewell*, 729 F. 3d 1025, 1036 (9th Cir. 2013)

b. *Plaintiffs Adequately Alleged Storage*.

The SCA defines "electronic storage" as (A) "any temporary, intermediate storage of a[n] … electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an [ECS] for purposes of backup protection of such communication." Plaintiffs allege Facebook gained access to the content of communications in cookies and referer URLs stored in browser-managed files, including: (1) URL requests present in the toolbar while a user remains present at a particular webpage; and (2) browsing history maintained by the web-browser ECS for purposes of back-up protection.

The definitions of storage are "extraordinary – indeed, almost breathtakingly – broad." *See Councilman I* at 73 (citing *U.S. v. Councilman*, 245 F.Supp.2d 319, 320 (D. Mass. 2013)) (Congress intended to protect "[e]mail messages in the sender's and the recipient's computers" which "could be accessed by electronically 'breaking into those computers[.]") Though this is a web-browser case, the concept is the same regarding the URLs stored in the plaintiffs' toolbar.

Defendant's argument that a URL stored in a user's toolbar is not stored "in the middle of a transmission" (MTD at 20) is a factual, and stretched, argument. The contents of these communications, including all information after the .com, enter storage in the toolbar "once a user hits Enter or clicks on a link [and] the communication is *in the process* of being sent and received between the user and the first-party website." SAC ¶ 206. The web-browser stores a copy of the user's URL requests in the toolbar for only so long as "the user remains present at a particular webpage." *Id*. When users send their next communication, the stored communication is removed from the toolbar. As pleaded in the SAC, this is the everyday experience of millions of American Internet users including the plaintiffs.

Storage in browsing history also satisfies the second part of the definition because the storage is for "purposes of backup protection," which the Ninth Circuit has held applies to backup protection for the user's benefit. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004).

c. Plaintiffs Alleged Facebook "Accessed" Facilities.

The SCA does not separately define "access." The common definition of access is not limited to physically entering a protected facility, but instead to "obtain" information from it or make use of it. *See Segan LLC v. Zynga*, 2015 WL 5315945 (N.D. Cal. Sept. 10, 2015) (patent case). The Oxford dictionary defines "access" to include "the opportunity to use or benefit from something" or to "obtain, examine, or retrieve."[5] In the computer context, Webopedia defines access as "to use."[6] The Computer Desktop Encyclopedia defines access as, among other things, "in computer security, the opportunity for use of a resource."[7] The ECPA's legislative history shows Congress intended access to have a broad meaning. *See* Senate Report 99-541 at 38-39, Grygiel Decl. Ex. 2 (Discussing §2703(c) and (d) as providing for "access to records or other information pertaining to a subscriber" and providing for "orders requiring access by a Government entity to the contents of an electronic communication," effectively making access synonymous in the ECPA with the obtaining of information).

[5] http://www.oxforddictionaries.com/us/definition/american_english/access

[6] http://www.webopedia.com/sgsearch/results?cx=partner-pub-8768004398756183%3A6766915980&cof=FORID%3A10&ie=UTF-8&q=access

[7] http://www.yourdictionary.com/access#computer

Facebook's behavior fits all of these definitions. Furthermore, contrary to Facebook's argument, plaintiffs' interpretation would not lead to liability for "any third-party provider of webpage content that receives referer URL information" just because they received the communication.[8] If a browser communicates a referer URL to a third-party, that normal functioning is not an interception or an unlawful access of a facility, because it is impliedly consensual. *In re Doubleclick*, 154 F.Supp.2d 497 (S.D.N.Y. 2001). Facebook, however, acquired content without any consent, and the general rule articulated in *Doubleclick* does not apply. The only third parties facing liability under plaintiffs' theory are those who circumvent privacy settings on browsers or those who misrepresent the nature of the cookies being written to the browser – in other words, those parties who cannot claim implied consent.

C. Plaintiffs Have Adequately Pled California Law Claims

1. The California Invasion of Privacy Act ("CIPA")

a. CIPA § 631

A claim under Section 631 mirrors the ECPA with two relevant differences.[9] First, CIPA is an all-party consent statute. Even if Facebook prevails on its theory that the relevant communication is the GET request sent to Facebook, and Facebook is a "party" to the intercepted referer URLs (making it the "one party" consenting to the communication), it cannot demonstrate that the plaintiffs consented. Lacking all-party consent, the CIPA could provide a basis for liability even where the Wiretap Act would not. Furthermore, all parties Additional, Facebook is a third-party.[10] But it is not a "content" provider.

Second, CIPA does not require the use of a "device." Facebook argues that the relevant requirement is instead a "machine, instrument, or contrivance," see Motion at 16, but this argument selectively edits the statute. CIPA's actual text prohibits interceptions "by means of any machine, instrument, or contrivance, *or in any other manner*." Plaintiffs adequately alleged seven instruments or contrivances as detailed in their federal Wiretap section. *See* SAC ¶ 217. Even if these facts do not

[8] Facebook here concedes it is a third-party.

[9] Plaintiffs restate their arguments on "content" and "consent" from the federal Wiretap Act.

[10] Facebook again concedes it is not a party to communications between users and websites.

technically qualify as a "machine, instrument or contrivance," Facebook has ignored the portion of the statute allowing "any other manner."

b. CIPA § 632

Section 632 forbids recording a conversation where "a party to [the] conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002). As Facebook notes, California courts have held that Internet communications are not confidential in some circumstances. However, plaintiffs know of no case holding that an Internet communication is not confidential for purposes of Section 632 when the recording entity explicitly promised the actual parties to the communication that the conversation would not be recorded.[11] Facebook explicitly promised not to record the communications at issue creating the privacy expectation. "When you log out of Facebook, we remove the cookies that identify your particular account." SAC ¶ 23. Even after Facebook was caught, its Engineering Director said, "We've said that we don't do it, and *we couldn't do it without some form of consent and disclosure*." SAC ¶ 27. *See also* SAC ¶74-78; SAC ¶107.

Facebook cites the Court's prior holding that "Internet users have no expectation of privacy in the … IP addresses of the websites they visit," Motion at 18, but this holding is irrelevant to the Section 632 analysis. As alleged in the SAC, Facebook intercepted detailed URLs in addition to simple IP addresses. *See* SAC ¶ 35; *see also In re Application for Pen Register*, 396 F.Supp.2d at 49-50; *U.S. v. Forrester*, 512 F.3d at n. 6 (URLs, unlike IP addresses, "reveal[] much more information" about user's Internet activity, including articles viewed); *Google Cookie Placement*, 806 F.3d at 138 (citing *Forrester*). Even if the SAC only alleged interceptions of IP addresses (which is not the case), even IP addresses can be the subject of objectively reasonable expectations of privacy in the context of a Section 632 claim. As *Forrester* noted, the government must obtain a court order even if only tracking the IP addresses to and from which a person is communicating.

Plaintiffs also adequately alleged the use of a recording device - the same devices used to intercept their communications. SAC ¶ 217. Facebook cites an inapposite pre-Internet case – and fails to

[11] Defendant is not a party to any of the communication between the plaintiffs and the websites. By its own admissions, it is a third-party. Regardless of whether the Court deems Facebook a party, it is liable under Section 632.

cite any case supporting its position that the devices it uses to record its users' Internet communications while logged-off fail to qualify. *See* SAC ¶ 48-52 regarding recording of information in [redacted] database and third-party cookies "designed to track *and record* an individual Internet user's communications." *See also In re Google Inc. Gmail Litig*, 2013 WL 5423918 at *21 (California Supreme Court has repeatedly interpreted CIPA broadly and "regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme"); *People v. Nakai*, 183 Cal. App. 4th 499, 518 (Cal. App. 2010) (computer "screenshots … fall within the ambit of a recording device."). The devices, instruments, contrivances, and scheme used by Facebook to record its user's communications fit the statutory scheme.

2. Invasion of Privacy and Intrusion Upon Seclusion

a. *Invasion of Privacy*

Enshrined in the state Constitution, the California tort of invasion of privacy has three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) the intrusion must be so serious as to constitute an egregious breach of social norms. *Hill v. NCAA*, 7 Cal.4th 1 (1994). The plaintiffs allege facts to support all three elements. Without consent, Facebook intercepted billions of URLs appended to cookies that provided user identity (*c_user, fr, lu*), time and date (*act*), location (*locale*) and other personal information. By associating multiple URLs with the same user, a comprehensive picture of each subscriber's personal life can be assembled with frightening detail, based on data that Facebook was not authorized to receive. In short, there is a reasonable expectation of privacy in *aggregate* web browsing history, even if not in any single URL.

The first court to address whether this wholesale surveillance of the Internet gives rise to a claim for the tort of invasion of privacy was the California Superior Court, in *Ung v. Facebook, Inc.*, No. 12-CV-217244, Order (Cal Super. Ct. Santa Clara Cnty July 2, 2012), attached to the SAC as exhibit HH. Yes, the Court found, "there is a legally protected privacy interest in a person's identifiable browsing history," slip op. at 3, and using cookies to "track large portions of people's browsing histories across numerous other websites . . . constitutes a serious invasion of a privacy interest." *Id*. at 5.[12]

[12] Facebook may be collaterally estopped from challenging the *Ung* court's factual ruling regarding invasion of privacy. Though the decision was a denial of a demurer, Facebook opted not to seek interlocutory appeal. "Once an issue has been resolved in a prior proceeding, there is no further fact

Every other court since *Ung* has reached the same conclusion. The Court of First Instance in Belgium found that using Facebook's browser-specific *datr* cookie to track web browsing (even without evidence that *datrs* could be linked to actual users) violated "fundamental rights and freedoms." SAC, Ex. EE. In *Google Cookie Placement,* which this Court found to be factually "virtually indistinguishable," the Third Circuit held that even sophisticated internet users can "reasonably expect" that URL queries would not be associated with each other without consent. *Google Cookie Placement,* 806 F.3d at 151. The Third Circuit specifically found that Google's aggregation of the URLs "intrud[ed] upon reasonable expectations of privacy" and allowed the California tort to proceed. *Id*. The Third Circuit also found Google's conduct to "constitute an egregious breach of social norms," *id*., conduct which is nearly identical to that alleged here, in particular with respect to the IE Subclass. Finally the French data protection authority (CNIL) recently followed the decision of the Belgian Court of First Instance, finding Facebook's use of the *datr* cookie to track web browsing to be neither fair nor lawful without consent. *See* Grygiel Decl. Exs. 4 and 5.

Supreme Court Fourth Amendment jurisprudence mirrors these decisions and reflects the growing and reasonable public desire to be free from electronic surveillance. *See, e.g., United States v. Jones*, 132 S. Ct. 945, 955 (2012) (prolonged electronic location monitoring by government, even in public spaces, violates reasonable privacy expectations). The Supreme Court repeated this logic in unanimously deciding *Riley v. California*, 134 S. Ct. 2473, 2490 (2014), finding a legitimate privacy interest in aggregated electronic data on a smart phone (including Internet history) even if any individual item of data may not give rise to a legitimate interest. In the same way, internet users have a reasonable expectation of privacy in the pervasive aggregation of web histories, even if they do not in a single URL.

Considering *Jones* and *Riley*, Judge Koh recently observed that "Justice Sotomayor was particularly concerned with "the existence of a reasonable societal expectation of privacy in the *sum* of one's public movements." *In re Application for Telephone Information*, 2015 WL 4594558 at * 8 (N.D.

finding function to be performed" in future cases. *Murray v. Alaska Airlines, Inc*., 50 Cal. 4th 860, 864 (2010). The Restatement (Second) of Judgments §27 cmt. d suggests the denial of a demurer might be "final" for purposes of collateral estoppel because "an issue . . . submitted and determined on a motion to dismiss for failure to state a claim" is a final judgment. This is true even if determination is "based on a failure of pleading or of proof as well as on the sustaining of the burden of proof." *Id*.

Cal., July 29, 2015) (quoting *Jones*) (emphasis added by Judge Koh). She further observed that *Riley* also focused on the new technological ability to aggregate personal data, *id*. at *9, and concluded: "Based on the preceding U.S. Supreme Court cases, the following principles are manifest: (1) an individual's expectation of privacy is at its pinnacle when government surveillance intrudes on the home; (2) long-term government surveillance by the government implicates an individual's expectation of privacy; and (3) location data . . . can reveal a wealth of private information about an individual." *Id*. She then concluded that cell phone users have a legitimate expectation of privacy in the aggregate collection of cell phone location data, even if there would not be in a single data point. "Such an expectation is one that society is willing to recognize as reasonable." *Id*.

In its Motion, however, Facebook ignores the tectonic jurisprudential shifts above and argues as if the technological advances discussed above had never happened. Thus, Facebook relegates *Ung* to a footnote and brushes it off as "wrongly decided" without offering any analysis. Facebook also never mentions *Google Cookie Placement* and never mentions the recent decisions in Europe finding that pervasive web tracking via the *datr* cookie violates fundamental freedoms absent consent. Facebook also never mentions *Jones*, and disregards as mere *dicta* the Supreme Court's ruling in *Riley.*

b. *Intrusion Upon Seclusion*

The California tort of "intrusion upon seclusion" is similar to but distinct from the tort of invasion of privacy and both are cognizable separately on the same facts. *See, e.g., Google Cookie Placement,* 806 F.3d at 151. Specifically, unauthorized taking of electronic information can give rise to an action for intrusion upon seclusion. *Id*. (unauthorized taking of personal Internet communications under California law); *Opperman,* 87 F.Supp.3d at 1058-61 (unauthorized taking of personal contact lists under California law).

i. Facebook Intruded Upon a Private Matter

A plaintiff must plead the defendant intruded into "some zone of …privacy surrounding, or obtained unwanted access to data about the plaintiff . . . [and] an objectively reasonable expectation" of privacy in "the place, conversation or data source." *Shulman v. Group W. Productions, Inc.*, 18 Cal. 4th 200, 232 (1998). Facebook obtained unauthorized access to Plaintiffs' computers and Internet communications by (1) tracking users' communications while they were logged-off of Facebook in

violation of Facebook's own privacy policy and public promises; and (2) circumventing users' privacy settings on Internet Explorer. Plaintiffs' SAC pleads "an objectively reasonable expectation of [privacy] in the place, conversation or data source." *Id.* at 232. This objectively reasonable expectation was created (1) by Facebook when it explicitly promised not to track its users while they were logged-off; and (2) by state and federal statutes, in particular, the Wiretap Act, Stored Communications Act, CIPA, Pen Register Act, and other statutes plead in plaintiff's petition. *See* SAC ¶ 17-27, 225. Plaintiffs also had an objectively reasonable expectation of privacy that Facebook would not circumvent the chosen privacy settings on plaintiffs' web-browsers. *Cf. Kewanee Oil v. Bicron*, 416 U.S. 470, 487 (1974) ("A most fundamental human right, that of privacy, is threatened when industrial espionage is condoned or is made profitable; the state interest in denying profit to such illegal ventures is unchallengeable.").

ii. A Reasonable Person Could Find Facebook's Behavior Highly Offensive

"Highly offensive" is a mixed question of law and fact. *Hill* at 40. It is ultimately a jury question unless a court determines that "as a matter of policy, such conduct should be considered, as a matter of law, not highly offensive." *Taus v. Loftus*, 151 P.3d 1185 (Cal. 2007). Congress and every state has already made this policy decision by enacting criminal statutes against conduct like Facebook's that is inherently highly offensive or would not be punishable by incarceration -- violations of the Wiretap Act, Pen Register Act, Stored Communications Act, CIPA, California Computer Crime Law and Cal. Penal Code §§ 484, 496, 631 and 632 are each subject to prison terms. *See, e.g.* 18 U.S.C. § 2511(4)(a); 18 U.S.C. § 2701(b); and 18 U.S.C. § 1030(2)(B). California explicitly declared that activities such as the SAC alleges are "serious threat[s] to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Crim. Code § 630. California's Supreme Court has held that "eavesdropping [or] wiretapping" gives rise to the tort of intrusion upon seclusion. *Shulman* at 868.

Even if Facebook technically violated no law, its conduct would still be highly offensive. Determining offensiveness requires consideration of all circumstances of the intrusion, including the degree, setting, and intruder's motives and objectives. *Miller v. National Broadcasting Co.*, 187

Cal.App.3d 1463, 1483-84 (Ct. App. 1986); *Hernandez v. Hillsides, Inc*., 47 Cal. 4th 272 (Cal. 2009). Facebook's unauthorized intrusion involved the plaintiffs' home computers and personal computing devices. The Supreme Court has repeatedly emphasized the importance of privacy in a person's home, computer, and web-browsing history. *See e.g., U.S. v. Jones*, 132 S. Ct. 945 (2012); *Riley v. California*, 134 S. Ct. 2473 (2014). The degree and circumstances of the intrusion was so widespread and pervasive that Facebook agreed to 20 years of independent privacy audits. SAC ¶ 111. Facebook's motive and objective of Facebook's conduct was Facebook's own financial gain at the expense of the privacy interests of its millions of users, which is not enough to overcome its surreptitious theft of the plaintiffs' personal information. *Opperman*, 87 F.Supp.3d at 1061 ("surreptitious theft of personal contact information … has [not] come to [be] qualified as 'routine commercial behavior'").

3. California Statutory Larceny

a. The SAC Properly Alleges Claims for Statutory Larceny

The California Penal Code states that persons who defraud other persons of personal property by false pretense are guilty of theft. Cal. Penal Code § 484(a). Cal. Penal Code § 496(c) provides a private right of action for "[a]ny person who has been injured" by the sale of stolen property. Cal. Penal Code § 496(c). Thus, regardless of plaintiffs' entitlement to a cause of action under § 484, due to the incorporation of theft by false pretense by § 496, plaintiffs have alleged a claim for theft by false pretense.

b. Personally Identifying Information is Property

Defendants cite *In re Zynga Privacy Litig.*, 2011 WL 7479170 (N.D. Cal. June 15, 2011) and *Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010, 1026 (N.D. Cal. 2012) (cases involving the California Unfair Competition Law) in arguing PII is not "property" subject to Penal Code 496. *See* Motion at 39. However, Section 496 does not define "property" and California courts have stated that anything that can be stolen can be property under § 496. *People v. Norwood*, 26 Cal.App.3d 148, 157 (App. 2 Dist. 1972). California has specifically recognized that one's personal identifying information ("PII") can be the object of theft, and criminalizes the unauthorized use of same. *See CTC Real Estate Services v. Lepe*, 140 Cal.App.4th 856 (App. 2 Dist. 2006) (citing Cal. Penal Code § 530.5).

For the purposes of Chapter 8 (False Personation and Cheats) of Title 13 (Of Crimes Against Property), the Penal Code defines "personal identifying information" as including, *inter alia*, any names,

addresses, personal identification numbers or passwords, unique electronic data, including information identification numbers assigned to persons or addresses, and telecommunications identifying information or access devices. Cal. Penal Code § 530.55(b). Much of the aforementioned information was contained in the information Facebook collected from the plaintiffs as alleged in the SAC, and furthermore, the list of PII set forth in § 530.55 ends with "or an equivalent form of identification." *Id.*

Courts have explained that the word "property" signifies "something that one has the exclusive right to possess and use." *People v. Kwok*, 63 Cal.App.4th 1236, 1250–51 (App. 1 Dist. 1998) (interpreting Cal. Civil Code § 654). Making unauthorized copies, whether of physical objects, trade secrets, or computer data, is, then, theft. *Kwok*, 63 Cal. App.4th at 1251 (referencing Cal. Penal Code §§ 499c(b)(3) and 502(c)(2)); *see People v. Gopal*, 171 Cal.App.3d 524 (App. 1 Dist. 1985) (trade secrets were property under § 496). Such actions destroy "the intangible benefit and prerogative" of being able to control access to such property. *Id.* Plaintiffs had the exclusive right to possess and use their PII, including their respective browsing histories. Facebook interfered with this right. Plaintiffs' information is property and Facebook's actions constituted theft under the California Penal Code.

c. Plaintiffs Have Sufficiently Alleged Theft by False Pretenses

Echoing its "party to the communication" argument, Facebook claims that because it received the information at issue "directly from Plaintiffs," it was not stolen. Motion at 39. But the SAC alleges that, when users logged into Facebook, various session cookies and tracking cookies were written to their browsers. SAC ¶ 3. When the users' browsers sent referer URLs to Facebook, they were appended to user-identifying data without the users' consent, which fundamentally changes the nature of the communication. Plaintiffs, simply put, sent the URLs under false pretenses.

Incredibly, Facebook claims it "had no reason to believe the information was stolen, nor was it." Motion at 39. But this factual defense is not only inappropriate at the 12(b)(6) stage, [redacted]. Not only did Facebook track and transmit plaintiffs' data to itself without plaintiffs' knowledge or consent, it represented to plaintiffs that it was not doing so. SAC ¶¶ 23–25, 63, 85, 102. No inference is reasonable other than Facebook intended these representations to induce plaintiffs to use its website and to allow Facebook to continually collect valuable personal user information. SAC ¶ 227-f, 263–266, 278. In

choosing to contract with and use Facebook, plaintiffs relied on Facebook's false representations. SAC ¶ 267.[13] Plaintiffs' reliance can also be inferred from all of the circumstances. *Harris v. Garcia*, 734 F.Supp.2d 973, 989 (N.D. Cal. 2010) (citing *People v. Wooten*, 44 Cal.App.4th 1834, 1843 (1996).

d. The Facts do not Preclude a Claim for Theft by False Pretenses

Facebook argues that it cannot have stolen plaintiffs' property because plaintiffs' browsers sent "GET" requests to Facebook "as part of the Internet's normal operation." Motion at 39. A browser's sending a GET request to a website in order to view its content is part of the Internet's normal operation. But a website's surreptitious installation of cookies on their browsers in order, post-log out, to collect personal information, is not.

Facebook further elides the point in arguing it neither purchased plaintiffs' property nor received it from a third party. Liability, however, attaches from Facebook's extraction of plaintiffs' property without their knowledge or consent, and without compensation.

Facebook then argues that because Facebook did not actually conceal or withhold plaintiffs' browsing histories from them, plaintiffs have no Sec. 496 claim. However, Section 496 more broadly reaches not only to persons who conceal or withhold property, but also those who *sell* property, and those who "aid[] in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained." Cal. Penal Code. § 496(a). But the facts alleged in the SAC show Facebook cannot disclaim knowledge of the non-consensual manner in which plaintiffs' personal information was acquired. Facebook did sell its users' personal information because it charged more to advertisers based on this very information.

4. Breach of Contract and Implied Covenant of Good Faith and Fair Dealing

As the SAC alleges, Facebook breached its contractual promises (both explicit and implicit) not to track the web browsing of subscribers who had logged out. Facebook makes three argument in its Motion to dismiss the breach of contract claim: (1) Facebook is not contractually bound by its own Privacy Policy nor referenced Help Pages; (2) no damages; and (3) no allegations of plaintiffs'

[13] Contrary to Facebook's assertion that Plaintiffs have not properly pled the elements of theft by false pretenses, all of the foregoing information in this paragraph was incorporated into Count XI of the SAC. *See* SAC ¶ 286.

performance. Facebook makes these same arguments with respect to the implied covenant of good faith and fair dealing, and also argues that the claim is merely duplicative of the contract claim.

a. The Privacy Policy and Help Center Pages Are a Part of the SRR

Facebook remarkably posits that it is not contractually bound by its own Privacy Policy or Data Use Policy, merely because the SAC "never identifies any section in the SRR that contained hyperlinks" to the specifically relevant portions of the other documents. Motion at 34. However, under California law, contracts can incorporate other documents by reference without hyperlinks or mentioning specific provisions. So says the very case Facebook cites, *Chan v. Drexel Burnham Lambert, Inc.*, 178 Cal.App.3d 632, 641 (1986). In *Chan*, a contract failed to incorporate a second document because the second document was never identified; the contract simply included a term that required a signatory to abide by unspecified other contracts governing membership in unspecified other organizations. The *Chan* court distinguished that term from other contracts that "clearly referred to and identified the incorporated documents." *Id*. (citing *King v. Larsen Realty, Inc.*, 121 Cal.Ap.3d 349 (1981)); s*ee also Baker v. Aubry*, 216 Cal.App.3d 1259, 1264 (1989) ("The distinguishing factor in *King*, found lacking in *Chan*, was the fact that the incorporated document was readily available to the appellants.").

Here, the SRR clearly identifies and incorporates the Privacy Policy (and later Data Use Policy), and the Privacy Policy clearly identifies and incorporates the Help Center pages,[14] constituting the "layered approach" that Facebook represented to Congress. SAC ¶¶ 21-23. Indeed, the very first term of the SRR is called "Privacy" and Facebook represents that the Privacy Policy makes "important disclosures about . . . how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions." SAC, Ex. A. The Privacy Policy, in turn, repeatedly references the SRR and even represents that the terms of the Privacy Policy may be changed pursuant to the SRR, and that the Privacy Policy "applies to all information we have about you." It then contains links to the Help Pages. SAC, Ex. G, ¶ 9.

[14] Facebook objects that copies of certain cited Help Center pages were not appended to the SAC. However, plaintiffs requested these pages during discovery almost two years ago and Facebook has refused to produce them. The parties are currently negotiating this point.

Other courts addressing this issue have implicitly found the Facebook SRR to incorporate the Privacy Policy. Thus, for example, the breach of contract claim in *In re Facebook Privacy Litigation* was premised on a contract consisting of both documents, *see* 791 F. Supp. 2d 705, 717 (N.D. Cal. 2011), and the Ninth Circuit later held that the complaint adequately pled breach of contract. *See* 572 Fed. Appx. 494 (9th Cir. 2014).[15] While Facebook also argues it is not contractually bound by the Privacy Policy, it routinely claims that subscribers are. So for example, in *Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090 (N.D. Cal. 2011), Facebook argued that subscribers consented to sharing names and pictures based on the terms of the Privacy Policy. *Id*. at 1095; *see also Campbell v. Facebook, Inc*., 77 F. Supp. 3d 836, 846 (N.D. Cal. 2014) ("Facebook points to its 'Statement of Rights and Responsibilities' and its 'Data Use Policy,' *both of which must be agreed to by users in order to use the Facebook website*" (emphasis added)).

b. Damages

The issue of contractual damages is addressed above in the "Standing" section, and include loss of computer resources caused by the presence of the unauthorized cookies as well as loss of privacy. The Ninth Circuit ruled that a complaint adequately pleads contract damages under California law on almost identical facts. *In re Facebook Privacy Litig.*, 572 Fed. Appx. at 494.

c. Alleging Performance

In the SAC, plaintiffs alleged that they accepted the terms of the contract with Facebook, SAC ¶ 247, and had active Facebook accounts during the entire class period. SAC ¶¶ 12-15. These allegations are sufficient to generally allege their performance under the contract. Facebook, however argues in the Motion that plaintiffs are required to allege that they did not breach negative obligations, i.e., provisions of the SRR forbidding certain behavior. The only case cited by Facebook, however, does not support this expansive view of notice pleading. In *Bennett-wofford v. Bayview Loan Servicing, LLC*, 2015 WL 8527333 (N.D. Cal. Dec. 11, 2015), plaintiffs alleged a breach of a contract to settle a case, a contract which required the plaintiff to perform many things, including dismissing a complaint. *Id*. at *6. But a review of the contact also reveals that plaintiffs had other ancillary contractual obligations, including

[15] Because the Ninth Circuit decision is "final," it is possible that Facebook is now collaterally estopped from arguing that its SRR does not incorporate the Privacy Policy by reference.

agreeing that they had no intention to bring suit against a number of persons, and knew of no facts constituting a basis for suit; they also agreed to cooperate and use best efforts, and also represented that each had the authority to sign the contract. Nevertheless, the court found the following sentence sufficient to plead performance: "The case was dismissed on March 11, 2013." *Id.*

d. Breach of Implied Covenant

In California, all contracts contain an implied term of good faith and fair dealing. *Careau & Co. v. Security Pacific Business Credit, Inc.*, 22 Cal. App.3d 1371, 1395 (1990). Facebook objects that plaintiffs' claim here is merely duplicative of the breach of contract claim, but plaintiffs' claim is brought in the alternative to the extent the promises made in the Help Pages or Privacy Policy are deemed not to be contractually binding on Facebook. If these documents are contractually binding, Facebook had a contractual duty to expire cookies each time a subscriber logged out. Failure to do so is a breach of contract, and the breach of the implied covenant is superfluous. If, however, Facebook's Privacy Policy is deemed not to be contractually binding, Facebook's actions – alleged in the SAC to be done knowingly and bad faith – violate the implied covenant which would not be duplicative of the excluded Privacy Policy terms.

5. California Penal Code 502

The California's Comprehensive Computer Data Access and Fraud Act protects persons from unauthorized access to their computers, Cal. Penal Code § 502. Pursuant to section 502(e)(1), individuals have a private right of action against persons causing them damage by reason of a violation of any one of eight subsections 502(c); plaintiffs alleged violations of four subsections.

a. Damage

No statutory minimum amount of damage is required for a section 502 claim, and Facebook cites to none. The prevailing view is that "any amount of loss may be sufficient" under the statute. *In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236 at *11 (N.D. Cal. Mar. 26, 2013). Facebook failed to expire certain cookies upon logout, [redacted]. Facebook's actions resulted in larger amounts of data being sent to Facebook's servers each and every time a subscriber communicated with Facebook-enabled websites. The amount of this unauthorized extra data –stored and repeatedly transmitted throughout the day – is robust. *See* SAC ¶¶

58-60. Appending user-identifying cookies to billions of URLs allows Facebook to associate multiple URLs with an actual person, painting a comprehensive picture of that person's life, intruding upon a reasonable expectation of privacy. This is injury under California law as discussed above and thus satisfies "damage" under section 502.

b. Permission

All relevant subsections of section 502(c) require that the defendant act "without permission." Courts routinely interpret "without permission" to mean "in a manner that circumvents technical or code-based barriers in place to restrict or bar a user's access." *Opperman*, 87 F.Supp.3d at 1053. Plaintiffs' section 502 claim is therefore limited the IE Subclass. But as Facebook concedes (*see* Motion at 27, fn. 15), the SAC alleges that Facebook circumvented the cookie blocking technology used by the IE Subclass without permission. *See Google Cookie Placement*, 806 F.3d at 151 (Google circumvented cookie blockers on browsers). Facebook argues that it disclosed the use of cookies generally, Motion at 27, fn. 15 ("the Privacy Policy informed users that Facebook used these cookies"), but the Third Circuit rejected Google's similar argument ("Google's emphasis on tracking and disclosure amounts to a smokescreen") because the browser was only accessed after Google circumvented cookie blockers. *Google Cookie Placement*, 806 F.3d. at 150.

c. Contaminant

The statute defines computer contaminants to include (but are not limited to) "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." Section 502(b)(10). As alleged in the SAC, cookies fit this definition. Self-replicating, they copy themselves to each and every referrer URL sent to Facebook, potentially hundreds of times a day for any subscriber, contaminating an otherwise anonymous referrer URL with user identification. And they consume computer resources, both by occupying computer storage and by increasing the size of communications sent to Facebook's servers.

6. Fraud

To state an action for fraud, a plaintiff must plead with specificity an intentional misrepresentation of material fact with knowledge of its falsity and intent to induce reliance, actual

reliance, and damages proximately caused by the reliance. *Gonsalves v. Hodgson*, 38 Cal.2d 91, 100-102 (Cal. 1951). Plaintiffs' actual and constructive fraud claims satisfy Rule 9(b)'s specificity requirement. Plaintiffs allege the "who" – Facebook and its employees and engineers, many by name. Plaintiffs allege the "what" – surreptitious post-log out tracking contrary to Facebook's promise. Plaintiffs allege the "when" – during the class period (and during the IE Subclass period), prior to public discovery of Facebook's deceit. Plaintiffs allege the "where" – in the interactions between plaintiffs' computers, third-party websites and Facebook's servers. Plaintiffs allege the "how" – through specifically identified, improperly planted cookies. Having falsely promised to delete user-identifying tracking cookies from browsers after logout, Facebook was duty bound to make, and did not, a corrective disclosure.

Facebook does not deny that the SAC alleges all of the elements necessary to establish fraud; instead, Facebook argues in the Motion that the elements were not *sufficiently* pled. First, Facebook's fraud was intentional – Facebook cites *Engalla v. Permanente*, 15 Cal. 4th 951, 976 (1997),[16] in arguing that "[f]raud requires intent to induce, not just knowledge of falsity." Motion at 22. Fraud's elements are not at issue. The facts are. Plaintiffs allege facts showing Facebook's intent to deceive – which must be taken as true on this dismissal motion. Facebook's arguments from other cases with fully developed factual records cannot defeat those facts – which allege Facebook making a false promise and knowingly breaking it. *See* SAC ¶¶ 4, 23-27, 63, 66, and 68-73.

Facebook's engineering director [redacted] SAC ¶ 74. And Facebook [redacted]. *See* SAC ¶ 78 ("[redacted] Were more needed, Facebook's effort to patent its post-log out tracking method confirms inftent. *See* SAC ¶¶ 79-84. Further confirming Facebook's intent, when caught, Facebook blamed post-log out tracking on "a bug." SAC ¶ 105. But Facebook's internal emails [redacted]. *See also* SAC ¶¶ 75-76.

[16] *Engalla* also involved a well-developed factual record of twelve depositions and thirteen motions demonstrating the fraudulent inducement that invalidated an arbitration agreement. *Engalla*, 15 Cal. 4th at 914. Even without depositions plaintiffs have pleaded facts demonstrating Facebook's fraud.

Facebook's assertion that the "SAC fails to allege that Facebook intended to induce reliance or conduct," Memo at 23, simply cannot be squared with the SAC's factual allegations that (a) Facebook wanted to track users; (b) logged out users posed an obstacle to that desire; and (c) Facebook developed a way of tracking logged out users (d) all the while internally admitting that Facebook's public promises were to the contrary. These are not "bare allegations" of concealment. Besides, although intent can be alleged generally (Fed. R. Civ. P. 9(b)), Plaintiffs allege facts showing intent. *See, e.g.,* SAC ¶¶ 69 ("[redacted]."), 75 ("[redacted]").

Plaintiffs' SAC also specifically pleads Facebook's false promises to not track logged-off users. *See* SAC ¶¶ 4, 23, 24, 27, 74, 78. It also specifically pleads the plaintiffs "relied on Facebook's false assertions in contracting with and using Facebook." SAC ¶ 267. Plaintiffs, relying on Facebook's promises, visited numerous websites while logged out without any inkling that Facebook was tracking their post-log out comings and goings. SAC ¶¶ 5, 115 (Davis), 118 (Quinn), 121 (Lentz), 124 (Vickery).

Facebook's argument about the alleged inspecificity of the reliance allegations ignores the governing law permitting generalized reliance claims. *See Anthony v. Yahoo, Inc.*, 421 F. Supp. 2d 1257, 1264 (N.D. Cal. 2006) (reliance element not required to meet heightened Rule 9(b) standard) *See also Interserve, Inc. v. Fusion Garage PTE, Ltd.*, 2011 WL 500497, at *3 (N.D. Cal. Feb. 9, 2011). Facebook's internal emails also support the reliance element at this stage. *In re Clorox Consumer Litig.*, 894 F. Supp. 2d 1224 (N.D. Cal. Aug. 24, 2012), is instructive. There the court found allegations identifying commercials "upon which the Plaintiffs allegedly relied" and their "contents," when they aired, plus the allegation that plaintiffs purchased in reliance on the advertisements was "detailed information…sufficient to place Clorox on notice of the basis of Plaintiffs' claims and demonstrates that Plaintiffs are not on a fishing expedition." *Id.* at 1234. Just as the *Clorox* defendant was sufficiently apprised of the claims to be able "to locate and produce videos" of the allegedly false commercials, Facebook was able to produce emails corresponding precisely to the fraud Plaintiffs claim. Facebook's claim that no "immediate" causal link exists between Facebook's misrepresentation and Plaintiffs' injurious behavior" (Def. Memo at 24) ignores the totality of facts showing that absent Facebook's falsehood, Plaintiffs "'would not, in all probability, have entered into the contract'" of use

with Facebook. *Clear Solutions, Inc. v. Clear Channel Comm.*, 365 F. 3d 835, 840 (9th Cir. 2004) (reliance on truth of fraudulent statement need not be sole or predominant factor influencing plaintiff's behavior, discussing California law's recognition of "'highly subjective nature of a causation analysis'" and noting cases saying causation is usually a jury question (quoting *Alliance Mortgage Co. v. Rothwell*, 10 Cal. 4th 1226, 1239 (1995)). That argument also ignores the SAC's allegations that plaintiffs never consented to Facebook's tracking (SAC ¶ 125), never changed the default cookie blocking settings that Facebook evaded (SAC ¶ 126), or employed devices to prevent Facebook's post-log out information gathering. SAC ¶ 127.

Plaintiffs have also sufficiently alleged damages (specific and general) proximately resulting from Facebook's fraud.[17] Cause and effect, sufficient for this pleadings stage, is clear. *See Interserve*, 2011 WL 500497, at * 2 (Rule 9(b) purposes do not require heightened damages specificity). Facebook secretly collected, post-log out, plaintiffs' confidential personal information. *See, e.g.*, SAC ¶¶ 113-115, Davis); 116-118 (Quinn); 119-121 (Lentz); 122-124 (Vickery). That information has economic value on its own (*see* SAC ¶¶ 129-143), and is further protected by statutory damages under the ECPA, CIPA, and Cal. Penal Code § 502. No more direct cause-and-effect allegation is necessary, under *Moncada v. West Coast Quartz Corp.*, 221 Cal. App. 4th 768, 776 (2013), or any other case.

Plaintiffs also sufficiently alleged affirmative falsity. Facebook falsely represented its post-logout cookie practices on its Help Center pages, which plaintiffs were directed to by the Privacy Policy. When the public learned of the practice, Congress held hearings and the FTC required two decades of privacy audits. Facebook admitted it lacked consent to track post-logout. Facebook cannot now argue no falsity. Moreover, having made that false statement Facebook concomitantly had "a duty to disclose" the truth of post log-out tracking. If the telling of a "half-truth" triggers a duty to disclose the full truth, Facebook's flat-out lie that it does not track post-log out surely compels corrective disclosure. *See, e.g.*, *Barnes & Noble, Inc. v. LSI Corp.*, 849 F. Supp. 2d 925, 936 (N.D. Cal. 2012) ("where a party volunteers information…'the telling of a half-truth calculated to deceive is fraud'" (citation omitted); *House of Stuart, Inc. v. Whirlpool Corp.*, 33 F. 3d 58, 3 (9th Cir. 1994) (unpub.) ("Absent a fiduciary

[17] Facebook should be precluded from arguing this issue under the doctrine of collateral estoppel based on the Ninth Circuit's ruling in *In re Facebook Privacy Litig.*, 572 Fed. Appx. 494 (9th Cir. 2014).

relationship, a duty to disclose arises only where there are 'special circumstances,' such as when the party in fault creates a false or misleading impression in the first instance." (citation omitted)).

Finally, plaintiffs have also asserted a claim for constructive fraud. For example, in *Dealertrack, Inc. v. Huber*, 460 F. Supp. 2d 1177 (C.D. Cal. 1177) "a confidential relationship was created" when the parties executed a Mutual Confidentiality Agreement for evaluating information concerning a possible business deal. Reaching Facebook's adhesive contract with Plaintiffs, the rule is that "'[a]s a general principle constructive fraud comprises any act, omission, or concealment involving a breach of legal or equitable duty, trust or confidence which results in damage to another even though the conduct is not otherwise fraudulent.'" *Id*. at 1183 (citation omitted). Factors elevating a contractual relationship into a confidential one are present here. *See Portney v. CIBA Vision Corp*., 2008 WL 5505517, at * 5 (C. D. Cal. July 17, 2008). Facebook had superior technological "sophistication and bargaining power" and Plaintiffs' reliance on Facebook's privacy promises were "'so substantial as to give rise to equitable concerns.'" *Id*. (citation omitted). Facebook's other constructive fraud cases are not to the contrary.[18]

7. Trespass to Chattels

"Under California common law, the tort of trespass to chattel encompasses unauthorized access to a computer system where '(1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff.'" *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 980 (N.D. Cal. 2013) (quoting *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069-70 (N.D. Cal. 2000) (further citation omitted)). Plaintiffs adequately allege, among other things, that Facebook placed cookies on their computers post-logout without their consent, allowing Facebook to track their activity without permission and interfering with plaintiffs' use of their computers, and were harmed by the loss of otherwise valuable private information. *See* SAC ¶¶ 129-43, 270-73. Such claim is proper both for the IE Subclass, members of which never consented to any cookies, and by the entire class to the extent Facebook exceeded the scope of consent. *See eBay*, 100 F. Supp. 2d at 1069-70 ("California does recognize a trespass claim where the defendant exceeds the scope of consent").

[18] In addition, whether a confidential relationship exists is generally a fact question, see *Patriot Sci. Corp. v. Korodi*, 504 F. Supp. 2d 952, 966 (S.D. Cal. 2007) and plaintiffs' allegations at minimum generate that question.

Defendant misreads Hamidi, which held a plaintiff need only allege that the defendant's access caused some "actual damage." Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1357 (2003) (citing Prosser & Keeton, Torts (5th ed. 1984), § 15). But damage is defined broadly; "who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial amount of time, or some other legally protected interest of the possessor is affected." Id. at 1351 (quoting Rest. 2d of Torts § 218) (emphasis added). Here, unlike in In re iPhone Application Litigation, 2011 WL 4403963, at *13-14 (N.D. Cal. Sept. 20, 2011), plaintiffs adequately allege "actual damage" under Hamidi, including that the activity affects Plaintiffs' "legally protected interest" in the privacy of their communications and website browsing. Defendant's cookies interfere with the "ordinary and intended operation" of Plaintiffs' computers, including by circumventing various privacy protections (¶¶ 85-101) and tracking Facebook users when the users intended to log out of Facebook and not be tracked (¶¶ 63-84).

What Defendant calls "trivial," LaCourt v. Specific Media, Inc., 2011 WL 1661532, at *7 (C.D. Cal. Apr. 28, 2011), is a question of fact not susceptible for resolution at this stage. See Coupons, Inc. v. Stottlemire, 2008 WL 3245006, at *6 (N.D. Cal. July 2, 2008) (denying motion to dismiss trespass to chattels claim, finding that the defendants' "trivial" interference argument "premature" here there were not enough facts for the court to make a determination). If "other operators of parasitic websites widely replicated the defendants' conduct, the plaintiffs' business and computer operations would surely suffer." Atl. Recording Corp. v. Serrano, 2007 WL 46128921, at * 5 (S.D. Cal. Dec. 28, 2007) (citing Hamidi, 30 Cal. 4th at 1354-57). Defendant's conduct, if condoned, would give other "parasitic" websites reason to replicate similar conduct.

V. CONCLUSION

Plaintiffs request that the Court deny Facebook's Motion and allow discovery to continue.

Dated: February 18, 2016

KIESEL LAW LLP

By: /s/ Paul R. Kiesel
Paul R. Kiesel (SBN 119854)
8648 Wilshire Blvd.
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
kiesel@kiesel-law.com

Interim Liaison Counsel

SILVERMAN, THOMPSON, SLUTKIN & WHITE LLC

By: /s/ Stephen G. Grygiel
Stephen G. Grygiel (admitted pro hac vice)
201 N. Charles St., #2600
Baltimore, MD 21201
Telephone (410) 385-2225
Facsimile: (410) 547-2432
sgrygiel@mdattorney.com

Interim Co-Lead Counsel

KAPLAN, FOX & KILSHEIMER LLP

By: /s/ David A. Straite
Frederic S. Fox (admitted pro hac vice)
David A. Straite (admitted pro hac vice)
850 Third Avenue
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
dstraite@kaplanfox.com

Laurence D. King (206423)
Mario Choi (243409)
350 Sansome Street, 4th Floor
San Francisco, CA 94104
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com

Interim Co-Lead Counsel

ATTESTATION OF E-FILED SIGNATURE

I, David A. Straite, court-appointed interim lead counsel for the proposed Class, am the ECF User whose ID and password are being used to file the foregoing. In compliance with Civil L.R. 5-1(i)(3), I hereby attest that Paul R. Kiesel and Stephen Grygiel have concurred in this filing.

/s/ David A. Straite