United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

In re Facebook Internet Tracking Litigation	Case No. 5:12-md-02314-EJD **ORDER GRANTING DEFENDANT'S MOTION TO DISMISS** Re: Dkt. No. 101

Plaintiffs allege that Defendant Facebook, Inc. violated their privacy by tracking their browsing activity on third-party websites. This Court previously granted Facebook's motion to dismiss, with leave to amend, for lack of standing and failure to state a claim. Plaintiffs filed an amended complaint, and Facebook now moves to dismiss. Facebook's motion will be GRANTED.

I. BACKGROUND

Facebook operates a social networking website.[1] Second Am. Consolidated Class Action Compl. ("SAC") ¶ 16, Dkt. No. 93. Third-party websites can embed Facebook "like" buttons to let users share content on Facebook—for instance, CNN can embed "like" buttons on news articles that it publishes on http://www.cnn.com/ to let users share content with their Facebook friends. Id. ¶ 49. To make the "like" button appear on the page, CNN embeds a small code snippet that

[1] For a more detailed discussion of Plaintiffs' factual allegations, see this Court's order granting Facebook's previous motion to dismiss, Dkt. No. 87 at 2–6.

Facebook provides. Id. That code snippet causes the user's browser to send a background request to Facebook's servers. Id. That request includes the URL of the page where the "like" button is embedded, as well as the contents of "cookies"—small text files—that Facebook has stored on that user's browser. Id. ¶¶ 3, 52.

Plaintiffs allege that Facebook uses "like" buttons to track Plaintiffs' web browsing activity. Id. ¶¶ 3–5. Because URLs are transmitted to Facebook each time a user visits a page that contains a "like" button, Plaintiffs allege that Facebook violated various privacy laws by collecting detailed records of Plaintiffs' private web browsing history. Id. Plaintiffs allege that Facebook's cookies enable it to uniquely identify users and correlate their identities with their browsing activity, even when users are logged out of Facebook. Id. ¶¶ 48–49. As discussed below, Plaintiffs also allege that Facebook circumvented certain privacy settings of the Internet Explorer web browser. Id. ¶¶ 85–101.

Plaintiffs' initial class-action complaint alleged various statutory and common-law privacy violations. Dkt. No. 35. Facebook moved to dismiss. Dkt. No. 44. This Court granted Facebook's motion to dismiss, with leave to amend, on the grounds that Plaintiffs failed to establish Article III standing with respect to some of their claims, and that Plaintiffs failed to state a claim with respect to the rest. Order Granting Def.'s Mot. to Dismiss ("MTD Order"), Dkt. No. 87. Plaintiffs filed an amended complaint alleging violations of the federal Wiretap Act, 18 U.S.C. § 2510 et seq. (SAC ¶¶ 179–92); violations of the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq. (SAC ¶¶ 193–208); violations of the California Invasion of Privacy Act ("CIPA"), Cal. Crim. Code §§ 631, 632 (SAC ¶¶ 209–19); invasion of privacy under the California Constitution (SAC ¶¶ 220–31); intrusion upon seclusion (SAC ¶¶ 232–41); breach of contract (SAC ¶¶ 242–52); breach of the duty of good faith and fair dealing (SAC ¶¶ 253–61); fraud, Cal. Civ. Code §§ 1572, 1573 (SAC ¶¶ 262–69); trespass to chattels (SAC ¶¶ 270–73); violations of the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502 (SAC

¶¶ 274–85); and larceny, Cal. Penal Code §§ 484, 496 (SAC ¶¶ 286–95).[2] Facebook now moves to dismiss the SAC under Fed. R. Civ. P. 12(b)(1) and 12(b)(6). Def.'s Mot. to Dismiss ("MTD"), Dkt. No. 101.

II. LEGAL STANDARD

A. Rule 12(b)(1)

Dismissal under Fed. R. Civ. P. 12(b)(1) is appropriate if the complaint fails to allege facts sufficient to establish subject-matter jurisdiction. Savage v. Glendale Union High Sch., 343 F.3d 1036, 1039 n.2 (9th Cir. 2003). The Court "is not restricted to the face of the pleadings, but may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction." McCarthy v. United States, 850 F.2d 558, 560 (9th Cir. 1988). The nonmoving party bears the burden of establishing jurisdiction. Chandler v. State Farm Mut. Auto. Ins. Co., 598 F.3d 1115, 1122 (9th Cir. 2010).

B. Rule 12(b)(6)

A motion to dismiss under Fed. R. Civ. P. 12(b)(6) tests the legal sufficiency of claims alleged in the complaint. Parks Sch. of Bus., Inc. v. Symington, 51 F.3d 1480, 1484 (9th Cir. 1995). Dismissal "is proper only where there is no cognizable legal theory or an absence of sufficient facts alleged to support a cognizable legal theory." Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001). The complaint "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)).

III. DISCUSSION

A. Standing

To establish Article III standing, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be

[2] Plaintiffs dropped their claims for conversion and violations of the Computer Fraud and Abuse Act, the California Unfair Competition Law, and the California Consumer Legal Remedies Act. Plaintiffs added claims for fraud, larceny, breach of contract, and breach of the duty of good faith and fair dealing.

redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016). The plaintiff bears the burden of proving these elements. Id.

The plaintiff's injury must be "particularized" and "concrete." Id. at 1548. To be particularized, it "must affect the plaintiff in a personal and individual way." Id. To be concrete, it must be real, not abstract. Id. at 1548–49. A concrete injury can be tangible or intangible. Id. A plaintiff cannot "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirements of Article III." Id. at 1549. A plaintiff does not "automatically satisf[y] the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." Id. However, a statutory violation can confer standing when the "alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." Id. "In determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles." Id. If a plaintiff lacks Article III standing to pursue a claim, then the claim must be dismissed for lack of subject-matter jurisdiction. Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 101–02 (1998).

i. Wiretap Act, SCA, and CIPA

This Court previously found that Plaintiffs had established standing for their Wiretap Act, SCA, and CIPA claims. MTD Order 13–15. Economic injury is not required to establish standing under any of those three statutes. See In re Google Inc. Gmail Litig., No. 13-md-02430-LHK, 2013 WL 5423918, at *16 (N.D. Cal. Sept. 26, 2013) ("courts in this district have found that allegations of a Wiretap Act violation are sufficient to establish standing"); In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1055 (N.D. Cal. 2012) ("Other courts in this district have recognized that a violation of the Wiretap Act or the Stored Communications Act may serve as a concrete injury for the purposes of Article III injury analysis."); Gaos v. Google, Inc., No. 10-cv-4809-EJD, 2012 WL 1094646, at *3 (N.D. Cal. Mar. 29, 2012) ("a violation of one's statutory rights under the SCA is a concrete injury"); Cal. Penal Code § 637.2 ("It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened

with, actual damages."); In re Google Inc. Gmail Litig., 2013 WL 5423918, at *17 ("the Court finds that CIPA and the Wiretap Act are not distinguishable for the purposes of standing").

Plaintiffs allege that Facebook "intercepts" and "tracks" their internet communications in violation of all three statutes. SAC ¶¶ 179–219. These allegations are sufficient to confer standing for Plaintiffs' Wiretap Act, SCA, and CIPA claims.

ii. Trespass to Chattels, CDAFA, Fraud, and Larceny

This Court previously found that Plaintiffs did not establish standing for their claims for trespass to chattels and violations of the CDAFA. MTD Order 8–11. Unlike the statutory claims discussed above, claims for trespass to chattels and CDAFA violations require a showing of economic harm or loss. To prevail on a claim for trespass to chattels based on access to a computer system, a plaintiff must establish that (1) the defendant intentionally and without authorization interfered with the plaintiff's possessory interest in the computer system and (2) the defendant's unauthorized used proximately caused damage to the plaintiff. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000). The property owner "may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use." Id. at 1070 (quoting Itano v. Colonial Yacht Anchorage, 267 Cal. App. 2d 84, 90 (1968)). Likewise, to prevail on a CDAFA claim, "Plaintiffs must allege they suffered damage or loss by reason of a violation of Section 502(c)." In re Google Android Consumer Privacy Litig., No. 11-MD-02264-JSW, 2013 WL 1283236, at *5, *11 (N.D. Cal. Mar. 26, 2013) (finding that the plaintiffs had standing to pursue a CDAFA claim where they alleged that the defendant's conduct drained the batteries of their mobile devices).

In their SAC, Plaintiffs have added claims for fraud (Cal. Civ. Code § 1572), constructive fraud (Cal. Civ. Code § 1573), and larceny (Cal. Penal Code §§ 484, 496). SAC ¶¶ 262–69, 286–95. As with claims for trespass to chattels and violations of the CDAFA, Plaintiffs' fraud claims require a showing of actual damage. See Rodriguez v. JP Morgan Chase & Co., 809 F. Supp. 2d 1291, 1296 (S.D. Cal. 2011) (noting that a § 1572 claim requires (1) misrepresentation, (2) knowledge of falsity, (3) intent to defraud, (4) reliance, and (5) resulting damage); Dealertrack,

Inc. v. Huber, 460 F. Supp. 2d 1177, 1183 (C.D. Cal. 2006) (noting that a § 1573 claim requires (1) a fiduciary or confidential relationship, (2) an act, omission, or concealment involving a breach of that duty, (3) reliance, and (4) resulting damage). And Plaintiffs' larceny claim requires a showing of "an intent to permanently deprive an individual of his property." Castillo-Cruz v. Holder, 581 F.3d 1154, 1160–61 (9th Cir. 2009).

This Court previously found that Plaintiffs have not established a "realistic economic harm or loss that is attributable to Facebook's alleged conduct." MTD Order 10. Although Plaintiffs' personal web browsing information might have "some degree of intrinsic value," this Court held that Plaintiffs failed to show, "for the purposes of Article III standing, that they personally lost the opportunity to sell their information or that the value of their information was somehow diminished after it was collected by Facebook." Id. The SAC contains no new facts that establish economic harm or loss. Nor does the SAC establish that Facebook intended to permanently deprive Plaintiffs of property of any sort. As such, Plaintiffs lack Article III standing to pursue their claims for trespass to chattels, violations of the CDAFA, fraud, and larceny. These claims must be dismissed under Fed. R. Civ. P. 12(b)(1) for lack of subject-matter jurisdiction.

iii. Invasion of Privacy and Intrusion upon Seclusion

Plaintiffs allege that Facebook committed privacy tort violations by collecting URLs of pages that Plaintiffs visited and by using persistent cookies to associate Plaintiffs' identities with their web browsing histories. SAC ¶¶ 68–78. Unlike the claims discussed in the previous section, a plaintiff need not show actual loss to establish standing for common-law claims of invasion of privacy and intrusion upon seclusion. See, e.g., Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037, 1043 (9th Cir. 2017) (noting that "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts," and finding that the plaintiffs had Article III standing to pursue their privacy claim); In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 134 (3d Cir. 2015) (noting that "the Supreme Court itself has permitted a plaintiff to bring suit for violations of federal privacy law absent any indication of pecuniary harm," and finding that the plaintiffs had Article III standing to pursue

privacy tort claims arising from the defendant's web tracking activity). The Court finds that Plaintiffs' alleged privacy violations are sufficient to establish standing for Plaintiffs' privacy tort claims.

iv. Breach of Contract and Breach of the Duty of Good Faith and Fair Dealing

In the SAC, Plaintiffs add claims for breach of contract and breach of the duty of good faith and fair dealing. Actual damages are not required to establish standing for contractual claims. In re Facebook Privacy Litig., 192 F. Supp. 3d 1053, 1060–62 (N.D. Cal. 2016) (holding that Article III standing exists where a plaintiff seeks to "recover nominal damages for breach of contract even in the absence of actual damages" because the contractual claim alleges "a legal wrong that is fully distinct from the actual damages" (quoting Sweet v. Johnson, 169 Cal. App. 2d 630, 632 (1959)). The Court finds that Plaintiffs have standing to pursue their claims for breach of contract and breach of the duty of good faith and fair dealing.

B. Sufficiency of Allegations

i. Wiretap Act and CIPA

A claim under the Wiretap Act requires a showing that the defendant "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device." Google Cookie Placement, 806 F.3d at 135 (citing 18 U.S.C. § 2510 et seq.).

Facebook contends that it did not "intercept" Plaintiffs' communications within the meaning of the Wiretap Act. The Court agrees. The Wiretap Act provides that, with some exceptions, "[i]t shall not be unlawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication." 18 U.S.C. § 2511(2)(d) (emphasis added). Plaintiffs argue that Facebook's acquisition of URL data constitutes an "interception" of Plaintiffs' communications with websites they visit. Pls.' Opp'n to Def.'s Mot. to Dismiss 13–14, Dkt. No. 104-3. But Plaintiffs' argument misstates the means by which Facebook receives that data. As Facebook points out, two separate communications occur when someone visits a page where a Facebook "like" button is embedded. MTD 12–13. First, the

user's browser sends a GET request to the server where the page is hosted. Second, as the page loads, the code snippet for the Facebook button triggers a second, independent GET request to Facebook's servers. That second request contains the URL of the page where the "like" button is embedded, as well as the contents of cookies that Facebook has previously set on that user's computer. The parties to the first transaction are the web user (e.g., one of the Plaintiffs) and the server where the page is located (e.g., the server that handles requests for http://www.cnn.com/). The parties to the second transaction are that same web user and a Facebook server—but not cnn.com. As to the second transaction, Facebook has not "intercepted" the communication within the meaning of the Wiretap Act because it is "a party to the communication" under 18 U.S.C. § 2511(2)(d). Facebook is not a party to the first communication (between the user and cnn.com), and it does not intercept any data that those parties exchange. The fact that a user's web browser automatically sends the same information to both parties does not establish that one party intercepted the user's communication with the other. As such, the Court finds that Plaintiffs have failed to state a claim under the Wiretap Act.

Plaintiffs' CIPA claims (under Cal. Crim. Code §§ 631 and 632) fail for the same reason. See Google Cookie Placement, 806 F.3d at 152 (finding that eavesdropping claims under the CIPA were properly dismissed for the same reason that those claims were dismissed under the Wiretap Act). § 631 "broadly proscribes third party access to ongoing communications." Powell v. Union Pac. R. Co., 864 F. Supp. 2d 949, 955 (E.D. Cal. 2012) (emphasis added). "California courts interpret 'eavesdrop,' as used in § 632, to refer to a third party secretly listening to a conversation between two other parties." Thomasson v. GC Servs. Ltd. P'ship, 321 F. App'x 557, 559 (9th Cir. 2008) (emphasis added). Because Facebook did not intercept or eavesdrop on communications to which it was not a party, Plaintiffs' CIPA claims must be dismissed.

ii. SCA

To state a claim under the SCA, a plaintiff must show that the defendant "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility." 18 U.S.C.

§ 2701(a). The SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purpose of backup protection of such communication." 18 U.S.C. § 2510(17)(A), (B).

In their initial complaint, Plaintiffs argued that Facebook's persistent cookies were in "electronic storage" because they permanently resided in Plaintiffs' web browsers. MTD Order 16–17. This Court rejected Plaintiffs' argument because Facebook's cookies were not in "temporary, intermediate storage." MTD Order 16–17.

In their SAC, Plaintiffs now allege that URLs are in "electronic storage" because they reside "in the toolbar" and "in [the] browsing history" of Plaintiffs' web browsers. SAC ¶¶ 206–07. Plaintiffs' new allegations fare no better. The SCA "is specifically targeted at communications temporarily stored by electronic services incident to their transmission." In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001) (emphasis added). The SCA "only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it." Id. at 512; see also Google Cookie Placement, 806 F.3d at 146 (finding that storage in a web browser on a personal computer is not "[t]emporary storage incidental to transmission" within the meaning of the SCA). URLs stored in a web browser's toolbar or browsing history are not stored "in the middle of a transmission." Rather, they are stored locally on the user's personal computer for the user's convenience. For instance, a user might look through her browsing history to find a website she visited in the past. Similarly, the "toolbar" (or address bar) displays the URL of the page that the user is currently viewing, but the URL is stored independently of the transmission between a user's browser and a remote web server. Plaintiffs' claim fails because the SCA applies to information that is temporarily stored "incident to [the] transmission" of a communication; it does not apply to information in local storage on a user's computer.

Plaintiffs' claim also fail because personal computers are not "facilities" under the SCA. See id. ("an individual's personal computing device is not a 'facility' through which an electronic

communications service is provided . . . . a home computer of an end user is not protected by the [SCA]" (quoting Garcia v. City of Laredo, Tex., 702 F.3d 788, 793 (5th Cir. 2012))). Moreover, Plaintiffs' computers are not "electronic communication service" providers. See, e.g., In re Zynga, 750 F.3d at 1104 (holding that the SCA "covers access to electronic information stored in third party computers") (emphasis added); In re DoubleClick, 154 F. Supp. 2d at 511 ("Clearly, the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers.").

Plaintiffs' SCA claim must be dismissed.

iii. Invasion of Privacy and Intrusion upon Seclusion

To state a claim for intrusion upon seclusion, a plaintiff must show (1) that the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy and (2) that the intrusion was "highly offensive" to a reasonable person. Hernandez v. Hillsdale, 47 Cal. 4th 272, 285 (2009). To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a specific, legally protected privacy interest, (2) a reasonable expectation of privacy, and (3) a "sufficiently serious" intrusion by the defendant. In re Vizio, Inc., Consumer Privacy Litig., No. 8:16-ml-02693-JLS-KES, 2017 WL 1836366, at *17 (C.D. Cal. Mar. 2, 2017) (quoting Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1, 26 (1994)). When both claims are present, courts conduct a combined inquiry that considers "(1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests." Hernandez, 47 Cal. 4th at 287.

Here, Plaintiffs have not established that they have a reasonable expectation of privacy in the URLs of the pages they visit. Plaintiffs could have taken steps to keep their browsing histories private. For instance, as Facebook explained in its privacy policy, "[y]ou can remove or block cookies using the settings in your browser." MTD 6. Similarly, users can "take simple steps to block data transmissions from their browsers to third parties," such as "using their browsers in 'incognito' mode" or "install[ing] plugin browser enhancements." In re Hulu Privacy Litig., No. C

11-03764 LB, 2014 WL 2758598, at *8 (N.D. Cal. June 17, 2014). Facebook's intrusion could have been easily blocked, but Plaintiffs chose not to do so. In addition, websites routinely embed content from third-party servers in the form of videos, images, and other media, as well as through their use of analytics tools, advertising networks, code libraries and other utilities. Each tool transmits to third parties the same data that Plaintiffs claim is highly sensitive. Since these requests are part of routine internet functionality and can be easily blocked, the Court finds that they are not a "highly offensive" invasion of Plaintiffs' privacy interests. See Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 2015 (N.D. Cal. 2012) (finding that LinkedIn did not commit a "highly offensive" invasion of users' privacy by disclosing users' browsing histories to third parties); In re Google, Inc. Privacy Policy Litig., 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (finding that Google's collection and disclosure of users' data, including their browsing histories, "do not plausibly rise to the level of intrusion necessary to establish an intrusion claim"); In re Nickelodeon Consumer Privacy Litig., No. 12-07829, 2014 WL 3012873, at *19 (D.N.J. July 2, 2014) (dismissing plaintiffs' invasion-of-privacy claim because plaintiffs failed to show that defendants' "collection and monetization of online information," including users' browsing histories, "would be offensive to the reasonable person, let alone exceedingly so").

Plaintiffs raise specific allegations with respect to a subclass of people who used the Internet Explorer web browser (the "IE Subclass"). Under a protocol called the Platform for Privacy Preferences Project (or "P3P"), a website can publish a policy containing a machine-readable version of the website's privacy policy. SAC ¶¶ 86–88. Plaintiffs allege that, by default, Internet Explorer blocked cookies from websites that did not publish P3P policies, or from sites with policies that conflict with a user's browser privacy settings. Id. ¶ 91. However, Internet Explorer allowed cookies from websites that published policies that did not conform to the syntax of the P3P protocol. Id. ¶ 94. During the class period, Plaintiffs allege that Facebook's P3P policy contained "the tokens DSP and LAW, indicating that the Facebook privacy policy references a law that may determine remedies for breaches of their privacy policy and that there are ways to resolve privacy-related disputes." Id. ¶ 95. Plaintiffs allege that this policy did not accurately reflect

Facebook's cookie policies. Facebook later changed its P3P policy to a string that stated: "Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p." Id. ¶¶ 97–100. This second policy does not conform to the P3P syntax. As a result, Internet Explorer allowed Facebook to set cookies on users' computers.

Plaintiffs allege that Facebook adopted an "affirmatively false" P3P policy in order to trick Internet Explorer into allowing Facebook's cookies to be stored on users' browsers. Id. ¶¶ 93–98. Facebook responds that it "did not circumvent technical barriers," and in any event, Plaintiffs have not alleged that any Plaintiff actually used the versions of Internet Explorer that implemented P3P. MTD 27 n.15.

Plaintiffs' argument would compel Facebook to adopt the P3P protocol and publish a policy with specific contents. But adoption of P3P is voluntary: Facebook can choose to publish a machine-readable version of its privacy policy, but it has no legal duty to do so. Similarly, browser manufacturers can choose to support the P3P protocol, but they have no power to require websites to publish P3P policies, or to dictate the contents of those policies. In this respect, the facts are different from the scenario underlying the Third Circuit's decision in Google Cookie Placement. There, the Plaintiffs alleged that Google deliberately circumvented cookie-blocking settings in users' browsers, while claiming that it respected users' decisions to "[set] your browser to refuse all cookies." 806 F.3d at 150. "Characterized by deceit and disregard," the court held, "the alleged conduct raises different issues than tracking or disclosure alone." Id. On that basis, the court found that the plaintiffs had stated claims for intrusion upon seclusion and invasion of privacy under the California Constitution. Id. at 151. The claims here are different. Unlike the allegations in Google Cookie Placement, Facebook never promised to adopt the P3P protocol. Rather, Facebook publicly stated that it "does not have a P3P policy." SAC ¶ 100; see also id. ¶ 99 (quoting a public statement in which Facebook indicated that it chose not to adopt P3P because the protocol does not "allow a rich enough description to accurately represent our privacy policy"). Because Facebook had no obligation to adopt P3P, the Court finds that Plaintiffs have not stated claims for privacy tort violations as to the IE subclass.

iv. Breach of Contract and Breach of the Duty of Good Faith and Fair Dealing

Plaintiffs allege that Facebook "breached its contract with Plaintiffs and each of the Class members by tracking and intercepting" their communications with third-party websites. SAC ¶ 250. The relevant contract during the class period was Facebook's "Statement of Rights and Responsibilities" ("SRR"). Id. ¶ 17. Plaintiffs allege that Facebook's privacy policy was incorporated by reference into the SRR, and that some of Facebook's "help pages" were also incorporated by reference. Id. ¶ 20, 23. According to Plaintiffs, "[o]ne help page entry provided more detail related to Facebook's use of cookies," and Facebook "represented in the social plug-in discussion that 'when you log out of Facebook, we remove the cookies that identify your particular account.' " Id. ¶ 23.

Other than general references to "help pages" and a "social plug-in discussion," Plaintiffs fail to explain where or when these statements appeared. Plaintiffs also fail to explain how these statements were incorporated into the binding SRR, other than by reference in the complaint to a "layered approach" through which Facebook made its policies easier to understand by "summarizing our practices on the front page and then allowing people to click through the Policy for more details." Id. ¶ 22. Plaintiffs do not, for instance, identify a trail of links leading from the SRR to the statements it identifies.

"In an action for breach of a written contract, a plaintiff must allege the specific provisions in the contract creating the obligation the defendant is said to have breached." Woods v. Google Inc., No. 05:11-cv-1263-JF, 2011 WL 3501403, at *3 (N.D. Cal. Aug. 10, 2011). Statements "spread across a variety of pages in a variety of formats make it difficult to identify the terms of any actual and unambiguous contractual obligations." Id. at *4. Because Plaintiffs have not identified the specific contractual provisions they allege were breached, Plaintiffs' breach-of-contract claim will be dismissed with leave to amend.

Plaintiffs' claim for breach of the duty of good faith and fair dealing also fails. "[T]he implied covenant of good faith and fair dealing 'cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement.' "

Rosenfeld v. JPMorgan Chase Bank, N.A., 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010) (quoting Agosta v. Astor, 120 Cal. App. 4th 596, 607 (2004)). Plaintiffs have not identified the terms of the agreement that imposed a duty on Facebook not to engage in the tracking activity at issue. As such, Plaintiffs' breach-of-duty claim will also be dismissed with leave to amend.

IV. CONCLUSION

The Court orders as follows:

1. Facebook's motion to dismiss Plaintiffs' claims for trespass to chattels (SAC ¶¶ 270–73), violations of the CDAFA (SAC ¶¶ 274–85), fraud (SAC ¶¶ 262–69), and larceny (SAC ¶¶ 286–95) is GRANTED without leave to amend for lack of standing under Fed. R. Civ. P. 12(b)(1).

2. Facebook's motion to dismiss Plaintiffs' claims for violations of the Wiretap Act (SAC ¶¶ 179–92), violations of the SCA (SAC ¶¶ 193–208), violations of the CIPA (SAC ¶¶ 209–19), invasion of privacy (SAC ¶¶ 220–31), and intrusion upon seclusion (SAC ¶¶ 232–41) is GRANTED without leave to amend for failure to state a claim under Fed. R. Civ. P. 12(b)(6).

3. Facebook's motion to dismiss Plaintiffs' claims for breach of contract (SAC ¶¶ 242–52) and breach of the duty of good faith and fair dealing (SAC ¶¶ 253–61) is GRANTED with leave to amend.

4. Facebook's motion for a protective order temporarily staying further discovery (Dkt. No. 108) is DENIED.

5. Plaintiffs' motion to compel discovery (Dkt. No. 110) is TERMINATED and may be refiled in accordance with the procedures of the assigned magistrate judge.

IT IS SO ORDERED.

Dated: June 30, 2017

EDWARD J. DAVILA
United States District Judge