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. 44

Facebook, Inc. ("Facebook") operates an online "social network" that permits its members to interact with each other through a website - www.facebook.com. Id. at ¶ 9. This consolidated, multi-district lawsuit against the social network, brought by and on behalf of individuals with active Facebook accounts from May 27, 2010, through September 26, 2011 (the "Class Period"), seeks "in excess of $15 billion in damages and injunctive relief" and "arises from Facebook's knowing interception of users' internet communications and activity after logging out of their Facebook accounts." See Corrected First Am. Consolidated Class Action Compl. ("CCAC"), Docket Item No. 35, at ¶ 1. Plaintiffs Perrin Davis, Cynthia Quinn, Brian Lentz, and Matthew Vickery (collectively, "Plaintiffs"), each of whom had an active Facebook account during the entire Class Period, allege that Facebook tracked and stored their post-logout internet usage using small text files - or "cookies" - which Facebook had embedded in their computers' browsers. Id. at ¶¶ 103-106.

Federal jurisdiction arises pursuant to 28 U.S.C. §§ 1331 and 1332(d). Presently before the court is Facebook's Motion to Dismiss pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). See Docket Item No. 44. Plaintiffs oppose the motion. Having carefully considered

the parties' arguments, the court has concluded that Facebook's arguments are meritorious. Accordingly, the motion will be granted for the reasons explained below.

I. BACKGROUND

A. "Cookies"

As noted, a "cookie" is a small text file that a server creates and sends to a browser, which then stores the file in a particular directory on an individual's computer. Id. at ¶ 38. A cookie contains a limited amount of information which can relate to the browser or to a specific individual. Id. at ¶¶ 38, 39.

When an individual using a web browser contacts a server - often represented by a particular webpage or internet address - the browser software checks to see if that server has previously set any cookies on the individual's computer. Id. at ¶ 39. If the server recognizes any valid, unexpired cookies, then the computer "sends" those cookies to the server. Id. at ¶ 39. After examining the information stored in the cookie, the server knows if it is interacting with a computer with which it has interacted before. Id. at ¶ 41. Since servers create database records that correspond to individuals, sessions and browsers, the server can locate the database record that corresponds to the individual, session or browser using the information from the cookie. Id.

B. Facebook and its Use of "Cookies"

Plaintiffs allege that Facebook is the brainchild of the company's founder, Mark Zuckerberg, who wrote the first version of "The Facebook" in his Harvard University dorm room and later launched Facebook as a company in 2004. Id. at ¶ 10. Since then, Facebook has become the largest social networking site in the world with other 800 million users world-wide and over 150 million users in the United States. Id. at ¶ 11. According to Plaintiffs, the key to this success "was to convince people to create unique, individualized profiles with such personal information as employment history and political and religious affiliations, which then could be shared among their own network of family and friends." Id. at ¶ 10. Facebook uses this repository of personal data to connect advertisers with its users. Id. at ¶ 12. Historically, 90% of Facebook's revenue is attributable to third-party advertising and "Facebook is driven to continue to find new and creative

ways to leverage its access to users' data in order to sustain its phenomenal growth." Id. at ¶ 13.

Facebook does not charge a fee for membership. Id. at ¶ 14. However, Plaintiffs contend that Facebook membership is not free. Id. at ¶ 14. Specifically, they allege that through the Statement of Rights and Responsibilities and other documents and policies governing use of the website, "Facebook conditions its membership upon users providing sensitive and personal information . . . including name, birth date, gender and email address," and requires that users accept numerous Facebook cookies on their computers. Id. at ¶¶ 14, 16. These cookies allow Facebook to intercept a user's electronic communications and track internet browsing history. Id.

Facebook cookies come in two flavors. The first is a "session cookie," which is set when a user logs into Facebook. Id. at ¶ 15. It is directly associated with a user's Facebook account and contains unique information, such as the user's Facebook identification. Id. Session cookies are supposed to be deleted when the user logs out of Facebook. Id.

The second type is a "tracking cookie," which is also known as a persistent cookie. Id. This cookie sends data back to Facebook any time an individual makes a request of www.facebook.com, such as when an individual accesses a page with the Facebook "like" button. Id. The tracking takes place, however, regardless of whether the individual actually interacts with the "like" button; "[i]n effect, Facebook is getting details of where you go on the Internet." Id. Tracking cookies do not expire when a user logs out of Facebook. Id. In fact, Facebook sets these cookies on an individual's computer whether or not they have a Facebook account. Id.

When a Facebook user leaves the Facebook webpage without logging out and then browses the web, both tracking cookies (such as a "datr" cookie) and session cookies (such as a "c_user" cookie) are left to operate on the computer. Id. Under those circumstances, Facebook is notified through the datr cookie whenever the user loads a page with embedded content from Facebook, and also can easily connect that data back to the user's individual Facebook profile through the c_user cookie. Id.

For example, if a logged-in Facebook user accesses the news website www.cnn.com through the browser on his or her computer, the CNN server responds with the file for the CNN

homepage, which also contains embedded code from Facebook. Id. at ¶¶ 59, 60. The user's browser, triggered by the Facebook code, sends a request to the Facebook server to display certain content on the CNN webpage, such as the Facebook "like" button. Id. at ¶ 61. This request also includes information contained in the user's datr and c_user cookies as well as the specific details of the webpage that the user accessed. Id. at ¶ 63. When Facebook receives this information, the Facebook server adds it to its database records for the browser and the user. Id. at ¶ 67. The Facebook server then responds by sending the requested content to the user's browser. Id. at ¶ 70.

C. Facebook Tracks Logged-Out Users

Aside from tracking logged-in users, Plaintiffs allege that Facebook has also intentionally tracked users' browsing activity after they logged-out of the Facebook website despite contrary representations in the social network's governing materials. Id. at ¶ 17. Facebook is able to engage in such tracking though the persistent datr cookie its server embeds after the user accesses www.facebook.com. Id. at ¶ 73.

Again using the CNN website as an example, if a user logs out of Facebook and then directs his or her computer's browser to www.cnn.com, the CNN server responds in much the same way as if the user was still logged-in to Facebook: by sending to the browser a file with the contents of the CNN website which contains a piece of Facebook code pertaining to the "like" button. Id. at ¶¶ 72-75. The browser, triggered by the Facebook code, sends a request to the Facebook server to display the "like" button on the CNN webpage. Id. at ¶ 77. This request also includes any personally identifiable information contained in cookies associated with the browser, such as the datr cookie. Id. at ¶ 78. The Facebook server then creates a database log entry of the request, stores the cookie information it received, and responds by sending the content requested for display on the CNN website. Id. at ¶¶ 78-82.

Plaintiffs allege the information Facebook receives through tracking logged-out users is specific enough to identify the user without the need for an additional Facebook cookie containing the user's identification. Id. at ¶ 83. Indeed, they allege that "[f]rom the first time a Facebook user logs into Facebook and the datr tracking cookie is set on his machine, all of that user's

browsing to Facebook partner sites using that browser is linked by Facebook back to that user because the datr tracking cookie contains a unique number, which is also unique to that particular user's browser and his specific computer or mobile device, that indexes into the Facebook database which tracks users and browser sessions both on computers and mobile devices such as Android cell phones, iPhones, iPads, and the iPod Touch." Id. Furthermore, Plaintiffs believe that Facebook implemented a P3P "compact policy"[1] that circumvented privacy settings on Microsoft's Internet Explorer ("IE") browser to allow Facebook's cookies, thereby ensuring that IE would transmit information from Facebook cookies back to the Facebook server when users visited affiliated non-Facebook websites. Id. at ¶¶ 101, 102.

Plaintiffs contend that the personal information Facebook receives from its users, including users' browsing history, has "massive economic value" and that a market exists for such information. Id. at ¶¶ 112, 122-124. They point out that "internet giant" Google, Inc. conducts a panel called "Google Screenwise Trends," the purpose of which is "to learn more about how everyday people use the Internet." Id. at ¶ 118. Through this program, internet users consent to share with Google the websites they visit and how they use them in exchange for gift cards, "mostly valued at exactly $5." Id. at ¶¶ 119, 121.

Plaintiffs further allege the value of their personal information can be quantified. Id. at ¶ 116. Based on a study published in 2011, Plaintiffs allege that the contact information users must provide to Facebook when becoming a member is worth $4.20 per year. Id. In addition, demographic information is worth $3.00 per year and web browsing histories are worth $52.00 per year. Id. Aggregated across Facebook's approximately 800 million users, these values translate into membership "fees" of $3.36 billion, $2.4 billion and $41.6 billion, respectively, for each category of information. Id.

[1] According to the CCAC, "P3P" refers to the Platform for Privacy Preferences, which is a standard format for computer-readable privacy policies published by the World Wide Web Consortium in 2002. See CCAC, at ¶ 86. A P3P "compact policy" is a computer-readable encoded version of the portion of a privacy policy relating to cookies. Id.

D. Relevant Procedural History

A number of cases challenging Facebook's tracking practices were filed in and outside this district. They were eventually transferred to the undersigned. The court consolidated the cases for pretrial consideration and appointed interim class counsel. See Docket Item No. 19. Plaintiffs thereafter filed the CCAC, which is the currently operative pleading. See Docket Item No. 35. This motion followed.

II. LEGAL STANDARD

A. Federal Rule of Civil Procedure 12(b)(1)

A Rule 12(b)(1) motion challenges subject matter jurisdiction and may be either facial or factual. Wolfe v. Strankman, 392 F.3d 358, 362 (9th Cir.2004). A facial 12(b)(1) motion involves an inquiry confined to the allegations in the complaint, whereas a factual 12(b)(1) motion permits the court to look beyond the complaint to extrinsic evidence. Id. When, as here, a defendant makes a facial challenge, all material allegations in the complaint are assumed true, and the court must determine whether lack of federal jurisdiction appears from the face of the complaint itself. Thornhill Publ'g Co. v. General Tel. Elec., 594 F.2d 730, 733 (9th Cir.1979).

Standing is properly challenged through a Rule 12(b)(1) motion. White v. Lee, 227 F.3d 1214, 1242 (9th Cir. 2000). "A plaintiff has the burden to establish that it has standing." WildEarth Guardians v. United States Dep't of Agric., 795 F.3d 1148, 1154 (9th Cir. 2015).

B. Federal Rule of Civil Procedure 12(b)(6)

Federal Rule of Civil Procedure 8(a) requires a plaintiff to plead each claim with sufficient specificity to "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007) (internal quotations omitted). Although particular detail is not generally necessary, the factual allegations "must be enough to raise a right to relief above the speculative level" such that the claim "is plausible on its face." Id. at 556-57. A complaint which falls short of the Rule 8(a) standard may be dismissed if it fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). "Dismissal under Rule 12(b)(6) is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts

to support a cognizable legal theory." Mendiondo v. Centinela Hosp. Med. Ctr., 521 F.3d 1097, 1104 (9th Cir. 2008).

When deciding whether to grant a motion to dismiss, the court usually "may not consider any material beyond the pleadings." Hal Roach Studios, Inc. v. Richard Feiner & Co., 896 F.2d 1542, 1555 n. 19 (9th Cir.1990). However, the court may consider material submitted as part of the complaint or relied upon in the complaint, and may also consider material subject to judicial notice. See Lee v. City of Los Angeles, 250 F.3d 668, 688-89 (9th Cir. 2001).

In addition, the court must generally accept as true all "well-pleaded factual allegations." Ashcroft v. Iqbal, 556 U.S. 662, 664 (2009). The court also must construe the alleged facts in the light most favorable to the plaintiff. Love v. United States, 915 F.2d 1242, 1245 (9th Cir.1988). But "courts are not bound to accept as true a legal conclusion couched as a factual allegation." Id. Nor must the court accept as true "allegations that contradict matters properly subject to judicial notice or by exhibit" or "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." In re Gilead Scis. Sec. Litig., 536 F.3d 1049, 1055 (9th Cir. 2008).

III. DISCUSSION

Plaintiffs assert the following claims in the CCAC: (1) violation of the Federal Wiretap Act, 18 U.S.C. § 2510 et seq.; (2) violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq.; (3) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030[2]; (4) invasion of privacy; (5) intrusion upon seclusion; (6) conversion; (7) trespass to chattels; (8) violation of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200 et seq.; (9) violation of the California Computer Crime Law ("CCCL"), Penal Code § 502; (10) violation of the California Invasion of Privacy Act ("CIPA"), Penal Code § 630 et seq.; and (11) violation of California's Consumer Legal Remedies Act ("CLRA"), Civil Code § 1750.

Under Rule 12(b)(1), Facebook argues that all of these claims fail for lack of standing. Under Rule 12(b)(6), Facebook further argues that the fraud-based claims lack the factual

[2] Plaintiffs have withdrawn this claim. It will therefore be dismissed without leave to amend.

specificity required by Federal Rule of Civil Procedure 9(b), and that Plaintiffs have not stated an actionable claim. These arguments are discussed below.

A. Standing

i. Constitutional Standing

The constitutional standing doctrine "functions to ensure, among other things, that the scarce resources of the federal courts are devoted to those disputes in which the parties have a concrete stake." Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc., 528 U.S. 167, 191 (2000). Generally, the inquiry critical to any standing issue is "'whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.'" Allen v. Wright, 468 U.S. 737, 750-51 (1984) (quoting Warth v. Seldin, 422 U.S. 490, 498 (1975)). Standing under Article III of the Constitution has three basic elements: (1) an "injury in fact," which is neither conjectural or hypothetical, (2) causation, such that a causal connection between the alleged injury and offensive conduct is established, and (3) redressability, or a likelihood that the injury will be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992).

Noting the lack of allegations that anyone was willing to pay for their personal information or that its purported conduct lessened the value of that information or affected its marketability, Facebook argues that Plaintiffs have not established a cognizable injury in fact. To satisfy the "injury in fact" element, "the plaintiff must show that he personally has suffered some actual or threatened injury as a result of the putatively illegal conduct of the defendant." Gladstone Realtors v. Village of Bellwood, 441 U.S. 91, 100 (1979). Moreover, since this is a class action, at least one of the named plaintiffs must have suffered an injury in fact. See Lierboe v. State Farm Mut. Auto. Ins. Co., 350 F.3d 1018, 1022 (9th Cir. 2003) ("[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class.").

When confronted with data privacy claims similar to the ones brought by Plaintiffs, courts have found insufficient for standing purposes generalized assertions of economic harm based solely on the alleged value of personal information. In LaCourt v. Specific Media, Inc., No.

SACV 10-1256-GW(JCGx), 2011 U.S. Dist. LEXIS 50543, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), the plaintiffs alleged that Specific Media, "an online third party ad network that earns its revenue by delivering targeted advertisements," stored cookies on their computers, which it then used to collect browsing history information in order to create behavioral profiles and target specific categories of ads at different users. LaCourt, 2011 U.S. Dist. LEXIS 50543, at *2. The plaintiffs also claimed that Specific Media's conduct caused them economic loss "in that their personal information has discernable value" of which they were deprived, and which Specific Media retained and used for its own benefit. Id. at *3-4. Specific Media moved to dismiss the complaint for lack of Article III standing under Rule 12(b)(1), arguing that the plaintiffs' theory of economic harm did not make out an injury in fact. Id. at *7.

The district court agreed with Specific Media and dismissed the complaint. The court determined that, while it "probably would decline to say that it is categorically impossible for [the plaintiffs] to allege some property interest that was compromised" by Specific Media's information collection practices, the plaintiffs had not alleged they were actually deprived of the economic value of their browsing histories. Id. at *11. The court reasoned this was so because the plaintiffs had not cited "some particularized example" of "a single individual who was foreclosed from entering into a 'value-for-value exchange' as a result of Specific Media's alleged conduct," or explained how they were deprived of the information's value simply because it was collected by a third party. Id. at *11-12.

A similar conclusion was reached in Low v. LinkedIn Corporation, No.11-CV-01468-LHK, 2011 U.S. Dist. LEXIS 130840, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011). There, the plaintiff alleged economic loss from LinkedIn's practice of transmitting users' personal information, such as the name of each user and his or her profile viewing history, to third party tracking cookies which allowed the recipients to aggregate the data. Low, 2011 U.S. Dist. LEXIS 130840, at *3-4. Relying on LaCourt, the court found the plaintiff's allegations "too abstract and hypothetical to support Article III" standing. Id. at *10. The court reasoned that the plaintiff failed to demonstrate that he personally suffered some type of real economic harm due to the

transmission of his personal information. Id. at *12-15.

An out-of-circuit case, In re Google Inc. Cookie Placement Consumer Privacy Litigation ("Google Cookie Placement"), 988 F. Supp. 2d 434 (D. Del. Oct. 9, 2013), is also of note. The plaintiffs in that case alleged that Google had employed third-party cookies to track consumer internet browsing for use in targeted advertising without first obtaining consent to do so. 988 F. Supp. 2d at 440. Much like the district court did in LaCourt, the Delaware district court accepted the plaintiffs' contention that their personally identifiable information had "some modicum of identifiable value to an individual plaintiff." Id. at 442. But the court found that value alone was insufficient to establish Article III standing, explaining that the plaintiffs had not "sufficiently alleged that the ability to monetize their [personally identifiable information had] been diminished or lost by virtue of Google's collection of it." Id.

The court finds these decisions instructive mainly because Plaintiffs' allegations are virtually indistinguishable from those rejected in LaCourt, Low and Google Cookie Placement. Like the plaintiffs in those cases, Plaintiffs allege that the information collected by Facebook's cookies have economic value and, if the study cited in the CCAC is accurate, that value may be significant when user information is aggregated. The court accepts as true Plaintiffs' ascription of some degree of intrinsic value to their personal information for this motion. But what Plaintiffs have failed to do is adequately connect this value to a realistic economic harm or loss that is attributable to Facebook's alleged conduct. In other words, Plaintiffs have not shown, 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.

Unlike other data privacy cases, Plaintiffs have alleged the existence of a limited market for their browsing histories. That allegation, however, is still not enough to establish a qualifying injury in fact. That programs may exist to compensate internet users with $5 gift cards in exchange for monitoring their browsing activity is a fact of little assistance to Plaintiffs when they have not also alleged an inability to participate in these programs after Facebook collected their

information.[3]

Nor do the allegations of consequential damages incurred by one plaintiff, Davis, provide a persuasive basis to find a sufficiently-pled injury in fact. Other than a conclusory allegation deeming it so, it is not apparent how charges for an email service which alerts users when Facebook makes changes to its privacy policy or privacy settings are "fairly traceable" to the conduct alleged in the complaint.[4] See Lujan, 504 U.S. at 560. Moreover, the allegations related to the monitoring service are too vague without a specified timeframe describing when these damages accrued.

As pled, the CCAC only alludes to injury that is conjectural or hypothetical. Since Plaintiffs have not demonstrated that Facebook's conduct resulted in some concrete and particularized harm, they have not articulated a cognizable basis for standing pursuant to Article III.

ii. Statutory Standing

For their part, Plaintiffs do not directly address Facebook's constitutional standing argument, choosing instead to focus on statutory standing. Thus, the issue becomes whether any of the statutory claims asserted in the CCAC can satisfy the federal standing requirement.

Although it cannot be supplanted by a statute, an Article III injury can exist solely by virtue of "statutes creating legal rights, the invasion of which creates standing." Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010); see Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997) ("Congress cannot erase Article III's standing requirements by statutorily granting the right to sue

---

[3] Notably, this reasoning is unaffected by Ninth Circuit's 2014 limited standing discussion in In re Facebook Privacy Litigation, 572 Fed. Appx. 494 (2014). A review of the facts of that case, as illustrated in the companion opinion In re Zynga Privacy Litigation, 750 F.3d 1098 (2014), reveals that Facebook was disclosing identifying information to third-party websites in referer headers. Given that no such disclosure is alleged here, any Article III standing determination made in Facebook Privacy Litigation is inapplicable to this case.

[4] In their opposition, Plaintiffs raise several new facts relating to consequential damages and other issues. Those facts have no bearing on whether the CCAC is adequate. See Schneider v. Cal. Dep't of Corr., 151 F.3d 1194, 1197 n.1 (9th Cir. 1998) ("The 'new' allegations contained in the . . . opposition motion . . . are irrelevant for Rule 12(b)(6) purposes.").

to a plaintiff who would not otherwise have standing."). The relevant question in such circumstances is "whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." Id.

So-called "statutory standing" can be established by pleading a violation of a right conferred by statute so long as the plaintiff alleges "a distinct and palpable injury to himself, even if it is an injury shared by a large class of other possible litigants." Warth, 522 U.S. at 501. Whether or not a plaintiff has stated a basis for statutory standing is tested under Rule 12(b)(6) rather than Rule 12(b)(1). Maya v. Centex Corp., 658 F.3d 1060, 1067 (9th Cir. 2011).

Here, Plaintiffs' arguments in support of statutory standing are uncompelling for several of their claims. First, it is axiomatic that standing permitted by statute does not translate into standing for common law claims. See Davis v. Fed. Election Comm'n, 554 U.S. 724, 734 (2008) (holding that standing is not "dispensed in gross" and must be established for each claim and each form of relief). Thus, all of the common law claims asserted in the CCAC which rely on economic harm related to the loss of personal information as an element of damages, in particular the claims for conversion and trespass to chattels, are subject to dismissal for lack of constitutional standing under Article III.[5] See Low, 2011 U.S. Dist. LEXIS 130840, at *2 (dismissing similar common law claims for lack of Article III standing).

Second, the court agrees with Facebook that three of Plaintiffs' statutory claims, those for

---

[5] In any event, the claims for invasion of privacy and intrusion upon seclusion are also subject to dismissal for failure to state a claim even if Plaintiffs rely on some other form of damage for these claims. To the extent they can be considered separate claims - a concept which is itself questionable - both require "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." Shulman v.Group W Prods., Inc., 18 Cal. 4th 200, 214 & n.4 (1996); Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1, 66 (1994). To establish the first element, the plaintiff must have had an actual, subjective expectation of seclusion that was objectively reasonable. Med Lab. Mgmt. Consultants v. ABC, Inc., 306 F.3d 806, 812-13 (9th Cir. 2002). Under the current allegations, Plaintiffs could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable because "Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit . . . ." United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007). Plaintiffs "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." Id.

violation of the UCL, CLRA and the CCCL, require a plausible economic injury for standing. Reid v. Johnson & Johnson, 780 F.3d 952, 958 (9th Cir. 2015) ("To establish standing to bring a claim under [the UCL and CLRA], plaintiffs must meet an economic injury-in-fact requirement, which demands no more than the corresponding requirement under Article III of the U.S. Constitution."); Cal. Penal Code § 502(e) (conferring standing to bring a civil action on owners or lessees of a "computer, computer system, computer network, computer program, or data who suffer[] damage or loss by reason of a violation" of the CCCL). Consequently, the statutory standing analysis for these claims coincides with the Article III analysis.

The three remaining statutory claims are different, however, because economic injury is not a prerequisite for standing under their provisions. See Chapman v. Pier 1 Imps. (U.S.), Inc., 631 F.3d 939, 947 (2011) ("The existence of federal standing 'often turns on the nature and source of the claim asserted.'"). As to the Wiretap Act, "courts in this district have found that allegations of a Wiretap Act violation are sufficient to establish standing." In re Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784, at *63, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013); 18 U.S.C. § 2520(a) ("[A]ny person whose wire, oral, or electronic communication is . . . disclosed . . . may in a civil action recover from the person or entity . . . such relief as may be appropriate."). The same is true of the SCA. 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. 5:10-CV-4809 EJD, 2012 U.S. Dist. LEXIS 44062, at *9, 2012 WL 109446 (N.D. Cal. Mar. 29, 2012) ("Thus, a violation of one's statutory rights under the SCA is a concrete injury."); 18 U.S.C. § 2707(a) ("[A]ny . . . person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity . . . which engaged in that violation such relief as may be appropriate."). And because it specifically excludes economic damages as a precursor to liability, the court concludes that allegations of a CIPA violation sufficiently establish standing under that statute as well. 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 U.S. Dist. LEXIS 172784, at *67 ("[T]he Court finds that CIPA and the Wiretap Act are not distinguishable for the purposes of standing.").

Here, Plaintiffs allege that Facebook intercepted and tracked their internet activity and acquired this information after they logged out of the Facebook website using the datr cookie embedded on their computers. Plaintiffs also assert this conduct violated the Wiretap Act, SCA and CIPA. Consistent with other district courts to have examined statutory standing to bring similar claims, this court finds Plaintiffs' allegations sufficient to make out a distinct and palpable injury considering the conduct prohibited by those statutes. In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011) ("The Wiretap Act provides that any person whose electronic communication is 'intercepted, disclosed, or intentionally used' in violation of the Act may in a civil action recover from the entity which engaged in that violation."); Gaos, 2012 U.S. Dist. LEXIS 44062, at *8 (explaining that the SCA "prohibits an electronic communication service from divulging the contents of a communication in electronic storage . . . and prohibits a remote computing service from divulging the contents of communications carried or maintained on that service"); In re Google Inc. Gmail Litig., 2013 U.S. Dist. LEXIS 172784, at *58 (observing that CIPA "prohibits wiretapping or 'any other unauthorized connection' with a 'wire, line, cable, or instrument.'").

In sum, Plaintiffs have established statutory standing for claims under the Wiretap Act, SCA and CIPA. The court is mindful, however, that the issue of standing is distinct from whether or not Plaintiffs have actually stated a plausible claim. In re Facebook Privacy Litig., 791 F. Supp. 2d at 712 n. 5 ("A plaintiff may satisfy the injury-in-fact requirements to have standing under Article III, and thus may be able to 'bring a civil action without suffering dismissal for want of standing to sue,' without being able to assert a cause of action successfully."). All other claims, however, will be dismissed with leave to amend for lack of standing. Since this dismissal will encompass the UCL, CLRA and CCCL claims, the court need not address Facebook's argument

under Rule 9(b).

B. Sufficiency of Allegations

The court now turns to whether Plaintiffs have stated a plausible claim under the Wiretap Act, SCA or CIPA.

i. The Wiretap Act and SCA

The Wiretap Act and SCA represent "two chapters" within the Electronic Communications Privacy Act of 1986 ("ECPA"). In re Zynga Privacy Litig., 750 F.3d 1098, 1100 (9th Cir. 2014). Title I of the ECPA, which contains the Wiretap Act, "provides that (with certain exceptions), 'a person or entity' (1) 'providing an electronic communication service to the public' (2) 'shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof)' (3) 'while in transmission on that service' (4) 'to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.'" Id. at 1104 (quoting 18 U.S.C. § 2511(3)(a)). Title II of ECPA is the SCA, which "covers access to electronic information stored in third party computers." Id. (citing 18 U.S.C. §§ 2701-12). Under the portion of the SCA relevant here, "whoever (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; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system" is subject to liability. 18 U.S.C. § 2701(a). For a civil action under the SCA, the conduct constituting the violation must have been done with "a knowing or intentional state of mind." 18 U.S.C. § 2707(a).

Facebook argues the CCAC's claim under the Wiretap Act is insufficient because Plaintiffs did not plead that Facebook intercepted the "contents" of an electronic communication. Under the Wiretap Act, the "contents" of a communication are defined as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The Ninth Circuit has held that as used in the Wiretap Act "the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the

characteristics of the message that is generated in the course of the communication" such as a name, address, or the identify of a subscriber or customer. In re Zynga Privacy Litig., 750 F.3d at 1106-1107. Applying this holding, the court went on to find that a "referer header" - basically the portion of a webpage request message that provides the address of the webpage from which the request was sent - does not meet the Wiretap Act's definition of "contents." Id. "[T]he webpage address identifies the location of a webpage a user is viewing on the internet, and therefore functions like an 'address' . . . . Congress excluded this sort of record information from the definition of 'contents.'" Id.

For Plaintiffs' Wiretap Act claim, Zynga Privacy Litigation poses a significant hurdle. Although Plaintiffs do not specify just what information of theirs was intercepted by Facebook, Plaintiffs generally allege that, through cookies embedded on a user's browser, Facebook receives personal information about logged-out users information as well as the identity of the webpages that the users visited. But since they also allege in other portions of the CCAC that c_user and datr cookies contain only a Facebook user's unique identification information and a record of browsing history, they have not alleged that Facebook intercepted anything that qualifies as "content" under the Wiretap Act. In turn, Plaintiffs have not stated a claim under the statute. In fact, since the intercepted information described in the CCAC is so similar to the referer headers addressed in Zynga Privacy Litigation, Plaintiffs may never be able to state an action Wiretap Act claim, particularly since their arguments on this issue are unpersuasive.

The SCA claim is also deficient. As relevant here, "electronic storage" means "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). The "language and legislative history" of the definition "make evident" that "electronic storage" does include cookies stored on a user's computer; "[r]ather it appears that the section is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission - for example, when an email service stores a message until the addressee downloads it." In re Doubleclick Privacy Litig., 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001); In re Toys R Us, Inc.,

Privacy Litig., No. M-00-1381 MMC, 2001 U.S. Dist. LEXIS 16947, at *10-11, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001). Plaintiff's theory under the SCA as it is currently described in the CCAC - that Facebook accesses personal information through persistent cookies permanently residing in users' personal web browsers - cannot be reconciled with the temporary nature of storage contemplated by the statutory definition. The case upon which Plaintiffs rely, Doe v. City and County of San Francisco, No. C10-04700 TEH, 2012 U.S. Dist. LEXIS 81305, 2012 WL 2132398 (N.D. Cal. Jun. 12, 2012), does not hold otherwise and, in fact, is consistent with this discussion because the "electronic storage" at issue there was a webmail inbox. Accordingly, Plaintiffs have not stated a claim for violation of the SCA in the CCAC.

ii. CIPA

The section of CIPA upon which Plaintiffs base their claim, Penal Code § 631, establishes liability for:

> [a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state.

Cal. Penal Code § 631(a).

Facebook challenges the CIPA claim on multiple grounds, two of which are misplaced. It first contends that this criminal statute should be narrowly construed and should not be applied to electronic communications. Because that argument has been made before and squarely rejected, the court rejects it again here. In re Google Inc. Gmail Litig., 2013 U.S. Dist. LEXIS 172784, at *76-79.

Second, Facebook argues it cannot be considered an unauthorized participant in the transmission of Plaintiffs' personal information because the process of tracking their browsing

activity involved communication with a Facebook server. This characterization of the allegations is incomplete because Plaintiffs allege they were unaware that Facebook was surreptitiously tracking them after they logged out of the Facebook website. Thus, while it is true that a Facebook server was involved, there are no allegations in the CCAC which demonstrate that Plaintiffs knew that fact while their browsing activity was being tracked and collected. The cases relied on by Facebook are inapposite because each involved recording by a known participant to a telephone conversation. See Warden v. Kahn, 99 Cal. App. 3d 805, 808-809 (1979); see also Rogers v. Ulrich, 52 Cal. App. 3d 894, 896 (1976).

Facebook's third and fourth arguments are well-taken, however. Plaintiffs have not pled facts to show how Facebook used a "machine, instrument, or contrivance" to obtain the contents of communications. While it is undeniable that a computer may qualify as a "machine," Plaintiffs must complete the scenario by explaining how Facebook's cookies fall into one of the three categories enumerated in the statute. To be sure, the cookie is a required piece under Plaintiffs' theory because the offensive transmission of information between two computers - the user's computer and the Facebook server - apparently does not occur without it. Thus, if a cookie is truly a "contrivance" as Plaintiffs contend, a word they define as a "device, especially a mechanical one" or "plan or scheme," Plaintiffs must include facts in their pleading to show why it is so. In its current form, the CCAC only defines a cookie as a small text file containing a limited amount of information which sits idly on a user's computer until contacted by a server.

Nor have Plaintiffs adequately alleged that Facebook obtained the contents of a communication attributable to any of them. The section of the CCAC which does purport to provide Plaintiffs' "specific factual allegations" is anything but specific. In essence, it is just a list of the named plaintiffs coupled with the same set generalized facts for each one. See CCAC, at ¶¶ 103-106. Such allegations do not suffice to "nudge" their CIPA claim "across the line from conceivable to plausible." Iqbal, 556 U.S. at 680.

For these reasons, Plaintiffs have not stated a CIPA claim.

IV. ORDER

Based on the foregoing, Facebook's Motion to Dismiss (Docket Item No. 44) is GRANTED as follows:

1. The withdrawn claim for violation of the CFAA is DISMISSED WITHOUT LEAVE TO AMEND.

2. The claims for invasion of privacy, intrusion upon seclusion, conversion, trespass to chattels, and for violation of the UCL, violation of the CCCL and violation of the CLRA are DISMISSED WITH LEAVE TO AMEND for lack of standing.

3. The claims for violation of the Wiretap Act, violation of the SCA and violation of CIPA are DISMISSED WITH LEAVE TO AMEND for failure to state a claim.

Facebook's request for judicial notice (Docket Item No. 45) is DENIED because this motion was resolved without relying on those documents.

Any amended complaint must be filed on or before **November 30, 2015.**

The court schedules this case for a Case Management Conference at **10:00 a.m. on January 14, 2016.** The parties shall file a Joint Case Management Conference Statement on or before **January 7, 2016.**

IT IS SO ORDERED.

Dated: October 23, 2015

EDWARD J. DAVILA
United States District Judge