APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE FACEBOOK, INC. INTERNET TRACKING LITIGATION,	No. 17-17486
PERRIN AIKENS DAVIS; BRIAN K. LENTZ; CYNTHIA D. QUINN; MATTHEW J. VICKERY, *Plaintiffs-Appellants*, v. FACEBOOK, INC., *Defendants-Appellee*.	D.C. No. 5:12-md-02314-EJD OPINION

Appeal from the United States District Court
for the Northern District of California
Edward J. Davila, District Judge, Presiding

Argued and Submitted April 16, 2019
San Francisco, California

Filed April 9, 2020

Before: Sidney R. Thomas, Chief Judge, Milan D. Smith, Jr., Circuit Judge, and Katherine H. Vratil*, District Judge.

Opinion by Chief Judge Thomas

* The Honorable Kathryn H. Vratil, United States District Judge for the District of Kansas, sitting by designation.

SUMMARY**

Standing / Privacy Law

The panel affirmed the district court's dismissal of the Stored Communications Act ("SCA"), breach of contract, and breach of implied covenant claims; reversed the dismissal of the remaining claims; and remanded for further consideration, in an action alleging privacy-related claims against Facebook, Inc.

Facebook uses plug-ins to track users' browsing histories when they visit third-party websites, and then complies these browsing histories into personal profiles which are sold to advertisers to generate revenue. Plaintiffs filed an amended complaint on behalf of themselves and a putative class of people who had active Facebook accounts between May 27, 2010 and September 26, 2011. They alleged that Facebook executives were aware of the tracking of logged-out users and recognized that these practices posed various user-privacy issues.

As an initial matter, the panel held that plaintiffs had standing to bring their claims. Specifically, the panel held that plaintiffs adequately alleged an invasion of a legally protected interest that was concrete and particularized. As to the statutory claims, the panel held that the legislative history and statutory

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

text demonstrated that Congress and the California legislature intended to protect these historical privacy rights when they passed the Wiretap Act, SCA, and the California Invasion of Privacy Act ("CIPA"). In addition, plaintiffs adequately alleged that Facebook's tracking and collection practices would cause harm or a material risk to their interest in controlling their personal information. Accordingly, plaintiffs sufficiently alleged a clear invasion of their right to privacy, and plaintiffs had standing to pursue their privacy claims under these statutes.

As to plaintiffs' alleged theories of California common law trespass to chattels and fraud, statutory larceny, and violations of the Computer Data Access and Fraud Act, the panel held that plaintiffs sufficiently alleged a state law interest whose violation constituted an injury sufficient to establish standing to bring their claims. Because California law recognizes a legal interest in unjustly earned profits, plaintiffs adequately pled an entitlement to Facebook's profits from users' data sufficient to confer Article III standing. Plaintiffs also sufficiently alleged that Facebook profited from this valuable data.

Turning to the merits, the panel held that plaintiffs adequately stated claims for relief for intrusion upon seclusion and invasion of privacy under California law. First, the panel held that in light of the privacy interests and Facebook's allegedly surreptitious and unseen data collection, plaintiffs adequately alleged a reasonable expectation of privacy to survive a Fed. R. Civ. P. 12(b)(6) motion to dismiss. Second, plaintiffs identified sufficient facts to survive a motion to dismiss on the ultimate question of whether

Facebook's tracking and collection practices could highly offend a reasonable individual.

The panel held that plaintiffs sufficiently alleged that Facebook's tracking and collection practices violated the Wiretap Act and CIPA. Both statutes contain an exemption from liability for a person who is a "party" to the communication. Noting a circuit split, the panel adopted the First and Seventh Circuits' understanding that simultaneous unknown duplication and communication of GET requests did not exempt Facebook from liability under the party exception. The panel concluded that Facebook was not exempt from liability as a matter of law under the Wiretap Act or CIPA, and did not opine whether plaintiffs adequately pleaded the other requisite elements of the statutes.

The panel held that the district court properly dismissed plaintiffs' claims under the SCA, which required plaintiffs to plead that Facebook gained unauthorized access to a "facility" where it accessed electronic communications in "electronic storage." The panel agreed with the district court's determination that plaintiffs' data was not in electronic storage. The panel concluded that plaintiffs' claims for relief under the SCA were insufficient.

The panel held that the district court properly dismissed plaintiffs' breach of contract claim for failure to state a claim. Plaintiffs alleged that Facebook entered into a contract with each plaintiff consisting of the Statement of Rights and Responsibilities, Privacy Policy, and relevant Help Center pages. The panel

held that plaintiffs failed to adequately allege the existence of a contract that was subject to breach. The panel also held that the district court properly dismissed plaintiffs' claim that Facebook's tracking practices violated the implied covenant of good faith and fair dealing, where the allegations did not go beyond the asserted breach of contract theories.

COUNSEL

David A. Straite (argued), Frederic S. Fox, and Ralph E. Labaton, Kaplan Fox & Kilsheimer LLP, New York, New York; Laurence D. King, Matthew George, and Mario M. Choi, Kaplan Fox & Kilsheimer LLP, San Francisco, California; Stephen G. Grygiel, Silverman Thompson Slutkin White LLC, Baltimore, Maryland; for Plaintiffs-Appellants.

Lauren R. Goldman (argued) and Michael Rayfield, Mayer Brown LLP, New York, New York; Matthew D. Brown, Cooley LLP, San Francisco, California; for Defendant- Appellee.

Marc Rotenberg, Alan Butler, Natasha Babazadeh, and Sam Lester, Electronic Privacy Information Center, Washington, D.C., for Amicus Curiae Electronic Privacy Information Center (EPIC).

Douglas Laycock, University of Virginia Law School, Charlottesville, Virginia; Steven W. Perlstein, Kobre & Kim LLP, New York, New York; Beau D. Barnes, Kobre & Kim LLP, Washington, D.C.; for Amicus Curiae Professor Douglas Laycock.

OPINION

THOMAS, Chief Judge:

In this appeal, we are asked to determine whether: (1) Facebook-users Perrin Davis, Brian Lentz, Cynthia Quinn, and Mathew Vickery ("Plaintiffs") have standing to allege privacy-related claims against Facebook, and (2) Plaintiffs adequately allege claims that Facebook is liable for common law and statutory privacy violations when it tracked their browsing histories after they had logged out of the Facebook application. We have jurisdiction pursuant to 28 U.S.C. § 1291. We affirm in part; reverse in part; and remand for further proceedings.

I

Facebook uses plug-ins[1] to track users' browsing histories when they visit third-party websites, and then compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue. The parties do not dispute that Facebook engaged in these tracking practices after its users had logged out of Facebook.

Facebook facilitated this practice by embedding third-party plug-ins on third-party web pages. The plug-ins, such as Facebook's "Like" button, contain bits of Facebook code. When a user visits a page that includes these plug-ins, this code is able to replicate

---

[1] A plug-in is a program that extends the functionality of an existing program, such as an internet browser.

and send the user data to Facebook through a separate, but simultaneous, channel in a manner undetectable by the user.

As relevant to this appeal, the information Facebook allegedly collected included the website's Uniform Resource Locator ("URL") that was accessed by the user. URLs both identify an internet resource and describe its location or address. "[W]hen users enter URL addresses into their web browser using the 'http' web address format, or click on hyperlinks, they are actually telling their web browsers (the client) which resources to request and where to find them. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1101 (9th Cir. 2014). Thus, the URL provides significant information regarding the user's browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it. In technical parlance, this collected URL is called a "referer header" or "referer." Facebook also allegedly collected the third-party website's Internet Protocol ("IP") address,[2] which reveals only the owner of the website.

Facebook allegedly compiled the referer headers it collected into personal user profiles using "cookies"—small text files stored on the user's device. When a user creates a Facebook account, more than ten Facebook cookies are placed on the user's browser. These cookies store the user's login ID, and they capture, collect, and compile the referrer headers from the web

---

[2] An "IP address" is a numerical identifier for each computer or network connected to the Internet. *hiQ labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 991 n.4 (9th Cir. 2019).

pages visited by the user. As most relevant to this appeal, these cookies allegedly continued to capture information after a user logged out of Facebook and visited other websites.

Plaintiffs claim that internal Facebook communications revealed that company executives were aware of the tracking of logged-out users and recognized that these practices posed various user-privacy issues. According to the Plaintiffs, Facebook stopped tracking logged-out users only after Australian blogger Nik Cubrilovic published a blog detailing Facebook's tracking practices.[3]

Plaintiffs filed a consolidated complaint on behalf of themselves and a putative class of people who had active Facebook accounts between May 27, 2010 and September 26, 2011. After the district court dismissed their first complaint with leave to amend, Plaintiffs filed an amended complaint. In the amended complaint, they alleged a number of claims. The claims relevant to this appeal consist of: (1) violation of the Wiretap Act, 18 U.S.C. § 2510, *et seq.*; (2) violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701; (3) violation of the California Invasion of Privacy Act ("CIPA"), Cal. Pen. Code §§ 631, 632; (4) invasion of privacy; (5) intrusion upon seclusion; (6) breach of contract; (7) breach of the duty of good faith

[3] The blog post quickly gained notoriety and played a role in a lawsuit that alleged multiple counts of deceptive trade practices brought against Facebook by the Federal Trade Commission. *In the Matter of Facebook Inc.*, FTC File No. 0923184. Facebook reached a settlement with the FTC in November 2011.

and fair dealing; (8) civil fraud; (9) trespass to chattels; (10) violations of California Penal Code § 502 Computer Data Access and Fraud Act ("CDAFA"); and (11) statutory larceny under California Penal Code §§ 484 and 496.

The district court granted Facebook's motion to dismiss the amended complaint. First, the district court determined that Plaintiffs had failed to show they had standing to pursue claims that included economic damages as an element, thus disposing of the claims for trespass to chattels, violations of the CDAFA, fraud, and statutory larceny. It dismissed these claims without leave to amend.

The district court also dismissed for failure to state a claim, without leave to amend, Plaintiffs' claims for violations of the Wiretap Act, CIPA, and the SCA, as well as their common law claims for invasion of privacy and intrusion upon seclusion. The district court dismissed the claims for breach of contract and the breach of the implied covenant of good faith and fair dealing, but granted leave to amend these claims. In response, Plaintiffs amended their complaint as to the breach of contract and implied covenant claims. The district court subsequently granted Facebook's motion to dismiss the amended claims. This timely appeal followed.

We review *de novo* a district court's determination of whether a party has standing. *San Luis & Delta-Mendota Water Auth. v. United States*, 672 F.3d 676, 699 (9th Cir. 2012). We review *de novo* dismissals for failure to state a claim under Rule 12(b)(6). *Dougherty v. City of Covina*, 654 F.3d 892, 897 (9th Cir. 2011).

II

The Plaintiffs have standing to bring their claims. "Where standing is raised in connection with a motion to dismiss, the court is to 'accept as true all material allegations of the complaint, and . . . construe the complaint in favor of the complaining party.'" *Levine v. Vilsack*, 587 F.3d 986, 991 (9th Cir. 2009) (quoting *Thomas v. Mundell*, 572 F.3d 756, 760 (9th Cir. 2009)).

To establish standing, a "[p]laintiff 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 redressed by a favorable judicial decision." *Spokeo v. Robins*, __ U.S. __, 136 S. Ct. 1540, 1547 (2016). To establish an injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized." *Id.* at 1548 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). A particularized injury is one that affects the plaintiff in a "personal and individual way." *Id.*; *see also Dutta v. State Farm Mutual Auto. Ins. Co.*, 895 F.3d 1166, 1173 (9th Cir. 2018).

A concrete injury is one that is "real and not abstract." *Spokeo*, 136 S.Ct. at 1548 (internal quotation marks omitted). Although an injury "must be 'real' and 'not abstract' or purely 'procedural' . . . it need not be 'tangible.'" *Dutta*, 895 F.3d at 1173. Indeed, though a bare procedural violation of a statute is insufficient to establish an injury in fact, Congress may "elevat[e] to the status of legally cognizable injuries concrete, *de*

facto injuries that were previously inadequate" to confer standing. *Spokeo*, 136 S. Ct. at 1549 (quoting *Lujan*, 504 U.S. at 578).

To determine whether Congress has done so, we ask whether: (1) "Congress enacted the statute at issue to protect a concrete interest that is akin to a historical, common law interest[,]" and (2) the alleged procedural violation caused real harm or a material risk of harm to these interests. *Dutta*, 895 F.3d at 1174.

A

The district court properly concluded that Plaintiffs had established standing to bring claims for invasion of privacy, intrusion upon seclusion, breach of contract, breach of the implied covenant of good faith and fair dealing, as well as claims under the Wiretap Act and CIPA, because they adequately alleged privacy harms.

Plaintiffs have adequately alleged an invasion of a legally protected interest that is concrete and particularized. "[V]iolations of the right to privacy have long been actionable at common law." *Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir. 2019) (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)). A right to privacy "encompass[es] the individual's control of information concerning his or her person." *Eichenberger*, 876 F.3d at 983 (quoting *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989)).

As to the statutory claims, the legislative history and statutory text demonstrate that Congress and the

California legislature intended to protect these historical privacy rights when they passed the Wiretap Act, SCA, and CIPA. *See* S. REP. NO. 99-541, at 2 (1986) ("[The Wiretap Act] is the primary law protecting the security and privacy of business and personal communications in the United States today."); *Id.* at 3 ("[The SCA] is modeled after the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. to protect privacy interests in personal and proprietary information . . . ."); Cal. Pen. Code § 630 (noting that CIPA was passed "to protect the right of privacy of the people of this state"). Thus, these statutory provisions codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing. *See Campbell v. Facebook, Inc.*, —F.3d—, 2020 WL 1023350, at *7–8 (9th Cir. Mar. 3, 2020).

Plaintiffs have adequately alleged harm to these privacy interests. Plaintiffs alleged that Facebook continued to collect their data after they had logged off the social media platform, in order to receive and compile their personally identifiable browsing history. As alleged in the complaint, this tracking occurred "no matter how sensitive" or personal users' browsing histories were. Facebook allegedly constantly compiled and updated its database with its users' browsing activities, including what they did when they were not using Facebook. According to Plaintiffs, by correlating users' browsing history with users' personal Facebook profiles—profiles that could include a user's employment history and political and religious affiliations—Facebook gained a cradle-to-grave profile without users' consent.

Here, Plaintiffs have adequately alleged that Facebook's tracking and collection practices would cause harm or a material risk of harm to their interest in controlling their personal information. As alleged, Facebook's tracking practices allow it to amass a great degree of personalized information. Facebook's user profiles would allegedly reveal an individual's likes, dislikes, interests, and habits over a significant amount of time, without affording users a meaningful opportunity to control or prevent the unauthorized exploration of their private lives.

"[A]dvances in technology can increase the potential for unreasonable intrusions into personal privacy." *Patel*, 932 F.3d at 1272. As the Third Circuit has noted, "[i]n an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion . . . that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data . . . is untenable. Nothing in *Spokeo* or any other Supreme Court decision suggests otherwise." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3rd Cir. 2019) ("*In re Google Cookie*").

Accordingly, Plaintiffs have sufficiently alleged a clear invasion of the historically recognized right to privacy. Therefore, Plaintiffs have standing to pursue their privacy claims under the Wiretap Act, SCA, and CIPA, as well as their claims for breach of contract and breach of the implied covenant of good faith and fair dealing.

B

Plaintiffs also alleged theories of California common law trespass to chattels and fraud, statutory larceny, and violations of the CDAFA. The district court dismissed these claims for lack of standing, concluding that the Plaintiffs failed to demonstrate that they had suffered the economic these claims.[4] We respectfully disagree.

Plaintiffs allege that Facebook is unjustly enriched through the use of their data. Facebook argues that unjust enrichment is not sufficient to confer standing, and that Plaintiffs must instead demonstrate that they either planned to sell their data, or that their data was made less valuable through Facebook's use. They similarly assert that Plaintiffs' entitlement to damages does not constitute an injury for purposes of standing.

However, "state law can create interests that support standing in federal courts." *Cantrell v. City of Long Beach*, 241 F.3d 674, 684 (9th Cir. 2001). As relevant here, California law recognizes a right to dis-

---

[4] To prevail on a claim for trespass to chattels, Plaintiffs must demonstrate that some actual injury may have occurred and that the owner of the property at issue may only recover the actual damages suffered as a result of the defendant's actions. *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1351–52 (2003). Fraud similarly requires damages, *Beckwith v. Dahl*, 205 Cal. App. 4th 1039, 1064 (2012), as does a violation of the CDAFA, *Mintz v. Mark Bartelstein & Assocs.*, 906 F. Supp. 2d 1017, 1032 (C.D. Cal. 2012) (noting that "[u]nder the plain language of the statute[,]" damages must be established). Damages is an inherent element of larceny.

gorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss. *See Cty. of San Bernardino v. Walsh*, 158 Cal. App. 4th 533, 542 (2007) (noting that where "a benefit has been received by the defendant but the plaintiff has not suffered a corresponding loss, or in some cases, any loss, but nevertheless the enrichment of the defendant would be unjust . . . [t]he defendant may be under a duty to give to the plaintiff the amount by which [the defendant] has been enriched" (quoting Rest., Restitution, § 1, com. e)); *see also Ghirardo v. Antonioli*, 14 Cal. 4th 39, 51 (1996) ("Under the law of restitution, an individual may be required to make restitution if he is unjustly enriched at the expense of another.").

In other words, California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable. *See, e.g.*, *CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860–61 (2006) (holding that a woman whose identity was stolen and used to obtain later-foreclosed-upon property was entitled to surplus funds from the sale at auction because "she was entitled to the product of identity theft"); *Ward v. Taggert*, 51 Cal. 2d 736, 742–43 (1959) (holding that plaintiffs could recover profits unjustly realized by a real estate agent who misrepresented the purchase price of real estate, even though the plaintiffs did not pay more than the land was worth when they purchased it); *cf. Walsh*, 158 Cal. App. 4th at 542–43 (holding that the district court did not err

where it solely relied on profit to the defendants rather than loss to the plaintiffs to calculate damages).

"The 'gist of the question of standing' is whether the plaintiff has a sufficiently 'personal stake in the outcome of the controversy.'" *Washington v. Trump*, 847 F.3d 1151, 1159 (9th Cir. 2017) (quoting *Massachusetts v. EPA*, 549 U.S. 497, 517 (2007)). Because California law recognizes that individuals maintain an entitlement to unjustly earned profits, to establish standing, Plaintiffs must allege they retain a stake in the profits garnered from their personal browsing histories because "the circumstances are such that, as between the two [parties], it is *unjust* for [Facebook] to retain it." *McBride v. Boughton*, 123 Cal. App. 4th 379, 389 (2004) (emphasis in original) (quoting *First Nationwide Savings v. Perry*, 11 Cal. App. 4th 1657, 1662 (1992)). Under California law, this stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable.

Because California law recognizes a legal interest in unjustly earned profits, Plaintiffs have adequately pleaded an entitlement to Facebook's profits from users' personal data sufficient to confer Article III standing. Plaintiffs allege that their browsing histories carry financial value. They point to the existence of a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories.

Plaintiffs also sufficiently allege that Facebook profited from this valuable data. According to the complaint, Facebook sold user data to advertisers in

order to generate revenue. Indeed, as alleged, Facebook's ad sales constituted over 90% of the social media platform's revenue during the relevant period of logged-out user tracking.

Plaintiffs' allegations are sufficient at the pleading stage to demonstrate that these profits were unjustly earned. As stated in the complaint, "despite Facebook's false guarantee to the contrary," the platform "charges users by acquiring the users' sensitive and valuable personal information" and selling it to advertisers for a profit. Plaintiffs allegedly did not provide authorization for the use of their personal information, nor did they have any control over its use to produce revenue. This unauthorized use of their information for profit would entitle Plaintiffs to profits unjustly earned.

Thus, Plaintiffs sufficiently alleged a state law interest whose violation constitutes an injury sufficient to establish standing to bring their claims for CDAFA violations and California common law trespass to chattels, fraud, and statutory larceny.

III

Plaintiffs adequately stated claims for relief for invasion of privacy, intrusion upon seclusion, breach of contract, breach of the implied covenant of good faith and fair dealing, as well as their claims under the Wiretap Act and CIPA. In order to survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), the facts alleged must "plausibly give rise to an entitlement to relief." *Dougherty*, 654 F.3d at 897 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009)). At the pleading stage, all allegations of material fact

are taken as true and construed in the light most favorable to the nonmoving party. *Id.*

A

Plaintiffs adequately stated claims for relief for intrusion upon seclusion and invasion of privacy under California law. To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead that (1) a defendant "intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]" and (2) the intrusion "occur[red] in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009).

A claim for invasion of privacy under the California Constitution involves similar elements. Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is "so serious . . . as to constitute an egregious breach of the social norms" such that the breach is "highly offensive." *Id.* at 287.

Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive. *Id.* We address both in turn.

1

The existence of a reasonable expectation of privacy, given the circumstances of each case, is a mixed question of law and fact. *Hill v. NCAA*, 7 Cal. 4th 1,

40 (1994). "[M]ixed questions of fact and law are reviewed de novo, unless the mixed question is primarily factual." *N.B. v. Hellgate Elem. Sch. Dist., ex rel. Bd. of Dirs., Missoula Cty., Mont.*, 541 F.3d 1202, 1207 (9th Cir. 2008). Here, because we are reviewing the district court's legal conclusions, we review *de novo*.

We first consider whether a defendant gained "unwanted access to data by electronic or other covert means, in violation of the law or social norms." *Hernandez*, 47 Cal. 4th at 286 (internal quotation marks omitted). To make this determination, courts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities. *Hill*, 7 Cal. 4th at 36.

Thus, the relevant question here is whether a user would reasonably expect that Facebook would have access to the user's individual data after the user logged out of the application. Facebook's privacy disclosures at the time allegedly failed to acknowledge its tracking of logged-out users, suggesting that users' information would not be tracked.

The applicable Facebook Statement of Rights and Responsibilities ("SRR") stated:

> Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to make informed decisions.

SRR, dated April 26, 2011.

Facebook's applicable Data Use Policy,[5] in turn, stated:

> We receive data whenever you visit a game, application, or website that uses [Facebook's services]. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, *if you are logged in to Facebook,* your user ID.

Data Use Policy, dated September 7, 2011 (emphasis added).

Finally, Facebook's "Help Center" at the time included answers to questions related to data tracking. Most relevantly, one answer from a Help Center page at the time answered the question "[w]hat information does Facebook receive about me when I visit a website with a Facebook social plug in?"[6] The Help Center page first stated that Facebook collected the date and time of the visit, the referrer URL, and other technical information. It continued, "[i]f you are logged into Facebook, we also see your user ID number and email address. . . . If you log out of Facebook,

---

[5] This policy was originally titled "Privacy Policy." During the class period, its title was changed to "Data Use Policy."

[6] Facebook disputes that some of the Help Center pages Plaintiffs attached to their complaint were dated during the class period. It does not dispute, however, that this particular Help Center page fell within the class period.

we will not receive this information about partner websites but you will also not see personalized experiences on these sites."

Plaintiffs have plausibly alleged that an individual reading Facebook's promise to "make important privacy disclosures" could have reasonably concluded that the basics of Facebook's tracking—when, why, and how it tracks user information—would be provided. Plaintiffs have plausibly alleged that, upon reading Facebook's statements in the applicable Data Use Policy, a user might assume that only logged-in user data would be collected. Plaintiffs have alleged that the applicable Help Center page affirmatively stated that logged-out user data would not be collected. Thus, Plaintiffs have plausibly alleged that Facebook set an expectation that logged-out user data would not be collected, but then collected it anyway.

In addition, the amount of data allegedly collected was significant. Plaintiffs allege that "[n]o matter how sensitive the website, the referral URL is acquired by Facebook along with the cookies that precisely identify the [logged-out] user" and that Facebook acquires an "enormous amount of individualized data" through its use of cookies on the countless websites that incorporate Facebook plug-ins. That this amount of information can be easily collected without user knowledge is similarly significant. Plaintiffs have plausibly alleged that Facebook did not disclose that the cookies would continue to track users' browsing history after they log out of the platform. Nor did it disclose the extent of information collected.

In light of the privacy interests and Facebook's allegedly surreptitious and unseen data collection, Plaintiffs have adequately alleged a reasonable expectation of privacy. Case law supports this determination. In *In re Google Cookie*—where the Third Circuit similarly interpreted California Law—the court held that users maintained a reasonable expectation of privacy in their browsing histories when Google tracked URLs after the users denied consent for such tracking. 806 F.3d at 129, 151; *see also In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 293–94 (3d Cir. 2016) ("*In re Nickelodeon*") (holding, under analogous New Jersey law, that a reasonable expectation of privacy existed when Nickelodeon promised users that it would not collect information from website users, but then did). That users in those cases explicitly denied consent does not render those cases distinguishable from the instant case, given Facebook's affirmative statements that it would not receive information from third-party websites after users had logged out. Indeed, in those cases, the critical fact was that the online entity represented to the plaintiffs that their information would not be collected, but then proceeded to collect it anyway.

The nature of the allegedly collected data is also important. Plaintiffs allege that Facebook obtained a comprehensive browsing history of an individual, no matter how sensitive the websites visited, and then correlated that history with the time of day and other user actions on the websites visited. This process, according to Plaintiffs, resulted in Facebook's acquiring "an enormous amount of individualized data" to compile a "vast repository of personal data."

Facebook argues that Plaintiffs need to identify specific, sensitive information that Facebook collected, and that their more general allegation that Facebook acquired "an enormous amount of individualized data" is insufficient. However, *both* the nature of collection and the sensitivity of the collected information are important. The question is not necessarily whether Plaintiffs maintained a reasonable expectation of privacy in the information in and of itself. Rather, we must examine whether the data itself is sensitive *and* whether the manner it was collected—after users had logged out—violates social norms.

When we consider the sensitivity of that data, moreover, we conclude there remain material questions of fact as to whether a reasonable individual would find the information collected from the seven million websites that employ Facebook plug-ins "sensitive and confidential." *Hill*, 7 Cal. 4th at 35. "Technological advances[,]" such as Facebook's use of cookies to track and compile internet browsing histories, "provide 'access to a category of information otherwise unknowable' and 'implicate privacy concerns' in a manner different from traditional intrusions as a 'ride on horseback' is different from 'a flight to the moon.'" *Patel*, 932 F.3d at 1273 (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)). Thus, viewing the allegations in the light most favorable to Plaintiffs, as we must at this stage, the allegations that Facebook allegedly compiled highly personalized profiles from sensitive browsing histories and habits prevent us

from concluding that the Plaintiffs have no reasonable expectation of privacy.[7]

Contrary to Facebook's arguments, this case can also be distinguished from *Forrester* and *Zynga* as it relates to an analysis of a reasonable expectation of privacy. *Forrester*, 512 F.3d 500; *Zynga*, 750 F.3d 1098. In *Forrester*, we considered whether the individuals had a reasonable expectation of privacy in "the

---

[7] Analogous cases decided in the Fourth Amendment context support a conclusion that the breadth of information allegedly collected would violate community norms. These cases hold that individuals have a reasonable expectation of privacy in collections of information that reveal "familiar, political, professional, religious, and sexual associations." *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (holding that individuals have a reasonable expectation of privacy in long-term location tracking data under the Fourth Amendment because it reveals all-encompassing information); *Riley*, 573 U.S. at 397–99 (holding that individuals have a reasonable expectation of privacy in the contents of their cell phones under the Fourth Amendment due to the large amount of personal data stored therein); *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (noting that, in a Fourth Amendment search context, URLs may be particularly sensitive because they "identif[y] the particular document within a website that a person views and thus reveals much more information about the person's Internet activity"). We acknowledge that the Fourth Amendment imposes higher standards on the government than those on private, civil litigants. *Carpenter*, 138 S. Ct. at 2213–14. But we have nonetheless found analogies to Fourth Amendment cases applicable when deciding issues of privacy related to technology. *See Patel*, 932 F.3d at 1272–73. And, viewed broadly, these cases stand for the proposition that individuals maintain the expectation that entities will not be able to collect such broad swaths of personal information absent consent.

to/from addresses of their messages or the IP addresses of the websites they visit." 512 F.3d at 510. Concluding that users did not maintain a reasonable expectation of privacy in such information, we determined that users "should know that this information is provided to and used by Internet service providers for the specific purposes of directing the routing information." *Id.* But, in a footnote, we went on to distinguish the IP addresses collected in *Forrester* from the collection of URLs, which we stated "might be more constitutionally problematic," explaining that, "[a] URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the per son's Internet activity." *Id.* at n.6.

In *Zynga*, the plaintiffs relied on this footnote to argue that they maintained a reasonable expectation of privacy in the URLs of gaming websites collected without their knowledge and disclosed to third parties by Zynga (a gaming platform) and Facebook. 750 F.3d at 1108–09. The *Zynga* plaintiffs alleged that users would log in to their Facebook account and "then click on the Zynga game icon within the Facebook interface." *Id.* at 1102. Facebook and Zynga would then collect a referer header containing the URL for the Zynga game, after which the Zynga server would load the game in a small frame embedded on the Facebook website. *Id.* According to the *Zynga* plaintiffs, "Zynga programmed its gaming applications to collect the information provided in the referer header, and then transmit this information to advertisers and other third parties." *Id.* This information included "the user's Facebook ID and the address of the Facebook

webpage the user was viewing when the user clicked the link." *Id.* at 1102.

In *Zynga*, we concluded that the collected information was not problematic because it differed from the URLs containing sensitive information alluded to in *Forrester*'s footnote. We determined that "[i]nformation about the address of the Facebook webpage the user was viewing is distinguishable from the sort of communication involving a search engine discussed in *Forrester*." *Id.* at 1108. We then continued to say that "a Google search URL not only shows that a user is using the Google search engine, but also shows the specific search terms the user had communicated to Google." *Id.* We continued, "the referer header information at issue here includes only basic identification and address information, not a search term or similar communication made by the user." *Id.* at 1108–09.

Here, Plaintiffs allege that Facebook collects a full-string detailed URL, which contains the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested. Their complaint notes that a user might type a search term into Google's search engine, which would return a link to an article relevant to the search term. According to Plaintiffs, when the user clicks the link, a communication is created that contains a "GET request and the full-string detailed URL." They allege that Facebook collected this communication, including the "full referral URL (including the exact subpage of the precise items being purchased)" and that Facebook then "correlates that URL with the user ID, time stamp, browser settings and even the type of browser used."

In sum, Plaintiffs allege that a Google search could generate links that include full-string, detailed URLs that Facebook then collected. Thus, they have sufficiently alleged that the collected URLs in this case are distinct from IP addresses collected in *Forrester*, as well as the URLs collected in *Zynga*. The URLs, by virtue of including "the particular document within a website that a person views" reveal "much more information" than the IP addresses collected in *Forrester*. 512 F.3d at 510 n.6. Unlike the URLs in *Zynga*, which revealed only that a Facebook user had clicked on a link to a gaming website, Plaintiffs allege that the URLs in the instant case could emanate from search terms inputted into a third-party search engine. These terms and the resulting URLs could divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's platform.

Moreover, the users in *Zynga* clicked on links to the gaming websites *after* they had logged into their Facebook user accounts. *Zynga*, 750 F.3d at 1102. Then, the linked material appeared within the Facebook interface. *Id.* Here, in contrast, Plaintiffs allege that users were not logged in to the website, making it impossible for the linked material to be viewed within Facebook's interface.

The fact that users could have taken additional measures to prevent cookies from tracking their browsing, as Facebook asserts, is not relevant at the pleading stage. This is a factbased defense to be developed and asserted at a later stage of the litigation. And Plaintiffs have alleged that these protections

would not have done any good, even if users had employed them. Specifically, they allege that Facebook would "hack its way past data protection software" to "bypass[] security settings for the purpose of gathering intelligence" on the users' real-time searches, and similarly, with respect to a subclass of individuals who used the Internet Explorer browser, that Facebook fraudulently maintained that it employed a protocol that would result in its tracking being automatically blocked by the browser. These issues cannot be resolved at the pleading stage.

In sum, Plaintiffs have sufficiently pleaded a reasonable expectation of privacy to survive a Rule 12(b)(6) motion to dismiss.

2

However, in order to maintain a California common law privacy action, "[p]laintiffs must show more than an intrusion upon reasonable privacy expectations. Actionable invasions of privacy also must be 'highly offensive' to a reasonable person, and 'sufficiently serious' and unwarranted so as to constitute an 'egregious breach of the social norms.'" *Hernandez*, 47 Cal. 4th at 295. Determining whether a defendant's actions were "highly offensive to a reasonable person" requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive. *Id.* at 287; *see also Hill*, 7 Cal. 4th at 25–26. While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the

highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy. *Hernandez*, 47 Cal. 4th at 287 (noting that highly offensive analysis "essentially involves a 'policy' determination as to whether the alleged intrusion is highly offensive under the particular circumstances").

The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage. Plaintiffs have identified sufficient facts to survive a motion to dismiss. Plaintiffs' allegations of surreptitious data collection when individuals were not using Facebook are sufficient to survive a dismissal motion on the issue. Indeed, Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue.

In sum, Plaintiffs have sufficiently pleaded the "reasonable expectation of privacy" and "highly offensive" elements necessary to state a claim for intrusion upon seclusion and invasion of privacy to survive a 12(b)(6) motion to dismiss.[8]

---

[8] The non-precedential cases cited by Facebook do not compel the opposite conclusion. For instance, in *In re Google, Inc. Privacy Policy Litig.*, the Northern District of California found no highly offensive conduct when Plaintiffs alleged that Google surreptitiously tracked their browsing data while using Google's services. 58 F. Supp. 3d 968, 987–88 (N.D. Cal. 2014). Here, on the other hand, Plaintiffs had logged out and were not using Facebook when Facebook tracked them. The same is true in *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1016–18 (N.D. Cal. 2012)

B

Plaintiffs also have sufficiently alleged that Facebook's tracking and collection practices violated the Wiretap Act and CIPA.

1

The Wiretap Act prohibits the unauthorized "interception" of an "electronic communication." 18 U.S.C. § 2511(1)(a)–(e). Similarly, CIPA prohibits any person from using electronic means to "learn the contents or meaning" of any "communication" "without consent" or in an "unauthorized manner." Cal. Pen. Code § 631(a). Both statutes contain an exemption from liability for a person who is a "party" to the communication, whether acting under the color of law or not. 18 U.S.C. § 2511(2)(c), (d); *see Warden v. Kahn*, 160 Cal. Rptr. 471, 475 (1979) ("[S]ection 631 . . . has been held to apply only to eavesdropping by a third party and not to recording by a participant to a conversation."). Courts perform the same analysis for both the Wiretap Act and CIPA regarding the party exemption. *See, e.g.*, *In re Google Cookie*, 806 F.3d at 152 (holding that CIPA claims could be dismissed because the parties were exempted from liability under the Wiretap Act's party exception).

The party exception must be considered in the technical context of this case. When an individual internet user visits a web page, his or her browser sends

---

and *In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1049–50 (N.D. Cal. 2012). In those cases, there were likewise no allegations that the defendants tracked the plaintiffs after the plaintiffs stopped using the defendant's services.

a message called a "GET request" to the web page's server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The GET request also transmits a referer header containing the personally-identifiable URL information. Typically, this communication occurs only between the user's web browser and the third-party website. On websites with Facebook plug-ins, however, Facebook's code directs the user's browser to copy the referer header from the GET request and then send a separate but identical GET request and its associated referer header to Facebook's server. It is through this duplication and collection of GET requests that Facebook compiles users' browsing histories.

The Wiretap Act does not define the term "party" in its liability exemption, and the other circuit courts that have considered the Act's scope have interpreted the term in different ways. The First and Seventh Circuits have implicitly assumed that entities that surreptitiously duplicate transmissions between two parties are not parties to communications within the meaning of the Act. In *In re Pharmatrak, Inc. Privacy Litig.*, the First Circuit considered whether the defendant could face liability under the Wiretap Act when it employed software that "automatically duplicated part of the communication between a user and a [third-party website] and sent this information to [the defendant]." 329 F.3d 9, 22 (1st Cir. 2003). The First Circuit rejected the defendant's argument that "there was no interception because 'there were always two separate communications: one between the Web

user and the [third-party website], and the other between the Web user and [the defendant].'" *Id.* Noting that the defendant "acquired the same URL . . . exchanged as a part of the communication between the [third-party website] and the user," it determined that the defendant's acquisition constituted an interception and could still render it liable. *Id.*

In *United States v. Szymuszkiewicz*, the Seventh Circuit reached a similar conclusion. 622 F.3d 701 (7th Cir. 2010). In that case, the Seventh Circuit considered whether a defendant violated the Wiretap Act when he employed a software that instructed his employer's email to duplicate and forward all emails the employer received to the defendant's own inbox. *Id.* at 703. The court determined that, because the copies were sent contemporaneously with the original emails, the defendant had intercepted the communications and could be held liable. *Id.* at 706.

However, the Third Circuit has held to the contrary. In *In re Google Cookie*, the court considered whether internet advertising companies were parties to a communication when they placed cookie blockers on web-users' browsers to facilitate online advertisements. 806 F.3d at 143. As in the instant case, the users sent GET requests to third-party websites and upon receipt, the website would duplicate the GET request and send it to the defendants. *Id.* at 140. The Third Circuit concluded that the defendants were "the intended recipients" of the duplicated GET requests, and thus "were parties to the transmissions at issue."

Id. at 143; *see also In re Nickelodeon*, 827 F.3d at 275–76 (citing *In re Google Cookie* for the same).[9]

We adopt the First and Seventh Circuits' understanding that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception. As we have previously held, the "paramount objective of the [Electronic Communications Privacy Act, which amended the Wiretap Act] is to protect effectively the privacy of communications." *Joffe v. Google*, 746 F.3d 920, 931 (9th Cir. 2013). We also recognize that the Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or "an unseen auditor." *See* S. REP. NO. 90-1097, *reprinted in* 1986 U.S.C.C.A.N. 2112, 2154, 2182. Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule.

Therefore, we conclude that Facebook is not exempt from liability as a matter of law under the Wiretap Act or CIPA as a party to the communication. We do not opine whether the Plaintiffs adequately

---

[9] In *Konop v. Hawaiian Airlines, Inc.*, we adopted a definition of "intercept" that encompassed both an "acquisition contemporaneous with transmission" and an act requiring a party to "stop, seize, or interrupt in progress or course before arrival." 302 F.3d 868, 878 (9th Cir. 2002). In that case, however, we considered whether items viewed on a private website were intercepted, in violation of the Wiretap Act, not plug-ins that duplicated and sent GET requests, as we consider here.

pleaded the other requisite elements of the statutes, as those issues are not presented on appeal.

C

The district court properly dismissed Plaintiffs' SCA claims. The SCA requires Plaintiffs to plead that Facebook (1) gained unauthorized access to a "facility" where it (2) accessed an electronic communication in "electronic storage." 18 U.S.C. § 2701(a).

Electronic storage is defined as either the "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

Plaintiffs allege that "[w]eb-browsers store a copy of the Plaintiffs' URL requests in the toolbar while the user remains present at a particular webpage," and that this storage is incidental to the electronic communication because once "the user hits the Enter button or clicks on a link, the communication is in the process of being sent and received between the user and the first-party website." Plaintiffs similarly assert that their browsing history—a record of previously viewed websites—serves purposes of "backup protection" of such communications. In short, Plaintiffs allege that the URL is in "electronic storage" in the toolbar during the split-second that it takes to complete a search. In Plaintiffs' view, because Facebook duplicates the URL and sends it to its servers during that split second, it accesses the URL while it is in this "electronic storage."

The district court considered the GET requests that Facebook duplicated and forwarded to its servers as wholly separate from the copy of the URL displayed in the search toolbar. Because the copy in the toolbar was not stored "incident to transmission" but was only present for the user's convenience, the district court determined that the Plaintiffs' data was not in electronic storage.

We agree. The communications in question—the GET requests themselves—are not the communications stored in the user's toolbar. Rather, the GET requests are sent directly between the user and the third-party website. The text displayed in the toolbar serves only as a visual indication—a means of informing the user—of the location of their browser. Thus, the URL's appearance in the toolbar is not "incidental" to the transmission of the URL or GET request.

What is more, Plaintiffs' interpretation of the SCA would stretch its application beyond its limits. True, the SCA's legislative history suggests that Congress intended the term "electronic storage" to be broadly construed, and not limited to "particular mediums, forms, or locations." *Hately v. Watts*, 917 F.3d 770, 786 (4th Cir. 2019) (citing H.R. REP., NO. 99- 647, at 39 (1986)). Nonetheless, the text and legislative history of the SCA demonstrate that its 1986 enactment was driven by congressional desire to protect third-party entities that stored information on behalf of users. *See id.* at 782 (noting that the SCA was enacted to protect against illicit access to stored communications in "remote computing operations and large data banks that stored emails"). Since then, the SCA has

typically only been found to apply in cases involving a centralized data-management entity; for instance, to protect servers that stored emails for significant periods of time between their being sent and their recipients' reading them. *See id.* at 798 (considering whether a web-based email service "stored" emails); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (considering whether emails stored by an internet service provider fell under the statute's purview). Here, the allegations, even construed in the light most favorable to Plaintiffs, do not show that the communications were even in "storage," much less that the alleged "storage" within a URL toolbar falls within the SCA's intended scope.

Plaintiffs alternatively argue that their browsing histories are stored for "purposes of back-up" and thus satisfy the SCA's electronic storage definition. Plaintiffs note that, in *Theofel*, we held that a copy of information stored on a user's computer "in the event that the user needs to download it again" constituted storage for backup purposes. 359 F.3d at 1075. In this case, however, the browsing histories are not composed of the actual communications sent between the individuals—rather, the browsing histories are merely a record of URLs visited. Thus, Plaintiffs' claims for relief under the SCA are insufficient, and the district court correctly dismissed them.[10]

---

[10] Because we hold that the URLs are not in electronic storage, we need not decide whether Plaintiffs sufficiently allege that their personal computers, web browsers, and browser managed files are "facilities," through which electronic communications service providers operate.

D

The district court also properly held that the Plaintiffs have not stated a breach of contract claim. In order to establish a contract breach, Plaintiffs must allege: (1) the existence of a contract with Facebook, (2) their performance under that contract, (3) Facebook breached that contract, and (4) they suffered damages. *Oasis West Realty, LLC v. Goldman*, 51 Cal. 4th 811, 821 (2011).

Plaintiffs allege that Facebook entered into a contract with each Plaintiff consisting of the SRR, Privacy Policy, and relevant Help Center pages. The parties agree that the SRR constitutes a contract. In their third amended complaint, Plaintiffs attached the SRR that was last revised April 26, 2011. This document states "[y]our privacy is very important to us" and "[w]e encourage you to read the Privacy Policy, and to use it to help make informed decisions." But this document does not contain an explicit promise not to track logged-out users. For that allegation, Plaintiffs instead rely on language from the Data Use Policy and the Help Center pages.

To properly incorporate another document, the document "need not recite that it incorporates another document, so long as it guide[s] the reader to the incorporated document." *Shaw v. Regents of the Univ. of Cal.*, 58 Cal. App. 4th 44, 54 (1997) (internal quotations and citations omitted). During the class period, Facebook changed the title of its "Privacy Policy" to "Data Use Policy" and made adjustments to its content. Although the relevant SRR directs readers to the Privacy Policy, Plaintiffs rely on the latest version

of this document, titled "Data Use Policy," last revised September 7, 2011. The attached SRR does not reference a Data Use Policy and thus, it does not guide the reader to the incorporated document on which Plaintiffs rely. As such, as a matter of law, any promise not to track logged-out users therein was not incorporated.

On appeal, Plaintiffs argue that the Data Use Policy constitutes an additional agreement separate from the SRR. Plaintiffs support this allegation with text from the September 2011 Data Use Policy, which states that, were Facebook to transfer ownership, the new owner would "still have to honor the commitments we have made in this privacy policy," and the December 2010 Privacy Policy, which states "[b]y using or accessing Facebook, you agree to our privacy practices outlined here."

First, the December 2010 Privacy Policy does not contain any agreement that Facebook would not track logged-out user data.[11] Second, and more generally, the Privacy and Data Use Policies do not outline shared commitments to which users must abide. For a contract to exist, there must be an exchange for a promise. *Steiner v. Thexton*, 48 Cal. 4th 411, 421 (2010). The 2011 Data Use Policy does not contain any

[11] The December 2010 Privacy Policy states: "If you log out of Facebook before visiting a pre-approved application or website, it will not be able to access your information." This statement merely provides that the third-party websites will not receive a user's information. It does not make any promises regarding Facebook's receipt of data.

exchange. To illustrate, while the SRR outlines commitments to which both Facebook and users agree (for example, users agree not to "send or otherwise post unauthorized commercial communications" on Facebook, while Facebook promises to "provide . . . tools to help you protect your property rights"), the 2011 Data Use Policy merely provides information—not commitments—regarding Facebook's use of information and how users can control that information (for example, it states that "[y]our information is the information that's required when you sign up for the site"). Plaintiffs' reliance on one use of the term "commitment" within this document cannot overcome the fact that the document does not require the user to make any commitment. Thus, the Data Use Policy does not constitute a separate contract. Because Plaintiffs have failed to allege adequately the existence of a contract that was subject to breach, we affirm the district court's dismissal of their breach of contract claim.

Plaintiffs also alleged that Facebook's tracking practices violated the implied covenant of good faith and fair dealing. However, as pleaded, the allegations did not go beyond the breach of contract theories asserted by Plaintiffs and were thus properly dismissed. *Carau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App.3d 1371, 1395 (1990).

IV

In sum, we conclude that Plaintiffs have standing to assert their claims. We affirm the district court's dismissal of the SCA, breach of contract, and breach of implied covenant claims. We conclude that Plaintiffs adequately pleaded their remaining claims at

this early stage to survive a motion to dismiss under Rule 12(b)(6). We remand these issues to the district court for further consideration. We do not reach any other issue argued by the parties, leaving those issues for consideration by the district court in the first instance. All pending motions are denied as moot. The parties shall bear their own costs.

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED.

APPENDIX B

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. 162

Plaintiffs' third amended complaint alleges that Defendant Facebook, Inc. violated its contractual obligations by tracking logged-out Facebook users on third-party websites. Facebook now moves to dismiss for the third time. Facebook's motion will be granted.

I. BACKGROUND

In this putative class action, Plaintiffs allege that Facebook improperly tracked the web browsing activity of logged-out Facebook users on third-party websites.[1] Third Am. Compl. ("TAC"), Dkt. No. 157. Plaintiffs previously asserted a variety of common law claims and claims for violations of federal and state statutes. After two rounds of motions to dismiss, this Court dismissed the majority of Plaintiffs' claims with

[1] For a more detailed discussion of Plaintiffs' factual allegations, see this Court's orders granting Facebook's motion to dismiss Plaintiffs' first amended complaint (Dkt. No. 87 at 2–6) and Facebook's motion to dismiss Plaintiffs' second amended complaint (Dkt. No. 148 at 1–3).

prejudice for lack of standing and for failure to state a claim. Order Granting Def.'s Mot. to Dismiss ("MTD Order"), Dkt. No. 148. This Court granted leave to amend only as to Plaintiffs' claims for breach of contract and breach of the duty of good faith and fair dealing. Id. Plaintiffs timely filed their third amended complaint. Facebook now moves to dismiss under Fed. R. Civ. P. 12(b)(6) and 15(c). Def.'s Mot. to Dismiss ("MTD"), Dkt. No. 162.

II. LEGAL STANDARD

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

Plaintiffs' TAC asserts causes of action for (1) breach of contract (TAC ¶¶ 139–48) and (2) breach of the duty of good faith and fair dealing (TAC ¶¶ 149–61). Plaintiffs also seek to enlarge the scope of the proposed class.

A. Breach of Contract

Plaintiffs allege that each of them entered into a contract with Facebook that consisted of (1) Facebook's Statement of Rights and Responsibilities ("SRR"), (2) Facebook's Privacy Policy, and (3) relevant pages from Facebook's Help Center. TAC ¶ 140. According to Plaintiffs, Facebook promised in the contract that it would not track the web browsing activity of logged-out Facebook users on third-party websites. Id. ¶ 142. Plaintiffs allege that Facebook broke that promise by collecting data about logged-out users' browsing activity and using cookies to connect that activity to users' identities. Id.

To state a claim for breach of contract, Plaintiffs must allege that (1) they entered into a contract with Facebook, (2) Plaintiffs performed or were excused from performance under the contract, (3) Facebook breached the contract, and (4) Plaintiffs suffered damages from the breach. Oasis W. Realty, LLC. v. Goldman, 51 Cal. 4th 811, 821 (2011) (citing Reichert v. General Ins. Co., 68 Cal. 2d 822, 830 (1968)). "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).

The parties agree that the SRR constitutes a contract. MTD 8; Pls.' Opp'n to Def.'s Mot. to Dismiss ("Opp'n"), Dkt. No. 163. However, the SRR itself does not contain a promise to not track logged-out users. Rather, Plaintiffs argue that the operative contract is

a combination of provisions from Facebook's SRR, Facebook's Privacy Policy,[2] and Facebook's Help Center pages.[3]

i. The Data Use Policy was not incorporated by reference into the Statement of Rights and Responsibilities.

Plaintiffs cite the following language from Facebook's Data Use Policy (dated September 7, 2011):

> We receive data whenever you visit a . . . site with a Facebook feature (such as a social plugin). This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, <u>if you are logged in to Facebook, your User ID</u>.

TAC ¶ 60 (emphasis added). Plaintiffs argue that this language "implicitly promises to the average user

---

[2] During the alleged class period, Facebook changed the title of this document from "Privacy Policy" to "Data Use Policy." Opp'n 4 n.4. As discussed below, Facebook also changed the substance of the document. In this order, unless otherwise indicated, the term "Privacy Policy" refers to both the Privacy Policy and the Data Use Policy.

[3] Plaintiffs' statement of their cause of action for breach of contract does not identify the specific contractual language that Facebook allegedly breached. TAC ¶¶ 139–48. However, Plaintiffs identify specific contractual language in their brief in opposition to Facebook's motion to dismiss. Opp'n 4 (citing factual allegations in the TAC at ¶¶ 24, 57, 60, and 62–67).

that Facebook will not receive [a user-identifying] cookie when the user is not logged in." Id.

Plaintiffs argue that this version of the Data Use Policy is part of the contract because it was incorporated by reference into the SRR. Opp'n 4–5. Under California law, for the terms of another document to be incorporated by reference into an executed document, "the reference must be (1) clear and unequivocal, the (2) reference must be called to the attention of the other party and he must consent thereto, and (3) the terms of the incorporated document must be known or easily available to the contracting parties." Woods, 2011 WL 3501403, at *3 (quoting Troyk v. Farmers Grp., Inc., 171 Cal. App. 4th 1305, 1331 (2009)).

Here, Plaintiffs argue that the Privacy Policy was incorporated by reference into the SRR because of the following language in the SRR:

> Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and 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.

TAC ¶¶ 24, 57.[4] According to Plaintiffs, this language means that the Privacy Policy is incorporated by ref-

[4] Plaintiffs' opposition brief quotes additional language from the SRR that is not cited in the TAC: "You may also want to review

erence into the SRR because the "SRR expressly refers to the Privacy Policy, says that the Policy is important, links to that Policy and tells users to read it to make important decisions about their privacy." Opp'n 5.

Plaintiffs' complaint cites four versions of Facebook's SRR, dated April 22, 2010 (TAC Ex. A), August 25, 2010 (TAC Ex. B), October 4, 2010 (TAC Ex. C), and April 26, 2011 (TAC Ex. D). TAC ¶¶ 19–20. The excerpt quoted above appears in all four versions of the SRR.

As discussed above, Plaintiffs argue that Facebook's Data Use Policy promised that Facebook would not track logged-out users. However, the version of the Data Use Policy that contains this language was not published until September 7, 2011—more than four months after the latest version of the SRR (dated April 26, 2011) that Plaintiffs attach to their complaint. See TAC Ex. D (attaching the April 26, 2011, version of the SRR), Ex. H (attaching the September 7, 2011, version of the Data Use Policy). Earlier versions of the Privacy Policy did not contain the language that Plaintiffs allege constitutes a promise not to track logged-out users. Compare id. Ex. H (attaching the September 7, 2011, version of the Data Use Policy, which states that Facebook "receive[s] data whenever you visit a . . . site with a Facebook feature (such as a social plugin) . . . . [including], if you are logged in to Facebook, your User ID") (emphasis

---

the following documents: Privacy Policy: the Privacy Policy is designed to help you understand how we collect and use information." Opp'n 5.

added), with id. Ex. E (attaching the April 22, 2010, version of the Privacy Policy), Ex. F (attaching the October 5, 2010, version of the Privacy Policy), and Ex. G (attaching the December 22, 2010, version of the Privacy Policy).

As Facebook points out, the SRR does not use the term "Data Use Policy" and does not contain any other references to the Data Use Policy. MTD 11–12. Nor could it, since the Data Use Policy Plaintiffs cite and rely on did not exist until several months after Facebook published the most recent version of its SRR that Plaintiffs attach to their complaint. Plaintiffs do not address this deficiency in their opposition brief. Compare MTD 11–12 (noting that the Data Use Policy "was active starting on September 7, 2011," and that the policy "was not incorporated into any of the SRR versions attached to the TAC, and was therefore not a part of the contract"), with Opp'n 4–5 (arguing that the SRR "expressly refers to the Privacy Policy," but offering no response to Facebook's point that the Data Use Policy was not operative at the time the cited SRR was published). In addition, Plaintiffs do not allege that earlier versions of the Privacy Policy contained similar promises to not track logged-out users.[5]

---

[5] During the hearing on Facebook's motion on November 16, 2017, Plaintiffs' counsel argued that the September 7, 2011, Data Use Policy is incorporated into the April 26, 2011, SRR because Facebook's users continuously agree to the SRR each time they use or access Facebook. Plaintiffs base this argument on the following statement from the SRR: "By using or accessing Facebook, you agree to this Statement." TAC Ex. D. Under this theory, Plaintiffs argue that they agreed to the SRR on or after September 7, 2011, which means that the Data Use Policy would

As such, the Court finds that the Data Use Policy was not incorporated by reference into the SRR because the SRR did not "clearly and unequivocally" reference it. See Troyk, 171 Cal. App. 4th at 1331.

ii. The relevant Help Center pages were not incorporated by reference into the Statement of Rights and Responsibilities.

Plaintiffs also argue that various Help Center pages were incorporated by reference into the SRR. Opp'n 5–8. Facebook notes, and Plaintiffs do not dispute, that the SRR contains no direct references to any Help Center pages. See MTD 8–9 ("the SRR does not reference—or even hint at—a single one of the Help Center pages Plaintiffs quote from"); Opp'n 6 ("the Help Center pages are the third link in the contractual chain . . . . the Privacy Policy linked to the Help Center pages and directed users to them"). Rather, Plaintiffs' theory is that certain Help Center pages were incorporated by reference into the Privacy Policy, and that the Privacy Policy was in turn incorporated into the SRR. Opp'n 7 ("the SRR incorporates the Privacy Policy, and, in turn, the Help Center pages"); TAC ¶¶ 61 ("The Help Center pages are incorporated by reference into the Privacy Policy and are a part of the contract."), 135 (stating that two

---

have been incorporated into the contract between the parties as of that date. This argument fails for two reasons: first, the TAC does not identify the dates that Plaintiffs "used or accessed" Facebook; and second, Plaintiffs have not alleged that the April 26, 2011, version of the SRR remained in effect as of September 7, 2011.

questions common to all members of the proposed class are "whether the SRR incorporates by reference the Privacy Policy" and "whether the Privacy Policy incorporates by reference the Help Center pages").

Even if the Court assumes that the Privacy Policy was incorporated into the SRR, Plaintiffs' argument fails because the Help Center pages were not incorporated into the Privacy Policy. In the TAC, Plaintiffs cite several Help Center pages that, according to Plaintiffs, contained promises not to track logged-out users. See TAC ¶¶ 62–67. Some Help Center pages contain explicit promises to that effect—for instance, one page states: "When you log out of Facebook, we remove the cookies that identify your particular account." Id. ¶ 62, Ex. I. However, none of those Help Center are referenced in the Privacy Policy. The Privacy Policy does not link to them, mention them, or otherwise reference them directly.

Instead, Plaintiffs appear to argue that the individual Help Center pages are subparts of a single "broader document." Opp'n 5–6 ("a mainstay of Internet contract law teaches that customers are often contractually bound to individual provisions . . . even when the hyperlink only links to the broader document"). This argument finds little factual support. The Help Center pages exist independently at different URLs, as underscored by the fact that Plaintiffs attached Help Center pages as separate exhibits to their TAC. See TAC ¶¶ 62–67 (citing, in order, TAC Exs. I, J, M, L, MM, NN, OO, PP, R, S). No evidence suggests that a Facebook user who reads one Help Center page has also read, or is even aware of, any of the others.

Plaintiffs also argue that the Help Center in its entirety is incorporated into the Privacy Policy because the Privacy Policy links to some of its pages. Opp'n 6 ("Here, the TAC demonstrates clearly how that the Help Center generally (not just specific pages) are incorporated into the SRR. . . . [T]he Privacy Policy linked to the Help Center pages and directed users to them, without exclusion.") (emphasis added). Plaintiffs' argument that the Privacy Policy "directed" users to Help Center pages "without exclusion" is at odds with TAC, which alleges that the Privacy Policy linked to some Help Center pages, but not to the Help Center pages containing Facebook's promises to not track logged-out users. TAC ¶¶ 62–67. This relationship is too attenuated to support Plaintiffs' position that the entire Help Center is incorporated into the Privacy Policy. See Woods, 2011 WL 3501403, at *3–4 (finding that pages within Google's Help Center were not incorporated by reference into another document, even when that document contained direct hyperlinks to the Help Center pages at issue).

As such, the Court finds that the Help Center pages cited in the TAC were not incorporated into the Privacy Policy because they were not "known or easily available to the contracting parties." Id. (quoting Troyk, 171 Cal. App. 4th at 1331).

B. Breach of the Duty of Good Faith and Fair Dealing

As Plaintiffs note, a claim for a violation of the duty of good faith and fair dealing must rest "upon the existence of some specific contractual obligation." Opp'n 15 (quoting Avidity Partners, LLC v. State, 221

Cal. App. 4th 1180, 1204 (2013)); see also Rosenfeld v. JPMorgan Chase Bank, N.A., 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010) ("[T]he implied covenant of good faith and fair dealing 'cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement.' ") (quoting Agosta v. Astor, 120 Cal. App. 4th 596, 607 (2004)).

As discussed in the previous section, Plaintiffs have not identified contractual provisions that prohibited Facebook from tracking logged-out users in the manner Plaintiffs allege. Plaintiffs' claim for breach of the duty of good faith and fair dealing must therefore be dismissed.

C. Expanded Class Period

Plaintiffs' second amended complaint alleged a class period that began on May 27, 2010, and ended on September 26, 2011. Second Am. Compl. ("SAC") ¶ 172, Dkt. No. 93. In the order granting Facebook's motion to dismiss Plaintiff's SAC, this Court dismissed the majority of Plaintiffs' claims without leave to amend. MTD Order 14. This Court granted leave to amend only as to Plaintiffs' claims for breach of contract and breach of the duty of good faith and fair dealing, and only "[b]ecause Plaintiffs [did] not identif[y] the specific contractual provisions they allege were breached." Id. at 13–14.

In their TAC, Plaintiffs allege a new class period that begins on April 22, 2010, and ends on "a later date to be determined upon the completion of discovery." TAC ¶ 132. This expanded class definition exceeds the scope of leave to amend that the Court

granted in its order dismissing Plaintiffs' SAC. Fed. R. Civ. P. 15(a)(2) provides that "a party may amend its pleading only with the opposing party's written consent or the court's leave." Plaintiffs did not obtain Facebook's consent or this Court's leave to expand its class allegations. Accordingly, Plaintiffs' expanded class allegations are stricken.

D. Leave to Amend

Courts "should freely give leave [to amend] when justice so requires." Fed. R. Civ. P. 15(a)(2); In re Korean Air Lines Co., Ltd., 642 F.3d 685, 701 (9th Cir. 2011). Absent a showing of prejudice, delay, bad faith, or futility, there is a strong presumption in favor of granting leave to amend. Eminence Capital, LLC v. Aspeon, Inc., 316 F.3d 1048, 1052 (9th Cir. 2003).

However, courts can dismiss without leave to amend in the event of a plaintiff's "repeated failure to cure deficiencies by amendments previously allowed." Foman v. Davis, 371 U.S. 178, 182 (1962); see also Abagninin v. AMVAC Chem. Corp., 545 F.3d 733, 742 (9th Cir. 2008) ("Leave to amend may also be denied for repeated failure to cure deficiencies by previous amendment."); Zucco Partners, LLC v. Digimarc Corp., 552 F.3d 981, 1007 (9th Cir. 2009), as amended (Feb. 10, 2009) ("where the plaintiff has previously been granted leave to amend and has subsequently failed to add the requisite particularity to its claims, '[t]he district court's discretion to deny leave to amend is particularly broad' ") (quoting In re Vantive Corp. Sec. Litig., 283 F.3d 1079, 1097–98 (9th Cir. 2002)).

Here, the Court previously allowed Plaintiffs to amend their claims for breach of contract and breach

of the duty of good faith and fair dealing. Since Plaintiffs' amendments did not cure the defects the Court identified, Plaintiffs' claims will be dismissed without leave to amend.

IV. CONCLUSION

Facebook's motion to dismiss is GRANTED. The Clerk shall close this file.

IT IS SO ORDERED.

Dated: November 17, 2017

/s/
EDWARD J. DAVILA
United States District Judge

APPENDIX C

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

[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.

their Facebook friends. Id. ¶ 49. To make the "like" button appear on the page, CNN embeds a small code snippet that 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.

[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.

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 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 Communi-

cations 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

/s/
EDWARD J. DAVILA
United States District Judge

APPENDIX D

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

---

[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.

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.

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

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

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 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

---

[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.

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,

---

[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.").

820 n.3 (1997) ("Congress cannot erase Article III's standing requirements by statutorily granting the right to sue 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 dis-

missal 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 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

---

[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.

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

/s/
EDWARD J. DAVILA
United States District Judge

APPENDIX E

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

In re FACEBOOK, INC. INTERNET TRACKING LITIGATION,	No. 17-17486
PERRIN AIKENS DAVIS, et al., Plaintiffs-Appellants, v. FACEBOOK, INC., Defendants-Appellee.	D.C. No. 5:12-md-02314-EJD Northern District of California, San Jose ORDER

Before: THOMAS, Chief Judge, M. SMITH, Circuit Judge, and VRATIL*, District Judge.

The panel has voted to deny the petition for rehearing.

The full court has been advised of the petition for rehearing en banc, and no judge of the court has requested a vote on the petition for rehearing en banc. Fed. R. App. P. 35(b).

The petition for rehearing and the petition for rehearing en banc are denied.

* The Honorable Kathryn H. Vratil, United States District Judge for the District of Kansas, sitting by designation.

APPENDIX F

RELEVANT STATUTORY PROVISIONS

18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited.

(1) Except as otherwise specifically provided in this chapter any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial

establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court

order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter 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 or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public

safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of

chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the

public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

[(c) Redesignated (b)]

(5)(a)(i) If the communication is--

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this

chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

18 U.S.C. § 2520. Recovery of civil damages authorized.

(a) In general.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a

civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.--In an action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages.--(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of--

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.--A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3), 2511(2)(i), or 2511(2)(j) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation.--A civil action under this section may not be commenced later than two years after the date

upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper disclosure is violation.--Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).