FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE FACEBOOK, INC. INTERNET TRACKING LITIGATION, PERRIN AIKENS DAVIS; BRIAN K. LENTZ; CYNTHIA D. QUINN; MATTHEW J. VICKERY, *Plaintiffs-Appellants*, v. FACEBOOK, INC., *Defendant-Appellee.*	No. 17-17486 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

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

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

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

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 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.

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

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 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

[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).

placed on the user's browser. These cookies store the user's login ID, and they capture, collect, and compile the referer headers from the web 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 and fair dealing; (8) civil

[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.

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

injury the district court viewed as necessary to bring each of 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 disgorgement 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

[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.

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 non-moving 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

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

> 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 referer 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, 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

[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.

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]

[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.

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 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 person'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 fact-based 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]

B

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

---

[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) 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.

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 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

[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.

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 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]

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."

---

[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.

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

[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 for a promise. *Steiner v. Thexton*, 48 Cal. 4th 411, 421 (2010). The 2011 Data Use Policy does not contain any 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.