No. 17-16206

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

WINSTON SMITH; JANE DOE I; AND JANE DOE II, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED,
Plaintiffs-Appellants,

v.

FACEBOOK, INC.,
Defendant-Appellee.

On Appeal from a Final Judgment of the
United States District Court for the Northern District of California
Honorable Edward J. Davila
Case No. 5:16-cv-01282-EJD

APPELLEE'S BRIEF

Lauren R. Goldman
Michael Rayfield
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020

John Nadolenco
MAYER BROWN LLP
350 South Grand Avenue
Los Angeles, CA 90071

Counsel for Appellee

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, appellee Facebook, Inc. states that it is a publicly held non-governmental corporation, that it does not have a parent corporation, and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes, Regulations, and Rules

INTRODUCTION

This is a straightforward dispute about routine data collection and marketing practices that are commonplace on the Internet. In 54 pages of briefing, plaintiffs do not mention the most important allegations in their own complaint: that when plaintiffs signed up for Facebook, they entered into a "valid contract" (their words) in which they agreed that Facebook could collect information about the websites they visit and use "all" such information to assist third parties in showing "relevant ads." The district court correctly held that all of plaintiffs' claims are barred by their undisputed, affirmative consent to Facebook's Data Policy and Cookie Use agreement. This Court should affirm.

Facebook is a free social networking service that allows people to connect and share content. Like countless other websites, Facebook earns revenue by allowing third parties to display ads to people who use Facebook's service around the world. To make this advertising as relevant and interesting as possible, Facebook gathers information about users' web traffic—mainly on Facebook but also on third-party websites that host Facebook tools and features—to allow advertisers to target their ads based on people's demonstrated interests. Facebook does not share any names, email addresses, or other contact information about specific people, and it

fully discloses its use of information to everyone who signs up for the service. Facebook also specifically offers users the opportunity to opt out of receiving advertising tailored to their use of websites and apps that employ Facebook tools and features.

Instead of opting out, plaintiffs filed this lawsuit, asserting a total of ten causes of action against Facebook and seven hospitals and nonprofit health organizations. Plaintiffs claimed that when they entered search terms or clicked links on healthcare websites with Facebook code, Facebook (1) would direct plaintiffs' browsers to send Facebook a "referer header," a URL address containing the communication with the healthcare site; and (2) would send a "cookie" to plaintiffs' browsers that would inform Facebook about any future interactions with its code. Plaintiffs alleged that Facebook then used the information gathered from the cookies for "direct marketing" without their knowledge.

The district court granted the defendants' motion to dismiss with prejudice, holding that the claims against Facebook failed "because Plaintiffs consented to Facebook's conduct." Specifically, each of the plaintiffs conceded that when he or she signed up for Facebook, he or she affirmatively attested to having "read" and "agreed[]" to Facebook's Data Policy and Cookie Use page. Plaintiffs attached these policies to the

complaint and described them as "valid contract[s]." These pages clearly disclose that Facebook "collect[s] . . . information about the websites . . . you visit"; receives information from "*all across the Internet and mobile ecosystem*"; "use[s] *all* of the information we have about you to show you relevant ads"; and provides "third parties . . . with information about the reach and effectiveness of their advertising." As the district court explained, "Plaintiffs admit[ted] that they understood and agreed to Facebook's policies," and these "policies disclose the precise activity at issue in this case." Because the absence of consent is an express or implied element of each of plaintiffs' claims, their agreement to Facebook's terms barred every claim, and "no amendment could change th[at] fact."[1]

Remarkably, plaintiffs' brief *does not mention* that they agreed to the Data Policy and Cookie Use agreement when they signed up for the service, and it omits almost all of the key language from these disclosures. Instead of addressing those facts, plaintiffs raise several scattershot challenges to the district court's analysis. First, they argue that when Facebook's disclosures are read in their "totality," they cannot be interpreted to cover "sensitive communications"—even though the

[1] The court also dismissed the claims against the healthcare defendants on the ground that it lacked personal jurisdiction over those companies. Plaintiffs do not appeal from that ruling.

disclosures broadly addressed "*all*" information about users' visits to third-party websites (and their communications were not "sensitive"). Plaintiffs next contend that Facebook's disclosures were "vague"—despite the fact that the disclosures describe the exact conduct alleged in the complaint. They then argue that the relevant disclosures were "buried" in the Data Policy—an assertion that is both incorrect and irrelevant, given plaintiffs' express agreement to the policy's terms. Finally, plaintiffs argue that Facebook could obtain their consent to its policies only by complying with the detailed conditions imposed by the Health Insurance Portability and Accountability Act ("HIPAA")—a statute that (1) has no private right of action, (2) does not govern Facebook, and (3) applies only to a narrow category of information that is not at issue here.

If this Court agrees with the district court's conclusion that plaintiffs' consent bars all of their claims, then it need not consider whether the other flaws outlined below bar each of their specific causes of action. In short: Plaintiffs' federal and state "wiretapping" claims fail because their own allegations belie any notion that they have been wiretapped; plaintiffs claim that their *own browsers* sent the communications at issue directly "to Facebook's server." Plaintiffs' two privacy-related claims fail because California law requires them to allege

"highly offensive" conduct, not just routine Internet functionality and marketing activities. Their claims for fraud and breach of the duty of good faith and fair dealing are little more than restatements of their claim that Facebook did not comply with its disclosures; it assuredly did.

At bottom, the complaint describes little more than the everyday use of data to provide a variety of services (often for free) that people enjoy and want to use—a practice that plaintiffs consented to when they signed up for Facebook. The Court should affirm the decision below.

JURISDICTIONAL STATEMENT

Facebook agrees with plaintiffs' jurisdictional statement.

STATEMENT OF THE CASE[2]

A. The Internet and Referer Headers

People navigate the Internet using web browsers (like Google Chrome, Apple Safari, and Microsoft Internet Explorer) that send, receive, and display content on computers and other electronic devices. ER211-12 ¶¶ 21-23. Every webpage is hosted by a computer server that communicates with browsers and provides them with content from the

[2] "ER__" refers to plaintiffs' Excerpts of Record. "PB__" is plaintiffs' opening brief. Because the district court dismissed this case on the pleadings, Facebook accepts the allegations in the complaint as true for purposes of this appeal; it does not admit the veracity of these allegations.

webpage. ER212 ¶ 24. The most basic communication between server and browser is a "GET request," a message sent from the browser to the server requesting information for display on the computer or device. ER212 ¶ 25.

GET requests come in various forms—a person can type information into the navigation bar of his browser, or type information into a search engine hosted by the webpage, or click on a hyperlink. *Id.* For example, when a person types "www.cancer.org" into his browser's navigation bar, the browser sends a GET request to the server for Cancer.org requesting information on the Cancer.org homepage. *Id.*

Although a webpage appears on a person's screen as a complete product, it is actually an assembly of independent parts, often including content (like advertisements) that exists on different servers operated by third parties. ER214 ¶ 30. The host server initially leaves blank the parts of the page that will be filled in by third parties. ER214 ¶ 31. When a browser sends the host a GET request to view a webpage that also contains third-party content, the host sends code back to the browser directing it to send a separate GET request to the third party's server. ER214 ¶ 32. Upon receiving that GET request from the user's browser, the third party fills in the blank portion of the webpage. *Id.* Thus, the user's browser sends at least two distinct requests: one to the host

webpage's server to load its portion of the webpage, and one to the third party's server to load its content onto that same webpage. *Id.*

Because the third party needs to know where to load the requested content, the GET request sent to the third-party server typically contains the Uniform Resource Locator ("URL") of the webpage being loaded. ER214 ¶ 33. An URL is generally displayed in an address bar at the top of the browser. It consists of several parts: (1) a protocol identifying the language of the interaction between the browser and the server (*e.g.*, "http://"); (2) the name of the website (*e.g.*, "www.cancer.org"); and (3) when applicable, particular folders and subfolders on the server that the browser has requested for display (*e.g.*, "/cancer/"). ER213 ¶ 28. When sent to a third-party server, an URL is called a "referer header" because it directs (or "refers") the third party to the site where the content is to be loaded. ER214 ¶ 33.

Many webpages contain Facebook content, such as its "Like" button and its "Share" button. ER225 ¶ 62. "Embedded third-party code is ubiquitous, not just in the form of Facebook buttons, but also in the form of videos, ads, analytics services, code libraries, content delivery networks, and myriad other tools." ER10. When a person's browser requests a webpage with Facebook content, the browser sends a GET request to

Facebook's server along with a referer header telling Facebook where to load the requested content. ER215 ¶ 35. The referer header is sent from "the user's web-browser . . . to Facebook's server" (ER220-21 ¶ 50(f)); it is "separate" from "the actual communication" between the browser and the host site (ER266 ¶ 255).

B. Cookies

A cookie is a small piece of text that a server creates and sends to a browser when the two communicate. ER216-17 ¶¶ 41-42. The browser sends information from the cookie back to the server whenever the browser makes additional requests of the same server. *Id.* By examining the cookie, the server can determine whether it has interacted with this browser before and can locate records about its history with that browser. ER216-22, 231 ¶¶ 42-43 45-46, 50, 85. As discussed above, when the browser requests a page with third-party content, the cookie is accompanied by a referer header. The receiving server can then connect the data from the cookie with the URL contained in the referer header, and thereby determine which browser has requested the information. *Id.* Cookies are widely used on the Internet for many purposes, including security, efficiency, and advertising. ER216-17 ¶ 42.

C. Facebook's Disclosures

Facebook fully discloses its receipt and use of data to everyone who joins and uses Facebook (including each of the named plaintiffs). The complaint acknowledges that "[o]n sign-up, Facebook requires people to click a green Sign Up button" directly underneath the following text: "By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use." ER224 ¶ 58. The phrases "Terms," "Data Policy," and "Cookie Use" are highlighted in blue and link directly to three disclosures (attached to the complaint). ER224 ¶ 59, ER297-320. Plaintiffs alleged that these disclosures "constitute[] a valid contract." ER224 ¶ 59.

1. Statement of Rights and Responsibilities

In the sign-up process, the phrase "Terms" is hyperlinked to Facebook's Statement of Rights and Responsibilities ("SRR"). ER297-301. The SRR attached to the complaint states that "[y]our privacy is very important to us"; that "[w]e designed our Data Policy to make important disclosures about . . . how we collect and can use your content and information"; and that "[b]y using or accessing Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy." ER298, 300.

2. Data Policy

The Data Policy attached to the complaint details Facebook's collection and use of information. First, it informs people that "[w]e collect information when you visit or use third-party websites and apps that use our Services," and that this includes web-traffic information—specifically, "information about the websites and apps you visit, your use of our Services on those websites and apps, [and] information the developer or publisher of the app or website provides to you or us." ER304; *see also id.* (Facebook "receives[s] information about you and your activities on and off Facebook from third-party partners, such as information from . . . an advertiser about your experiences or interactions with them").

Second, the Data Policy explains how Facebook *uses* this data: Among other things, Facebook "use[s] the information . . . to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services"; Facebook "work[s] with third party companies" to do so. ER305, 307. More specifically:

> We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, ***we use all of the information we have about you to show you relevant ads.*** We do not share information that personally identifies you (. . . like name or email

> address that can by itself be used to contact you or identifies who you are) with advertising . . . partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information . . . to these partners to help them understand their audience or customers . . . .

ER307 (emphasis added).

Third, the Data Policy tells people that they can "[l]earn more about advertising on our Services and how you can control how information about you is used to personalize the ads you see"; the phrases "Learn more" and "control" are hyperlinked to pages explaining how people can opt out of the use of certain data for targeted advertising. ER305.

3. Cookie Policy

A third disclosure addresses Facebook's use of cookies. The Cookie Policy attached to the complaint explains that cookies are "placed on your browser" and "are used to deliver, secure, and understand products, services, and ads, on and off the Facebook Services." ER315. Facebook uses them "for a variety of reasons." *Id.* Most relevant here:

> Cookies . . . are used to understand and deliver ads, make them more relevant to you, and analyze products and services and the use of those products and services. For example, we use cookies so we, or our affiliates or partners, can serve you ads that may be interesting to you on Facebook Services or other websites and mobile applications. We may also use a cookie to learn whether someone who was served an ad on Facebook Services later makes a purchase on the advertiser's site or installs the advertised app. Similarly, our partners may use a cookie or another similar technology to determine whether we've served an ad and how it performed or provide us with information about how you interact with them. We also may work with an advertiser or its marketing partners to serve you an ad on or off Facebook Services, such as after you've visited the advertiser's site or app, or show you an ad based on the websites you visit or the apps you use—***all across the Internet and mobile ecosystem***.

ER316 (emphasis added). Like the Data Policy, the Cookie Policy tells people that "[y]ou can adjust your ad preferences if you want to control your ad experience on Facebook." ER318.

D. Plaintiffs' Lawsuit

The three named plaintiffs—Winston Smith, Jane Doe I, and Jane Doe II[3]—allege that they are registered users of Facebook who visited the

[3] The complaint uses pseudonyms rather than the plaintiffs' real names for the purported purpose of "protect[ing] their medical information from further disclosure." ER210 ¶ 6 n.1. The lead plaintiff is not-so-subtly named after the protagonist in George Orwell's *1984*.

websites of seven healthcare organizations: the American Cancer Society; the American Society of Clinical Oncology; Melanoma Research Foundation, Adventist Health System; BJC HealthCare; Cleveland Clinic; and the University of Texas's MD Anderson Cancer Center (collectively the "healthcare defendants"). ER210-11 ¶¶ 6-8, 10-16.

The complaint alleges that when plaintiffs visited the healthcare defendants' websites, "Facebook acquired, tracked, and used the Plaintiffs' sensitive medical information" in order "to sell advertising that is customized based upon a particular person's Internet communications." ER209, 217 ¶¶ 2-4, 43. It further claims that Facebook sorts people into "154 separate medical categories" based on their interests—for example, a category of "84 million users who have expressed an interest in or like pages related to cancer awareness" and therefore might "have an interest in making donations to cancer causes." ER232-33 ¶¶ 89-90, ER333-46.

Plaintiffs originally brought ten causes of action (one under federal law, and nine under California law): (1) violation of the federal Wiretap Act; (2) intrusion upon seclusion; (3) violation of the California Invasion of Privacy Act ("CIPA"); (4) California constitutional invasion of privacy; (5) negligence per se; (6) negligent disclosure of confidential information; (7) breach of the fiduciary duty of confidentiality; (8) breach of the duty of

good faith and fair dealing; (9) fraud; and (10) quantum meruit. The first five were asserted against all defendants; the sixth and seventh were against only the healthcare defendants; and the last three were against only Facebook. The cases were assigned to Judge Edward J. Davila.

E. The District Court's Ruling and This Appeal

The defendants jointly moved to dismiss the complaint. ER148-98. After full briefing, the district court granted the motion and entered judgment in the defendants' favor. ER1-17. The court dismissed the claims against Facebook on the ground that plaintiffs had consented to the conduct at issue. ER11-17. It dismissed the claims against the healthcare defendants based on the absence of personal jurisdiction. ER7-11.

In its analysis of the claims against Facebook, the court first explained that "Plaintiffs agreed to several Facebook policies when they signed up for accounts," and that these policies (described above) "contain[] several broad disclosures, including information about how Facebook tracks users to improve its ad targeting." ER11-12. The court concluded that "Plaintiffs admit that they understood and agreed to Facebook's policies," that "Facebook's policies disclose the precise activity at issue in this case," and that plaintiffs' consent to these policies barred each of their claims against Facebook. ER16-17. The court also found that "no

amendment could change the fact that Plaintiffs consented to Facebook's conduct." *Id.* It therefore dismissed the complaint with prejudice. ER17.

Plaintiffs appealed the district court's ruling as to Facebook alone. ER18-20. Their appeal addresses six of the eight claims originally asserted against Facebook: (1) the Wiretap Act; (2) CIPA; (3) intrusion on seclusion; (4) California's constitutional right to privacy; (5) breach of the duty of good faith and fair dealing; and (6) fraud. *See* PB30-54.[4]

STANDARD OF REVIEW

The Court "review[s] de novo a district court's dismissal for failure to state a claim upon which relief can be granted," *Puri v. Khalsa*, 844 F.3d 1152, 1157 (9th Cir. 2017), asking whether the complaint "contain[s] sufficient factual matter, accepted as true, to state a claim for relief that is plausible on its face," *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotation marks omitted). The Court "need not accept as true allegations contradicting documents that are referenced in the complaint," *Lazy Y Ranch Ltd. v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008), or "legal conclusion[s] couched as a factual allegation," *Iqbal*, 556 U.S. at 678. And it may affirm on any ground supported by the record, "even one not relied

[4] Plaintiffs' opening brief does not address the claims they brought against Facebook for negligence per se and quantum meruit.

upon by the district court." *Democratic Party of Haw. v. Nago*, 833 F.3d 1119, 1122 (9th Cir. 2016).

SUMMARY OF ARGUMENT

Facebook relies on its Introduction for the summary of its arguments. *See* pp. 1-5 *supra*. The district court correctly dismissed all of plaintiffs' claims because plaintiffs consented to Facebook's receipt and use of the information at issue. But even if the claims were not barred by plaintiffs' consent, the Court should still affirm the decision below, because plaintiffs failed to plead other necessary elements of each claim.

ARGUMENT

I. THE DISTRICT COURT CORRECTLY HELD THAT ALL OF PLAINTIFFS' CLAIMS ARE BARRED BY THEIR CONSENT TO THE CONDUCT ALLEGED IN THEIR COMPLAINT.

A. Lack of Consent Is an Element of Each Claim.

The district court correctly determined—and, significantly, plaintiffs do not dispute—that the absence of consent is either an express or implicit component of each of the claims at issue on appeal. ER15-16; *see also* Cal. Civ. Code § 3515 ("He who consents to an act is not wronged by it."); *Kent v. Microsoft Corp.*, 2013 WL 3353875, at *6 (C.D. Cal. July 1, 2013) ("[P]laintiffs generally may not assert a wrong arising out of an action which they consented to."); RESTATEMENT (SECOND) OF TORTS § 892A

(1979) ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct."). The following authorities establish the consent element of each claim; the other elements of each claim are addressed in Part II below.[5]

Wiretap Act. The Wiretap Act expressly precludes liability where "one of the parties to the communication has given prior consent." 18 U.S.C. § 2511(2)(d); *see also Medina v. Cty. of Riverside*, 308 F. App'x 118, 120 (9th Cir. 2009) ("consent . . . vitiates plaintiffs' claims under the [Wiretap] Act"); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1045 (N.D. Cal. 2014).

CIPA. A CIPA claim requires the plaintiff to prove that the defendant intercepted or recorded information "without the consent of all parties" to the communication. Cal. Penal Code §§ 631(a), 632(a); *see also*

---

[5] Plaintiffs assert in a footnote that "Defendants bear the burden of proving the affirmative defense of consent." PB14 n.4. But consent is not an "affirmative defense" in this case; rather, lack of consent is an element of each of plaintiffs' claims on which they bore the burden. *See Garcia v. Enter. Holdings Inc.*, 78 F. Supp. 3d 1125, 1135-36 (N.D. Cal. 2015) ("[T]he Court disagrees with Plaintiff's assertion that lack of consent is not an element of his [CIPA] claim. . . . Where lack of consent is an express element of a claim, . . . it must be alleged in the complaint."). In any event, to the extent that Facebook had the burden of proof, it satisfied that burden; the documents bearing on this issue are all attached to the complaint, and Facebook relied solely on those attachments in moving to dismiss based on consent.

Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95, 118 & n.7 (2006) (because CIPA's "statutory scheme protects against" only "nonconsensual" conduct, "[a] business that adequately advises all parties to a telephone call . . . of its intent to record the call would not violate [CIPA]" (internal quotation marks omitted)); *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013).

Intrusion on seclusion/invasion of privacy. "The plaintiff in an invasion of privacy case"—whether brought under California common law or the California Constitution—"must not have manifested by his or her conduct a voluntary consent to the invasive actions of the defendant." *Hill v. NCAA*, 7 Cal. 4th 1, 26 (1994); *see also Gulec v. Boeing Co.*, 698 F. App'x 372, 373 (9th Cir. 2017) ("The district court properly dismissed [plaintiff's] invasion of privacy claim under California law because [plaintiff] failed to allege facts sufficient to show that he had a reasonable expectation of privacy in light of his consent to the phone interviews." (citing *Hill*, 7 Cal. 4th at 35-37)); *Baugh v. CBS, Inc.*, 828 F. Supp. 745, 757 (N.D. Cal. 1993) ("[P]laintiff gave her consent and she therefore has no remedy under [an intrusion-on-seclusion] theory.").

Implied duty of good faith. A claim for breach of the duty of good faith and fair dealing requires an allegation that the contracting party

"unfairly frustrat[ed] the other party's right to receive the benefits of the agreement actually made"—here, the agreement that plaintiffs formed with Facebook when they signed up and used the service. *Guz v. Bechtel Nat'l Inc.*, 24 Cal. 4th 317, 349 (2000). If Facebook's disclosures were accurate and addressed the conduct at issue here (*i.e.*, if plaintiffs consented to that conduct), then Facebook could not have "frustrated" plaintiffs' ability to receive the benefits of the agreement.

Fraud. A fraud claim requires a plaintiff to demonstrate that the defendant made a false statement or suppressed a material fact—here, in Facebook's disclosures. *S. Tahoe Gas Co. v. Hofman Land Improvement Co.*, 25 Cal. App. 3d 750, 765 (1972). If Facebook's disclosures accurately described the relevant conduct (*i.e.*, if plaintiffs consented to that conduct), then Facebook made no misrepresentation.

B. Plaintiffs Consented to the Collection and Use of Information About Their Visits to the Healthcare Sites.

The question in this case is not whether plaintiffs agreed to Facebook's SRR, Data Policy, and Cookie Policy, or whether those agreements are enforceable. Plaintiffs conceded both of those points below (ER224)—a fact notably omitted from their brief. The only question before this Court is whether Facebook's disclosures encompass the conduct at issue in this suit. "There may be subtle differences" among the consent

doctrines applicable to plaintiffs' various claims, but "the question under [each] is essentially the same: Would a reasonable user who viewed [Facebook's] disclosures have understood that [Facebook] was collecting [the information at issue]?" *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014) (Koh, J.).[6] The answer is clearly yes.

Facebook's policies disclose, among other things, that Facebook: (1) "work[s] with third-party companies who . . . use advertising or related products"; (2) "collect[s] information when you visit or use third-party websites," including "information about the websites"; (3) "use[s] *all* of the information we have about you to show you relevant ads"; (4) "provide[s] [third parties] with information about the reach and effectiveness of their advertising"; (5) uses "[c]ookies" to "deliver ads," "make them more relevant to you," and "show you . . . ad[s] based on the websites you visit or the apps you use—*all across the Internet and mobile ecosystem*"; and (6) permits people to "control" how this information is used for advertising purposes. ER304, 307, 316 (emphases added).

---

[6] Plaintiffs agree that, at least in the non-medical context, this is the correct test. *See* PB18, 25-26. They repeatedly assert that "[t]he 'validity of [a party's] consent is a question of fact.'" PB14 (quoting *United States v. Cormier*, 220 F.3d 1103, 1112 (9th Cir. 2000)). But the interpretation of Facebook's *written disclosures*—and whether those disclosures address the conduct alleged in this case—is a question of law. *See Pure Wafer Inc. v. City of Prescott*, 845 F.3d 943, 961 (9th Cir. 2017).

The district court correctly held that "Facebook's policies disclose the precise activity at issue in this case." ER16. Any "reasonable user" who read them would know (because they say so expressly) that Facebook collects *all* information about its users' visits to third party websites, and uses *all* of this information to help third parties improve the quality of advertisements based on people's interests. In short, Facebook's policies told users exactly the kind of information that Facebook was collecting and how it was using that information. Plaintiffs are bound by their consent to those policies.

C. Plaintiffs' Various Attempts to Escape the Consequences of Their Consent Are Unavailing.

Plaintiffs offer an array of allegations and authorities to poke holes at the district court's conclusion. Each of their arguments is meritless.

1. The District Court Did Not Overlook the "Totality of the Circumstances."

Plaintiffs first contend that the district court "read Facebook's consent provisions in isolation," and that "[t]aken in full, the facts alleged establish that no reasonable person would have believed that the specific data at issue was being disclosed to, tracked, acquired and sold by Facebook." PB18. Plaintiffs offer a bulleted list of these allegations (PB19-20), which are addressed in turn below. But broadly speaking, each

of these "allegations" is either a legal conclusion; a bare assertion that cannot be squared with the documents attached to the complaint; or entirely irrelevant to whether plaintiffs gave consent.

- *"Plaintiffs specifically and repeatedly alleged that they lacked knowledge of and did not authorize Facebook's acquisition of the data at issue."* PB19.[7] It makes no difference whether plaintiffs "lacked knowledge of" Facebook's use of cookies with respect to the particular healthcare sites at issue, because plaintiffs affirmatively attested to reading and agreeing to Facebook's policies, which disclosed that Facebook would be collecting information from the sites that plaintiffs visited. *See, e.g.*, *Circuit City Stores, Inc. v. Ahmed*, 283 F.3d 1198, 1200 (9th Cir. 2002) ("[O]ne who signs a contract is bound by its provisions and cannot complain of unfamiliarity with the language of the instrument."); *see also* pp. 34-36 & n.19 *infra*. Similarly, plaintiffs' allegation that they did not "authorize" Facebook's conduct has no legal effect, because it is contradicted by documents—the Data Policy and Cookie Policy—"that are referenced in the complaint." *Lazy Y Ranch*, 546 F.3d at 588; *see also Garcia v. Enter. Holdings, Inc.*, 78 F. Supp. 3d 1125, 1136 (N.D. Cal. 2015) ("[T]he documents proffered by Defendants . . . contradict Plaintiff's claim

[7] Italics are added to the quotes from plaintiffs' brief.

that he was unaware of and did not consent to the transfer of his personal information to a third party.").

- *"The communications at issue were with trusted health care entities and related to health conditions, doctors, treatment, or financing for themselves or, for Jane Doe II, her spouse."* PB19. As explained in detail below (*see* Part I.C.2 *infra*), neither the subject matter of the communications nor the nature of the websites has any relevance to the question of consent. Facebook disclosed the nature of the information that it would collect and how it would use that information.

- *"Plaintiffs were specifically promised that the communications would not be disclosed to third-parties like Facebook"; "Facebook had actual and constructive knowledge of these promises" and "knowingly acquired the data at issue in violation of" them.* PB19. Plaintiffs' use of the passive voice is telling: They are referencing disclosures on the websites of the *healthcare defendants*, not Facebook's disclosures.[8] The healthcare websites' disclosures do not help plaintiffs, for two reasons. First, while some of the healthcare defendants promised not to disclose *personally-identifying information*, they did not promise to keep

[8] *See also* Br. of *Amicus Curiae* Electronic Privacy Information Center ("EPIC Br.") at 15-16 (making similar argument).

web-traffic information confidential. To the contrary, the healthcare defendants affirmatively disclosed that information about users' web traffic would be communicated to third parties.[9] Once again, plaintiffs wholly omit that language.

Second, and more fundamentally, as far as plaintiffs' claims against Facebook are concerned, it does not matter what the healthcare defendants promised: Plaintiffs are bound by their agreement to *Facebook's* terms. Plaintiffs do not claim that Facebook ever suggested that its disclosures could be modified or limited by representations on other websites or that it intended to be bound by such representations. And they cite no authority for the remarkable proposition that a contract between two parties can be modified or rendered unenforceable by a

[9] *See, e.g.*, ER359 ("[T]he providers of third party Cookies may have the ability to link your activities on the Website with your browsing activities elsewhere on the Internet."); ER349 (stating that general "traffic" information, such as a user's "browser information and length of stay" on a website, may be disclosed); ER370 (advising that "the date and time of [a user's] visit and the solutions and information for which [she] searched and which [she] viewed" may be disclosed); ER376 (disclosing that user IP addresses would be automatically collected and shared, and could be used to determine "a visitor's Internet Service Provider and the geographic location of his or her point of connectivity"); ER395 (disavowing confidentiality of web traffic information and noting use of third-party cookies to serve ads "based on [a user's] visit to [its] site").

representation that one of the parties received from *someone else*, with or without the counterparty's knowledge.

- *"Facebook promised to make 'important disclosures,' but engaged in fraudulent 'suppression, with the intent to deceive its users, of [the conduct alleged in the complaint].'"* PB20. Stringing together these two quotes from different sources does not transform them into a valid legal argument. The "important disclosures" language is drawn from Facebook's SRR, and references the disclosures that Facebook *did* make in its Data Policy: "We designed our Data 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. . . . By using or accessing Facebook Services, you agree that we can collect and use [ ] content and information in accordance with the Data Policy." ER298, 300. The "suppression" language is taken from plaintiffs' cause of action for fraud (ER291-92 ¶ 366)—and that cause of action is meritless, because Facebook's disclosures "suppressed" nothing. See Part II.B *infra*.[10]

[10] Similarly, the *amicus* argues that plaintiffs' "[c]onsent is limited by the scope of Facebook's settlement with the FTC in 2012," in which it agreed not to "misrepresent . . . the extent to which it maintains the privacy or security of covered information." EPIC Br. at 13. Facebook did not "misrepresent" any information; its disclosures were entirely accurate.

- *"Plaintiffs enjoyed 'several specific legally protected privacy interests' in the communications at issue, including actual and reasonable expectations of privacy."* PB20. This quotation from plaintiffs' complaint has no bearing on whether Facebook's policies adequately disclosed its data-collection practices. It is a legal conclusion that the Court has no obligation to accept. *See Iqbal*, 556 U.S. at 678. And it is incorrect. *See* Part II.E.1 *infra*.

- *"Facebook tracking does not occur on all medical websites and is not necessary for a website to utilize some functionality."* PB20. This, too, has absolutely nothing to do with whether plaintiffs consented to Facebook's collection of data about their visits to the healthcare sites. Facebook has never argued that it receives information from "*all* medical websites"; for example, it does not gather data from sites that do not include any Facebook code. Nor has Facebook ever contended that a third-party website is unable to "function[]" without "Facebook tracking." Rather, Facebook's argument is that data collection is (1) a routine part of the Internet and (2) fully disclosed by Facebook's policies, to which

---

And Facebook's settlement with the FTC is irrelevant to whether the operative terms and disclosures at issue establish informed consent here.

plaintiffs agreed. That this activity is neither universal nor necessary to the function of the healthcare sites does not make it *illegal*.

In short, what plaintiffs call the "totality of the circumstances" is a series of kitchen-sink allegations with no bearing on consent. None changes the dispositive fact that plaintiffs admitted that they were bound by Facebook's terms, and those terms disclose all of the conduct alleged in their complaint.

2. Facebook's Disclosures Were Not "Vague"—They Cover the Exact Conduct at Issue in This Suit.

The district court rejected plaintiffs' argument "that Facebook's policies are too 'vague' and 'broad' to be enforceable," explaining that "Facebook's Data Policy discloses the precise conduct at issue in this case." ER13. Plaintiffs reprise this argument on appeal. PB21-25. The crux of their position is that Facebook's policies did not specifically disclose that Facebook would be collecting "communications about their health conditions, treatment, and financing." PB23-24; *see also* ER225 ¶ 65 (alleging that plaintiffs' consent to Facebook's policies was irrelevant

because Facebook did not disclose that it collects "medical information and communications" specifically).[11] This theory is meritless.

As a matter of both common sense and well-established case law, Facebook had no obligation to identify the precise *websites* from which it was collecting web-traffic information. Rather, it fulfilled its obligations by disclosing that it would collect and use all "information about the websites and apps you visit" containing Facebook's code, "your use of our Services on those websites and apps," and "information the developer or publisher of the app or website provides to you or us." ER304. No user would read a list of every conceivable kind of website from which Facebook collects information—even if such a list could be created and constantly updated to reflect the ever-expanding content on the Internet.

Circuit precedents are clear on this point: "A contractual term is not ambiguous *just because it is broad*." *F.B.T. Prods., LLC v. Aftermath Records*, 621 F.3d 958, 964 (9th Cir. 2010) (emphasis added).[12] Consistent

---

[11] The *amicus* makes a similar argument. *See, e.g.*, EPIC Br. at 8 (arguing that the district "court erred when it failed to construe ambiguous terms against the drafter").

[12] *See also Fober v. Mgmt. & Tech. Consultants, LLC*, 2016 WL 7626431, at *4 (C.D. Cal. July 29, 2016) ("Plaintiff . . . may not survive summary judgment . . . merely by noting the wide scope of the relevant consent provision and then labeling that provision 'ambiguous.'"); *Young v. Wideawake Death Row Entm't LLC*, 2011 WL 12565250, at *5 (C.D. Cal.

with that authority, courts in this Circuit routinely dismiss claims based on the collection of online information when the defendant discloses these practices—even where those disclosures are far less detailed and extensive than Facebook's.

In *Perkins*, for example, the plaintiffs alleged that LinkedIn had harvested non-user email addresses from the plaintiffs' contact lists and then sent marketing materials to those email addresses. 53 F. Supp. 3d at 1195. Judge Koh dismissed the plaintiffs' Wiretap Act claim based on consent, reasoning that when a user entered his email address into LinkedIn, he was notified that LinkedIn was "asking for *some* information from" the email account, and was then given a choice of permitting or forbidding this collection. *Id.* at 1212 (emphasis added). The court was "not persuaded by Plaintiffs' contention that the disclosures were not clear enough to alert Plaintiffs that the emails to their contacts would contain an endorsement of LinkedIn"; this argument was an "attempt to slice the disclosures too thin." *Id.* at 1215.

In *Del Vecchio v. Amazon.com, Inc.*, 2012 WL 1997697 (W.D. Wash. June 1, 2012) ("*Del Vecchio II*"), the plaintiffs alleged that Amazon used

---

Apr. 19, 2011 ("The terms 'manners' and 'distribution' are admittedly broad, but they do not appear to be unclear or ambiguous.").

cookies to "misappropriat[e]" "sensitive information about [the plaintiffs'] . . . purchases," their "financial information such as credit and debit card information," and their "mailing and billing addresses." *Id.* at *2. The court dismissed the claim because Amazon's terms of use "notif[ied] visitors that [Amazon] will take the very actions about which Plaintiffs now complain: place . . . *cookies* on their computers and use those cookies to monitor and collect information about their navigation and shopping habits." *Del Vecchio v. Amazon.com, Inc.*, 2011 WL 6325910, at *4 (W.D. Wash. Dec. 1, 2011) ("*Del Vecchio I*"). The court reached this conclusion even though Amazon's terms did not say anything *specific* about the kinds of information obtained using the cookies; they said only that "[w]e receive and store *certain* types of information whenever you interact with us." *Id.* at *4 n.7 (emphasis added).[13]

Finally, in *Mortensen v. Bresnan Communication LLC*, 2010 WL 5140454 (D. Mont. Dec. 13, 2010), the plaintiffs brought Wiretap Act and

[13] Plaintiffs argue that the *Del Vecchio* court "punted on 'the issue of authorization,' instead ordering further briefing." PB22. That is misleading. The court in *Del Vecchio I* dismissed the plaintiffs' claims on the pleadings based on their consent, with leave to amend. 2011 WL 6325910, at *4. In *Del Vecchio II*, the court declined to rule on consent as to the amended complaint, but reiterated that it was "very likely that Defendant's [terms] disclose[d] sufficient information to negate Plaintiffs' . . . claims." 2012 WL 1997697, at *1. The case settled soon after.

privacy claims against an internet service provider, alleging that the defendant had tracked their web-traffic information using cookies and had sent their "Internet communications to . . . a third-party Internet advertising company." *Id.* at *1. The plaintiffs argued that the terms of service did not bar their claim because the defendant "did not fully describe its intent to funnel [the] customer's complete, unfiltered Internet traffic to a third-party processor for profiling and ad-serving." *Id.* at *4 (internal quotation marks omitted). The court disagreed, concluding that it was sufficient for the defendant to disclose "that Plaintiffs' *electronic transmissions* would be monitored and would in fact be transferred to third-parties for the purposes of providing '*content or services*.'" *Id.* at *5 (emphases added).[14]

This is an even clearer case of consent. If it is enough for online services to tell users that they are collecting "some information" from users (*Perkins*), or "certain types of information" (*Del Vecchio I*), or "electronic transmissions" (*Mortensen*), then Facebook's disclosures—

[14] Plaintiffs attempt to distinguish *Mortensen* on the ground that Facebook "did not provide its users with the ability to opt-out of its tracking on health care websites that promised not to disclose their PII." PB21-22. That is nonsensical. Facebook *did* give users the opportunity to opt out of certain types of targeted advertising, and as discussed above, it would have been absurd for Facebook to attempt to provide a more limited opt-out with respect to specific "websites" that made specific "promise[s]."

including its disclosure that Facebook would collect "information about the websites and apps you visit, your use of our Services on those websites and apps, [and] information the developer or publisher of the app or website provides to you or us" (ER304)—plainly are more than sufficient.[15]

The cases that plaintiffs cite (PB24-25) are not to the contrary. Plaintiffs rely on *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*, 135 F.3d 1260 (9th Cir. 1998) for the proposition that plaintiffs' consent to "Facebook's general tracking of consumers on the Internet" does not establish their consent to "Facebook's tracking of their communications about medical conditions." PB24. *Norman-Bloodsaw*, however, had nothing to do with the tracking of web-traffic information; it was about "highly invasive" *physical testing*. 135 F.3d at 1270. The Court held that the plaintiffs' agreement to a "general medical examination," and their answers to "written questions as to whether they had [certain diseases]," did not mean they expected to "hav[e] their blood and urine tested for

---

[15] *See also, e.g.*, *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1030 (N.D. Cal. 2014) (dismissing Wiretap Act claim because "Yahoo obtained consent . . . to scan and analyze emails for the purposes of providing personal product features, providing targeted advertising, and detecting spam and abuse"); *Deering v. CenturyTel, Inc.*, 2011 WL 1842859, at *2-3 (D. Mont. May 16, 2011) (holding that the plaintiff "consented to the monitoring of his Internet activity"; "there is no reasonable expectation of privacy when a plaintiff has been notified that his Internet activity may be forwarded to a third party to target him with advertisements").

specific conditions that corresponded tangentially if at all to the written questions." *Id.* at 1267-68.[16] There is nothing controversial about that conclusion: An agreement to a "general" examination does not constitute consent to physical testing on every conceivable medical condition. *Id.* at 1270. And even if routine data collection could be analogized to a physical examination, Facebook did not tell users that it would collect "general" information; it told users the specific information that it would be collecting. ER304.

The Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473 (2014), has even less to do with this case. Plaintiffs suggest that *Riley* held that "Americans have a reasonable expectation of privacy" in any communications that even touch on matters related to healthcare. PB24. Not so. *Riley* held that a warrantless search of a cell phone is not subject to the "search incident to arrest exception" to the Fourth Amendment's warrant requirement, and noted that a cell phone could reveal a great deal of information about its owner, including the owner's visits to WebMD.

---

[16] The question in *Norman-Bloodsaw* was not whether the plaintiffs had consented to the conduct. It was whether, for purposes of the statute of limitations, their claims began to accrue at the time of the examinations or at the time they found out that they were being tested for certain diseases. The Court concluded that there was a triable issue of fact on when the plaintiffs gained the relevant knowledge. 135 F.3d at 1266.

134 S. Ct. at 2485, 2490. The case did not involve any form of alleged consent, nor was it interpreting the statutes and causes of action at issue in this case.[17]

3. Plaintiffs' Complaint Belies Their Assertion that Facebook's Disclosures Were "Buried."

Plaintiffs' next argument is that Facebook's disclosures about data collection were "buried within a Privacy Policy that no user was likely to read or understand." PB25; *see also* PB23.[18] This argument fails for each of three independent reasons.

First, whatever plaintiffs may assert about "users" generally, they do not argue that *they* failed to read, see, or understand Facebook's policies. Any such suggestion would be squarely contradicted by the complaint,

---

[17] Plaintiffs discuss two other cases in their background discussion of the law. PB14-17. In *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003), the plaintiff pharmaceutical companies "explicitly conditioned their purchase [of the defendant's product] on the fact that it would *not* collect [the] information" at issue. 329 F.3d at 20. And in *Thoefel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), this Court explained that "an overt manifestation of assent or willingness would not be effective . . . if the defendant knew, or probably if he ought to have known . . . , that the plaintiff was mistaken as to the nature and quality of the invasion intended." *Id.* at 1073. Nothing in the complaint suggests that Facebook knew that plaintiffs were "mistaken" about the data it was collecting.

[18] Notably, both plaintiffs and their *amicus* repeatedly misstate the operative title of Facebook's disclosure—referring to it as a "Privacy Policy" rather than a "Data Policy." This distinction underscores the policy's unambiguous subject matter: Facebook's *data collection*.

which (unlike plaintiffs' brief) recognizes that when plaintiffs signed up for Facebook, they were presented directly with hyperlinks to the terms, stated that they "agree[d]" to those terms, and acknowledged that they had "read" the Data Policy and Cookie Policy. ER224 ¶ 58.

Second, it would not matter if plaintiffs failed to read or understand the policies. As noted above, this Court has made clear that "one who signs a contract is bound by its provisions and cannot complain of unfamiliarity with the language of the instrument." *Circuit City*, 283 F.3d at 1200. This is equally true in the context of online contract formation: the "failure to read . . . [the] terms does not relieve a party of its obligations under the contract." *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176, 1179 (9th Cir. 2014).

Third, the complaint does not allege that the placement or language of the policies rendered them unenforceable. Again, it alleges precisely the opposite: that Facebook's disclosures "constitute[] a valid contract." ER224 ¶ 59. The district court explained why plaintiffs made this claim: "in their cause of action against Facebook for fraud, Plaintiffs allege that they *relied* on Facebook's assertions in the very same contracts." ER12 (emphasis added). The same is true of their claim for breach of the duty of good faith and fair dealing, which contends that Facebook frustrated the

contractual terms that plaintiffs agreed to when they signed up for Facebook. *See* Part II.A *infra*. Plaintiffs cannot claim that a contract was formed, assert two causes of action that are dependent on the terms of that contract, and then turn around and say that those contractual terms were too "buried" to be enforceable.[19]

In short, as the district court put it: "Having alleged that they understood and agreed to Facebook's policies, Plaintiffs cannot now claim to be ignorant of their contents." ER13.

4. Neither HIPAA Nor California Civil Code § 1798.91 Has Any Bearing on This Case.

In a final Hail Mary, plaintiffs argue that to obtain their legal consent, Facebook had to follow the detailed conditions set forth by HIPAA and California Civil Code § 1798.91. PB26-30. These statutes are designed "to improve . . . the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the

---

[19] If plaintiffs *had* made a contract-formation argument, it would have failed. Assent to online terms of service is generally satisfied where, as here, a website "user is required to affirmatively acknowledge the agreement before proceeding with use of the website." *Nguyen*, 763 F.3d 1171, 1176, 1179 (9th Cir. 2014) (declining to enforce the defendant's terms because they required "no affirmative action . . . by the website user," and specifically distinguishing Facebook's signup process).

electronic transmission of certain health information." HIPAA, Pub. L. No. 104-191, § 261, 110 Stat. 2021 (1996); *see* Cal. Civ. Code § 1798.91.

The district court rejected plaintiffs' HIPAA argument on the ground that "Facebook did not collect 'protected health information.'" ER14. This decision was correct, but the statutes are inapplicable for two other threshold reasons as well.

No private right of action. Neither HIPAA nor Section 1798.91 has a private right of action. *Webb v. Smart Doc. Sols., LLC*, 499 F.3d 1078, 1082 (9th Cir. 2007) ("HIPAA [ ] does not provide for a private right of action."); Cal. Civ. Code § 1798.91.[20] Nor have plaintiffs pointed to any case in which a court relied on one of these statutes to supply the consent standard for a *separate* statutory or common-law claim; to the contrary, courts have declined to incorporate HIPAA's provisions into other claims. *See, e.g.*, *Reed v. Columbia St. Mary's Hosp.*, 2014 WL 805919, at *3 (E.D. Wis. Feb. 28, 2014) ("invasion of privacy claim" "would [ ] fail" if it rested on the allegation that "defendant violated [HIPAA] by disclosing medical information without her consent"; "HIPAA does not furnish a private right

[20] Aside from the district court's decision below, Section 1798.91 has been mentioned in only a single reported case that did *not* involve a claim asserted under the statute. *See WorldMark v. Wyndham Resort Dev. Corp.*, 187 Cal. App. 4th 1017, 1034 (2010).

of action"); *Miller v. Elam*, 2011 WL 1549398, at *4 (E.D. Cal. Apr. 21, 2011) ("Because there is no private right of action under HIPAA, [a] HIPAA claim is not cognizable under 42 U.S.C. § 1983.").

The reason is obvious: If a plaintiff could import HIPAA's or Section 1798.91's statutory requirements into other causes of action—thereby *effectively* bringing a suit under those statutes—"[t]he absence of a private right of action . . . would be rendered meaningless." *Astra USA, Inc. v. Santa Clara Cty.*, 563 U.S. 110, 117-18 (2011). In *Astra*, the Supreme Court held that where the plaintiffs were unable to "sue under [a] statute" providing no right of action, "it would make scant sense to allow them to sue on a form contract implementing the statute." *Id.* at 114; *see Cuyler v. United States*, 362 F.3d 949, 952 (7th Cir. 2004) (it "clearly is not the law" that "every statute that specified a standard of care [is] automatically enforceable by tort suits for damages"—that "every statute in effect would create a private right of action"). The same principle applies here.

Facebook is not regulated by HIPAA. HIPAA applies only to certain "covered entit[ies]," 45 C.F.R. § 164.302—defined as (1) a "health plan," (2) a "health care clearinghouse," or (3) a "health care provider," *id.* § 160.103. Plaintiffs' complaint (but, again, not their appellate brief) acknowledges that Facebook is *not* a covered entity under HIPAA. ER257

¶ 214. It is therefore inconceivable that HIPAA's requirements could subject Facebook to any liability here. Given plaintiffs' acknowledgment that Facebook had no duty whatsoever to comply with HIPAA, they cannot credibly argue that the enforceability of Facebook's disclosures should be governed by HIPAA's requirements.

No protected health information. Finally, plaintiffs have not alleged disclosure of the *kind* of information protected by these statutes. HIPAA applies only to "protected health information," 45 C.F.R. § 164.502, defined as "*individually identifiable information*" that is "created or received by a health care provider," *id.* § 160.103 (emphasis added). Information is "individually identifiable" only if it "relates to the past, present, or future physical or mental health or condition of an *individual*." *Id.* (emphasis added). Similarly, Section 1798.91 applies only to "individually identifiable information . . . regarding the individual's medical history[] or medical treatment." Cal. Civ. Code § 1798.91(a)(2).

The complaint alleges no facts to support the conclusion that the information supposedly disclosed to Facebook is personally identifiable, sensitive, *or* related to plaintiffs' health. The communications alleged are limited to URLs that do not reveal plaintiffs' individual identities or relate these identities to any particular medical condition. As the district court

explained, and as shown in a chart submitted below (ER196), "[t]he URLS . . . point to pages containing information about treatment options for melanoma, information about a specific doctor, search results related to the phrase 'intestine transplant,' a wife's blog post about her husband's cancer diagnosis, and other publicly available medical information . . . that is accessible to the public at large." ER14.

Plaintiffs do not—and cannot—claim that their names, birthdates, billing information, or medical records were disclosed to Facebook. Plaintiffs do not allege that they have the medical conditions referenced in the URLs. Nor do they even allege that they were searching for information relating to their *own* medical issues, as opposed to conducting research for a friend or even a term paper. Because "[n]othing about the URLs . . . relates 'to the past, present, or future physical or mental health or condition *of an individual*,' . . . the stricter authorization requirements of HIPAA . . . do not apply." ER14-15 (quoting 45 C.F.R. § 160.103).

Plaintiffs baldly assert that it "should be obvious" that "Jane Doe I suffered from pain that stemmed from back problems, Jane Doe II's husband underwent an intestine transplant, and [ ] Winston Smith had melanoma." PB27. But whether those facts can be inferred from plaintiffs' allegations, they are far from "obvious" *from the URLs*. And

only the URLs (not the unadorned allegations in the complaint) were transmitted to Facebook from plaintiffs' browsers.

* * *

In sum, the absence of consent is undisputedly a requirement for each of plaintiffs' claims; their complaint concedes that they consented to the policies in Facebook's disclosures; and those disclosures informed plaintiffs of the exact conduct alleged in the complaint. The district court correctly held that all of plaintiffs' claims are barred for these reasons.

II. PLAINTIFFS' COMPLAINT FAILED TO ADEQUATELY PLEAD THE SPECIFIC ELEMENTS OF ANY OF THEIR CLAIMS.

Even if this Court disagrees with the district court's decision that plaintiffs' consent bars all of their claims, it should affirm because plaintiffs failed to plead other necessary elements of each cause of action. The district court did not have occasion to reach these issues.

A. Plaintiffs Failed to State a Claim For Breach of the Duty of Good Faith and Fair Dealing.

Plaintiffs argue that the district court erred by dismissing their claim that Facebook violated the "duty of good faith and fair dealing in its performance and enforcement" of the SRR, Data Policy, and Cookie Policy. PB30-33; ER289-90 ¶¶ 350-55. This claim fails because Facebook fully complied with these disclosures. *See* Part I *supra*.

It also fails because it is based *solely* on Facebook's alleged breach of the underlying contracts (ER290 ¶ 355) and is thus not cognizable under California law. "If the allegations [in an implied-covenant claim] do not go beyond the statement of a mere contract breach . . . they may be disregarded as superfluous as no additional claim is actually stated." *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990); *see also In re Facebook Internet Tracking Litig.*, 2017 WL 2834113, at *5 (N.D. Cal. June 30, 2017) ("*Facebook Internet*") (dismissing implied-duty claim against Facebook because "[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" (internal quotation marks omitted)). Although Facebook made this point below, plaintiffs ignore it on appeal; they simply complain about Facebook's supposed failure to comply with its *written* disclosures.

B. Plaintiffs Failed to State a Claim for Fraud.

Plaintiffs argue next that the district court erred in dismissing their claims of fraud under Sections 1572 and 1573 of the California Civil Code. PB33-34; ER291-92 ¶¶ 363-68.

A fraud claim has five elements: "(a) a misrepresentation (false representation, concealment, or nondisclosure); (b) knowledge of falsity (or

'scienter'); (c) intent to defraud, *i.e.*, to induce reliance; (d) justifiable reliance; and (e) resulting damage." *In re Estate of Young*, 160 Cal. App. 4th 62, 79 (2008). Federal Rule of Civil Procedure 9(b) requires that "the circumstances constituting fraud" be alleged with "particularity."

The complaint alleges only that Facebook "suppress[ed], with intent to deceive its users," facts about its collection and use of health-related communications, and that plaintiffs "relied on Facebook's false assertions in contracting with and using Facebook." ER291-92 ¶ 366. These bare conclusions do not satisfy Rule 12(b)(6), much less Rule 9(b).

First, as discussed above, Facebook made no misrepresentation or misleading omission. *See* Part I *supra*. Second, although plaintiffs asserted conclusorily that Facebook intended to "deceive" them, they do not allege that Facebook acted with intent to *induce* them to take any particular *action*—for example, to sign up for Facebook. *See Blickman Turkus, LP v. MF Downtown Sunnyvale, LLC*, 162 Cal. App. 4th 858, 869 (2008) ("It is not enough that the misstatement (or concealment) actually harmed the plaintiff; it must have been made by the defendant with the intent to *induce action* (or inaction) by the plaintiff."). Third, plaintiffs did not allege actionable reliance: either that absent the alleged misrepresentations, they "would not, in all reasonable probability, have

entered into the contract," *Engalla v. Permanente Med. Grp., Inc.*, 15 Cal. 4th 951, 976 (1997), or that any reliance was "justifiable" in light of Facebook's disclosures, *Young*, 160 Cal. App. 4th at 79. Finally, plaintiffs do not claim damage at all, let alone *as a result of the alleged fraud*. *See Moncada v. W. Coast Quartz Corp.*, 221 Cal. App. 4th 768, 776 (2013).[21]

C. Plaintiffs Failed to State a Claim Under the Federal Wiretap Act.

Plaintiffs contend that Facebook violated the Wiretap Act by intercepting the contents of their communications with the healthcare sites. PB34-48; ER266-67 ¶¶ 254-56. This statute provides a right of action against anyone who (1) "intercepts" the (2) "contents" of a "wire, oral, or electronic communication" using (3) a "device." 18 U.S.C. §§ 2510, 2511(1), 2520. Plaintiffs alleged none of these elements.

1. Facebook Never "Intercepted" a Communication.

A communication cannot be "intercepted" by one of its parties, because a party is the *direct recipient* of the communication. The Wiretap Act expressly provides that "[i]t shall not be unlawful . . . for a person . . . to intercept a wire, oral or electronic communication where such person is

---

[21] Plaintiffs' "constructive fraud" claim (ER292 ¶ 367) fails for the separate reason that they did not claim that Facebook had a duty to speak, which exists only when there is a "fiduciary or confidential" relationship. *Dealertrack, Inc. v. Huber*, 460 F. Supp. 2d 1177, 1183 (C.D. Cal. 2006).

a party to the communication." 18 U.S.C. § 2511(2)(d). This exemption is fundamental to the Act, which prohibits *wiretapping*, not receiving information. *See, e.g.*, *Marsh v. Zaazoom Sols., LLC*, 2012 WL 952226, at *17 (N.D. Cal. Mar. 20, 2012) ("[A]n 'interception' . . . could not exist where the plaintiff himself transmitted the information to [the defendant,] which was the second party to the communication.").

According to the complaint, when plaintiffs visited the healthcare sites, their browsers sent two *separate* communications: (1) a GET request to the healthcare site requesting that information be displayed on the browser; and (2) a separate GET request to Facebook accompanied by a referer header with the URL of the webpage on which Facebook content was to be loaded. ER214, 219-22 ¶¶ 32, 50-51; pp. 6-8 *supra*. Facebook did not receive the first communication, and plaintiffs expressly acknowledged that the second was sent *directly* from "the user's web-browser . . . to *Facebook's server*." ER220-21 ¶ 50(f) (emphasis added). "Facebook's acquisition of the plaintiff's communications to and from the medical websites was accomplished through a *separate channel* than the path of the *actual* communication between the users and the medical websites." ER266 ¶ 255 (emphases added).

This concession is dispositive, as the Third Circuit has held. In *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015) ("*Google Cookie*"), the court dismissed a substantively identical Wiretap Act claim because the defendants were parties to the communications; they had "acquired the plaintiffs' internet history information by way of *GET requests that the plaintiffs sent directly to the defendants*," and an "intended recipient of a communication is necessarily one of its parties." *Id.* at 142-43 (emphasis added).

Plaintiffs offer several responses. First, they cite *In re Pharmatrak*, 329 F.3d 9, 22 (1st Cir. 2003), for the proposition that a party can "intercept" a browser's communication if it receives a "[s]eparate, but simultaneous and identical, communication[]" from the browser. PB35, 39. But *Pharmatrak* did not address the Wiretap Act's "party" exception—§ 2511(2)(d)—because that exception was not before the court.[22] More broadly, *Pharmatrak* cannot be squared with this Court's precedents, which have held that an electronic communication can be "intercepted" only if it is "stop[ped], seize[d], or interrupt[ed] in progress or course." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002); *see*

[22] The same is true of *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010), cited at PB39.

also Bunnell v. MPAA, 567 F. Supp. 2d 1148, 1153 (C.D. Cal. 2007) (no interception where defendant configured plaintiffs' email software to simultaneously forward exact copies of emails to defendant); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (because "Amazon merely received the information transferred to it by [plaintiff]," it "acted as no more than the second party to a communication"; "[t]his is not an interception").

Second, plaintiffs argue that "Facebook's acquisition [of the information was] contemporaneous to, and in the middle of, the communications Plaintiffs exchanged with the health care entities." PB35-36. But the timing does not change the key fact: that plaintiffs' own browsers sent Facebook the referer header information directly. ER220-21 ¶ 50(f); *see Bunnell*, 567 F. Supp. 2d at 1153-54 (whether defendant "received the forwarded messages in milliseconds or days . . . ma[de] no difference"; they were not "intercepted" because they were sent by separate copy).

Third, plaintiffs draw an analogy in which Facebook "place[s] a bug on the plaintiffs' phones" and "then receive[s] the data directly from the phones." PB39. That, of course, is a *true* wiretap—tapping into the actual phone call with the third party. The situation here is different: Facebook

never "bugged" the actual communication with the healthcare website; it received a separate communication from the plaintiffs' own browsers. *See* ER220-21 ¶ 50(f). Courts have long held that even when a police officer *impersonates* the intended recipient of a phone call—unlike in this case, where Facebook engaged in no deception—that is not a "wiretap." *See United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964).

Finally, plaintiffs argue that Facebook was not a party to the communications because their browsers sent the referer headers to Facebook "without the user's knowledge or consent." PB43. The Third Circuit rejected this argument in *Google Cookie,* explaining that the plaintiffs' awareness (or lack of awareness) of their own browsers' communications was irrelevant: Because the Wiretap Act "is, after all, a *wiretapping* statute," "a deceit upon the sender" does not "affect[] the presumptive non-liability of parties." 806 F.3d at 143; *see also In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274-76 (3d Cir. 2016) (reaffirming *Google Cookie*'s holding);[23] *Facebook Internet*, 2017 WL

[23] Plaintiffs argue that the Third Circuit adopted a different position in *United States v. Eady*, 648 F. App'x 188 (3d Cir. 2016), which defined "party" as "a participant whose presence is known to the other parties contemporaneously with the communication." *Id.* at 191; *see* PB40-41. *Eady* was a criminal case about a person's recordings of phone calls among other people, 648 F. App'x at 189-90; it does not apply to communications

2834113, at *4 (because "two separate communications occur when someone visits a page where [Facebook code] is embedded," "Facebook has not 'intercepted' the communication"). A third-party server does not "intercept" a referer header every time the user was unaware that his browser sent it (and here, plaintiffs *were* aware and were *not* deceived).[24]

2. The Referer Headers Are Not "Content."

The Wiretap Act applies only to "information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). This Court has held that this definition does not cover "referer header information," because such information "functions like an 'address'"—it is "record information regarding the characteristics of the

---

between computers (browsers and servers) whose "presence" cannot be "known" to one another. In any event, *Eady* is unpublished and cited *Google Cookie* with approval. *Id.* at 192.

[24] Plaintiffs also argue that the Wiretap Act's "party" exception does not apply where a "'communication is intercepted for the purpose of committing any criminal or tortious act in violation of the . . . laws of the United States or of any State.'" 18 U.S.C. § 2511(2)(d); *see* PB45-47. But there is "no legal authority providing that [this provision] is triggered when . . . the tortious conduct is the alleged wiretapping itself." *Google Cookie*, 806 F.3d at 145. Plaintiffs pleaded no "facts to support an inference that [defendants] intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording." *Id.* *See also Sussman v. ABC*, 186 F.3d 1200, 1202 (9th Cir. 1999) (Section 2511(2)(d) exception applies where wiretapping is done to "facilitat[e] some *further* impropriety" (emphasis added)); *cf.* PB45.

message that is generated in the course of the communication.'" *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106-07 (9th Cir. 2014).

Plaintiffs argue that the referer headers here are different because they include the search queries that the plaintiffs sent to the medical websites. PB37. That misses the point. By definition, a URL does not convey the "meaning" of the communication with the host server; it simply identifies the *location* of the requested webpage on the Internet. Indeed, *Zynga* expressly contemplated that a referer header could disclose that a person viewed the "page of a gay support group," but it still held that such URLs "function[] like an 'address,'" not content. 750 F.3d at 1107-08.[25]

3. Plaintiffs Have Not Alleged a "Device."

Plaintiffs also failed to sufficiently allege the use of an "electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The complaint offers a bare list of items that it claims to be "devices": (a) "cookies"; (b) "Plaintiffs' web-browsers"; (c) "Plaintiffs' computing devices"; (d) "Facebook's

[25] As plaintiffs point out (PB37), *Zynga* did say in dicta that "[u]nder *some* circumstances, a user's request to a search engine for specific information could constitute . . . the contents of a communication. 750 F.3d at 1108-09 (emphasis added) (discussing "dicta about URL information" in *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008)). But the Court did not identify those circumstances. *Google Cookie* contains similar dicta, but did not resolve the issue because it dismissed the case under the "party" exception.

web-servers"; (e) "[t]he web-servers of the medical websites"; (f) "computer code deployed by Facebook"; and even (g) "[t]he plan Facebook carried out to effectuate the tracking and interception of user communications." ER268 ¶ 261; *see* PB47-48. But none of these items "can be used to intercept" a communication, as required under the statute. 18 U.S.C. § 2510(5).[26] A cookie is a small piece of text; it cannot intercept anything. Neither a browser, nor a server, nor code is a "device." *See, e.g.*, *Crowley*, 166 F. Supp. 2d at 1269 ("drive or server on which the e-mail was received" was not a device under Wiretap Act); *Potter v. Havlicek*, 2008 WL 2556723, at *8 (S.D. Ohio June 23, 2008) ("the word 'device' does not encompass software"; it is a "piece of equipment or a mechanism designed to serve a special purpose or perform a special function"). And if a "plan" could qualify, the statutory requirement would be meaningless.[27]

D. Plaintiffs Failed to State a Claim under CIPA

Plaintiffs asserted claims under two provisions of CIPA: Sections 631 and 632. *See* ER279-82 ¶¶ 305-21; PB48-50. Both are deficient.

---

[26] Plaintiffs invoke "the dictionary definition" of "device" (PB47), but that must yield to the *statutory* definition.

[27] Plaintiffs cite two cases. PB48. *In re Carrier IQ* did not consider whether software is a "device." 78 F. Supp. 3d at 1067. And *Szymuszkiewicz* is inconsistent with this Circuit's precedents.

Section 631(a). Like the Wiretap Act, Section 631(a) "prohibits the interception of wire communications and disclosure of the contents of such intercepted communications." *Tavernetti v. Super. Ct.*, 22 Cal. 3d 187, 190 (1978). It regulates "eavesdropping, or the secret monitoring of conversations by third parties." *Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985); *see Google Cookie*, 806 F.3d at 152. This claim fails for three reasons.

First, as with the federal wiretapping claim, this case does not involve "eavesdropping," because plaintiffs' own allegations establish that Facebook was a party to the relevant communications. *See Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (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."); ER220-21 ¶ 50(f); Part II.C.1 *supra*.[28] Second, plaintiffs did not allege that Facebook acquired the "contents" of any message. *See* Cal. Penal Code § 631(a); Part II.C.2 *supra*. Third, plaintiffs have not alleged that Facebook acquired their communications using "a machine, instrument, or contrivance" (*id.*); their claims are based

---

[28] *See also Google Cookie*, 806 F.3d at 152 (district court correctly "dismissed the [plaintiffs'] § 631(a) claim for the same reasons that it dismissed the plaintiffs' wiretapping claim": because "Google was itself a party to all the electronic transmissions"); *See Facebook Internet*, 2017 WL 2834113, at *5 ("Plaintiffs' CIPA claims . . . fail for the same reason [as their claim under the Wiretap Act."].).

on cookies—small pieces of text that sit idly on a user's computer until contacted by the server.[29]

Section 632(a). CIPA creates a cause of action against a "person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, . . . by means of a telegraph, telephone, or other device, except a radio." Plaintiffs *did* consent, and this claim fails for two additional reasons as well.

First, plaintiffs' communications were in no way "confidential"; they were transmitted automatically by plaintiffs' own browsers when they visited the healthcare sites. Plaintiffs concede that "California courts have held that Internet communications are not confidential . . . in certain circumstances," but argue that those decisions do not apply where "one party to each of the communications at issue"—here, the healthcare defendants—"explicitly promised not to disclose it." PB49. The healthcare

---

[29] Plaintiffs assert that CIPA "does not require the use of a 'device'" but rather "prohibits interceptions that occur 'by means of any machine, instrument, or contrivance, *or in any other manner*.'" PB48-49. But "[w]here general words [in a statute] follow the enumeration of specific classes of things, the general words must be construed as restricted to things of the same type as those specifically enumerated." *Aqua-Marine Constructors, Inc. v. Banks*, 110 F.3d 663, 677 (9th Cir. 1997). Thus, the phrase "in any other manner" must mean something *akin* to a "machine, instrument, or contrivance." Plaintiffs do not allege such a mechanism.

defendants made no such promise (*see* pp. 23-24 & n.9 *supra*), Facebook can be held liable only for its own promises (*see* pp. 24-25 *supra*), and ultimately, neither party's disclosures could make plaintiffs' communications "confidential": "decisions from the California appellate courts . . . suggest that internet-based communications *cannot* be confidential" under CIPA because they are easily recorded and shared. *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *22 (N.D. Cal. Sept. 26, 2013) (emphasis added); *see Facebook Internet*, 2017 WL 2834113, at *5.[30]

Second, plaintiffs have not alleged that Facebook used an "electronic amplifying or recording device." Indeed, the statute's specific reference to "a telegraph, telephone, or other device, except a radio," shows that it applies to traditional recording mechanisms, not idle text like cookies.

[30] *See, e.g.*, *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010) (defendant's instant messages not confidential, even though he intended that they be kept between him and recipient, because they "could have easily been shared or viewed by . . . any computer user with whom [the recipient] wanted to share the communication"); *People v. Griffitt*, 2010 WL 5006815, at *6 (Cal. Ct. App. Dec. 9, 2010) (rejecting Section 632 claim because "[e]veryone who uses a computer knows that the recipient of e-mails and participants in chat rooms can . . . share them with whoever they please, forward them or otherwise send them to others").

E. Plaintiffs Failed to State a Claim for Intrusion on Seclusion or Constitutional Invasion of Privacy.

Plaintiffs' two other privacy-related claims (PB50-53; ER276-79, 282-85 ¶¶ 295-304, 322-31) have similar elements and are commonly considered in tandem. *See Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009). "First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy." *Id.* at 286. "Second, the intrusion must occur in a manner highly offensive to a reasonable person." *Id.* "The gravamen is the mental anguish sustained when both conditions" exist. *Id.* Neither exists here.

1. Plaintiffs Could Not Reasonably Expect that the Identities of Websites They Visit Would Be Private.

This Court has squarely held that "Internet users have no expectation of privacy in [the identities of] . . . the websites they visit.'" *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). At least when it comes to the location of those sites, 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.*; *see Facebook Internet*, 2017 WL 2834113, at *6 ("Plaintiffs have not

established that they have a reasonable expectation of privacy in the URLs of the pages they visit.").

In addition, plaintiffs failed to take the available measures to safeguard their information. *See Med. Lab. Mgmt. Consultants v. ABC, Inc.*, 306 F.3d 806, 813 (9th Cir. 2002). Facebook gave them the opportunity to "manage the content and information [they] share[d]" (ER308), but they do not allege that they took any actions to prevent Facebook from collecting the challenged information. *See Facebook Internet*, 2017 WL 2834113, at *6 ("Plaintiffs could have taken steps to keep their browsing histories private.").

Plaintiffs argue, first, that they "alleged reasonable expectations of privacy through their legally protected privacy interests and the health care entities' explicit promises." PB52. That is circular—it *assumes* that plaintiffs have "legally protected privacy interests" relevant here. And as to the purported "promises" of the healthcare defendants, the assertion is false. *See* pp. 23-24 & n.9 *supra*. Plaintiffs argue next that the Supreme Court held in *Riley* that "Americans have a reasonable expectation of privacy in the type of data at issue in this case." PB52. They do not even bother specifying a page in *Riley*, and it held nothing of the sort; as discussed above, *Riley* addressed the applicability of a Fourth Amendment

exception to a search of a cell phone, not whether there is a "reasonable expectation of privacy" in the "data at issue." *See* pp. 33-34 *supra*.

2. Facebook's Conduct Was Not "Offensive"—Let Alone "Highly Offensive."

The "highly offensive" element of a privacy claim is demanding: It requires "an exceptional kind of prying into another's private affairs," such as "taking the photograph of a woman in the hospital with a 'rare disease that arouses public curiosity'" or "using a telescope to look into someone's upstairs bedroom window for two weeks and taking 'intimate pictures.'" *Med. Lab.*, 306 F.3d at 819. And naturally, conduct motivated by "legitimate business reasons"—as opposed to "socially repugnant . . . reasons"—fails this test. *Hernandez*, 47 Cal. 4th at 286, 297; *see also Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) (in intrusion-on-seclusion case, dismissing as "routine commercial behavior" the unauthorized procurement of plaintiff's home address to mail him marketing materials).

The ordinary commercial activities described in the complaint fall far short of these standards. Plaintiffs do not allege "the absence of any reasonable justification or beneficial motivation," *Hernandez*, 47 Cal. 4th at 297; to the contrary, they claim that Facebook uses their information for the exact reason disclosed in its Data Policy: to show people "relevant

ads." ER305. Courts in this Circuit have repeatedly rejected privacy claims based on such conduct. *See, e.g.*, *Facebook Internet*, 2017 WL 2834113, at *6; *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) ("Courts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of the social norms."); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (no privacy claim where LinkedIn allegedly disclosed user browsing history to third parties; "[e]ven disclosure of personal information, including social security numbers, does not constitute an 'egregious breach of social norms' [sufficient] to establish an invasion of privacy").

Plaintiffs again respond with naked assertions. They argue that "Congress and every state" have made a "'policy' decision" that Facebook's conduct is offensive "through the passage of criminal and civil laws designed to protect communications and health privacy." PB52. But the issue is not whether the law generally protects "communications and health privacy" on the Internet; it is whether Facebook's *specific conduct*—the collection of referer headers—is "highly offensive." And courts in this

Circuit have unanimously "refused" to characterize such conduct in this way. *Google Privacy Policy*, 58 F. Supp. 3d at 985.[31]

CONCLUSION

Plaintiffs agreed to a detailed, "valid contract" that expressly permitted Facebook to do what countless other Internet services do every day: collect and use information about people's web traffic to (among other disclosed reasons) improve advertising and measure its performance. There is no question that the privacy of Internet users is critically important. And that is why Facebook took all necessary steps to disclose its practices and protect its users' privacy. The Court should affirm.

---

[31] The cases plaintiffs cite (PB53) are inapposite. In *Google Cookie*, the plaintiffs alleged that Google had "overrid[den] the plaintiffs' cookie blockers" while assuring users that they would be effective, which "raise[d] different issues than tracking or disclosure alone." 806 F.3d at 150; *see also Facebook Internet*, 2017 WL 2834113, at *7 (distinguishing *Google Cookie* on this basis). In *Nickelodeon*, the defendant allegedly collected personal, private information from children despite telling their parents that they would not collect "ANY personal information about your kids." 827 F.3d at 269. In *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014), the intrusion claim was based on the alleged "surreptitious theft of personal contact information" from a cell phone. *Id.* at 1061.

Respectfully submitted,

/s/ Lauren R. Goldman

Lauren R. Goldman
Michael Rayfield
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
(212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

John Nadolenco
MAYER BROWN LLP
350 South Grand Avenue
Los Angeles, CA 90071
(213) 229-9500
jnadolenco@mayerbrown.com

Counsel for Defendant-Appellant

Dated: December 18, 2017

STATEMENT OF RELATED CASES

Counsel for appellee does not know of any case pending in this Court related to this one.

/s/ Lauren R. Goldman

Form 8. Certificate of Compliance Pursuant to 9th Circuit Rules 28.1-1(f), 29-2(c)(2) and (3), 32-1, 32-2 or 32-4 for Case Number 17-16206

Note: This form must be signed by the attorney or unrepresented litigant *and attached to the end of the brief.*

I certify that (*check appropriate option*):

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 28.1-1.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☒ This brief complies with the length limits permitted by Ninth Circuit Rule 32-1.
The brief is [13386] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 32-2(b).
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable, and is filed by (1) ☐ separately represented parties; (2) ☐ a party or parties filing a single brief in response to multiple briefs; or (3) ☐ a party or parties filing a single brief in response to a longer joint brief filed under Rule 32-2(b). The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the longer length limit authorized by court order dated [ ]
The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6). The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable.

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 32-2 (a) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32 (f), if applicable. The brief's type size and type face comply with Fed. R .App. P. 32(a)(5) and (6).

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 29-2 (c)(2) or (3) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits set forth at Ninth Circuit Rule 32-4.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

Signature of Attorney or Unrepresented Litigant: s/ Lauren R. Goldman

Date: 12/18/2017

("s/" plus typed name is acceptable for electronically-filed documents)

CERTIFICATE OF SERVICE

I hereby certify that on December 18, 2017, the foregoing brief was served electronically via the Court's CM/ECF system upon all counsel of record.

Dated: December 18, 2017 /s/ Lauren R. Goldman