UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

WINSTON SMITH, et al.,

Plaintiffs,

v.

FACEBOOK, INC., et al.,

Defendants.

Case No. 5:16-cv-01282-EJD

ORDER GRANTING DEFENDANTS' MOTION TO DISMISS

Re: Dkt. No. 96

Plaintiffs allege that the Healthcare Defendants[1] disclosed information about Plaintiffs' web browsing activity to Defendant Facebook, Inc. Defendants move to dismiss under Fed. R. Civ. P. 12(b)(1), 12(b)(2), and 12(b)(6). Defendants' motion will be GRANTED because this Court lacks personal jurisdiction over the Healthcare Defendants and because Plaintiffs consented to Facebook's conduct.

[1] The "Healthcare Defendants" are seven hospitals and healthcare organizations: American Cancer Society, Inc.; American Society of Clinical Oncology, Inc.; Melanoma Research Foundation; Adventist Health System Sunbelt Healthcare Corporation; BJC Health System d/b/a BJC HealthCare; Cleveland Clinic of Texas; and University of Texas—MD Anderson Cancer Center.

I. BACKGROUND

A. The Parties

The Healthcare Defendants operate websites that publish information about medical conditions and treatments. Compl. ¶¶ 2–3, 107–206, Dkt. No. 1. For instance, visitors to http://www.cancer.net/ (operated by Defendant American Society of Clinical Oncology) can read articles on topics like cancer treatment, types of cancer, and recent research in the field.

Facebook is a "free social networking service that allows people to connect and share content." Defs.' Mot. to Dismiss ("MTD") 1, Dkt. No. 96. It makes money by letting third parties show ads to its users. Id. To improve ad targeting, it "collects information about people's browsing activities, mainly on Facebook but also on third-party websites that host Facebook tools and features." Id.

Plaintiffs are registered Facebook users who visited the Healthcare Defendants' websites. Compl. ¶¶ 2, 6–8.

B. How Visitors Communicate with the Healthcare Defendants' Websites

To access one of the Healthcare Defendants' websites, a visitor might type www.cancer.net into the address bar of her web browser and click the "Go" button. The browser then sends a message called a "GET request"[2] to the web server associated with that address. The GET request specifies the page that the visitor wants to retrieve, like "the home page of the website located at cancer.net." It also provides information about the visitor, like her language, operating system, browser settings, and other technical parameters.

The web server responds with code that tells the visitor's browser how the page should appear. For example, the code might instruct the browser to display the phrase "timely, comprehensive, oncologist-approved information" as italic white text on a blue background. It might also contain links, images, videos, and other content.

[2] The mechanics of GET requests are described at Compl. ¶¶ 21–52 and MTD 3–5; see also R. Fielding et al., RFC 2068: Hypertext Transfer Protocol—HTTP/1.1, Internet Engineering Task Force (Jan. 1997), https://www.ietf.org/rfc/rfc2068.txt [https://perma.cc/2X3E-SYQV/].

The user might click a link to visit another page. That click triggers a second GET request that is similar to the first, but it requests a page at a new URL—for instance, it might ask for http://www.cancer.net/cancer-types/ instead of http://www.cancer.net/. The second request includes a "referer header" that contains the address of the first page.

C. How Facebook Tracks Visitors' Web Browsing Activity

Website owners can add Facebook functionality to their sites using tools that Facebook provides. Id. ¶¶ 78, 84; see also Social Plugins, Facebook for Developers, https://developers.facebook.com/docs/plugins/ [https://perma.cc/NL8B-859K/] (last visited April 25, 2017). For example, sites can add "Like" or "Share" buttons that let visitors share content on Facebook. Someone reading an article about cancer treatment could click a "Share" button to post the article to Facebook.

To display a Facebook button, a website owner embeds a code snippet that Facebook provides. When someone visits a page where a Facebook button is embedded, the visitor's browser makes two GET requests. First, it makes an ordinary request to load the page, as explained above. Second, the Facebook code snippet triggers a background request to Facebook's servers. The Facebook server responds with code that makes the button appear on the page. The communication with Facebook happens silently; a savvy user could use tools to watch her browser exchange information behind the scenes, but the connection to Facebook's servers is invisible by default. The request to Facebook includes a referer header containing the address of the page where the Facebook button is embedded. So, when someone reads a page on cancer.net that contains a Facebook "Like" button, Facebook knows which page that person visited.

Facebook uses these background requests to uniquely identify people. It uses at least three identification techniques. First, a visitor will likely have a unique IP address[3] that stays the same as she visits multiple pages. The IP address is included in each GET request, which enables Facebook to keep track of the page visits associated with that address. Id. ¶¶ 27–29, 85, 102.

[3] However, IP addresses can be shared among several users. For instance, users on the same Wi-Fi network will have the same public IP address.

Second, Facebook puts cookies on visitors' computers. It uses these cookies to store information about each visitor—for instance, the "c_user" cookie is a unique identifier, and the "lu" cookie identifies the last Facebook user who logged in using that browser. Id. ¶¶ 40–52, 82–85, 120. Like IP addresses, cookies are included with each request that the visitor's browser makes to Facebook's servers. Third, Facebook uses browser fingerprinting. Web browsers have several attributes that vary between users, like the browser software version, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777—and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Id. ¶¶ 96, 97. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party page.

Using these techniques, Facebook can identify individual users and watch as they browse third-party websites like cancer.net.

D. Plaintiffs' Allegations

Plaintiffs allege that Facebook used the techniques described above to uniquely identify Plaintiffs (and class members) and track the pages they visited on the Healthcare Defendants' websites. Id. ¶¶ 85, 97, 102. Based on this conduct, they bring causes of action against Facebook and the Healthcare Defendants for violations of the Wiretap Act, 18 U.S.C. § 2520(a) (id. ¶¶ 249–94), the California Invasion of Privacy Act, Cal. Penal Code §§ 631(a), 632 (id. ¶¶ 305–21), and privacy protections under the California Constitution (id. ¶¶ 322–31), as well as common-law tort claims for intrusion upon seclusion (id. ¶¶ 295–304) and negligence per se (id. ¶¶ 332–37). They also bring causes of action against Facebook (but not the Healthcare Defendants) for breach of the duty of good faith and fair dealing (id. ¶¶ 348–62), fraud (id. ¶¶ 363–68), and quantum meruit (id. ¶¶ 396–72). Finally, they bring causes of action against the Healthcare Defendants (but not Facebook) for negligent disclosure of confidential information (id. ¶¶ 338–42) and breach of the fiduciary duty of confidentiality (id. ¶¶ 343–47).

II. LEGAL STANDARDS

A. Rule 12(b)(1)

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

B. Rule 12(b)(2)

Fed. R. Civ. P. 12(b)(2) allows dismissal for lack of personal jurisdiction. When the motion to dismiss is a defendant's first response to the complaint, the plaintiff need only make a prima facie showing that personal jurisdiction exists. See Data Disc, Inc. v. Sys. Tech. Assocs., Inc., 557 F.2d 1280, 1285 (9th Cir. 1977). While a plaintiff cannot " 'simply rest on the bare allegations of its complaint,' uncontroverted allegations in the complaint must be taken as true" and "[c]onflicts between parties over statements contained in affidavits must be resolved in the plaintiff's favor." Schwarzenegger v. Fred Martin Motor Co., 374 F.3d 797, 800 (9th Cir. 2004) (quoting Amba Marketing Sys., Inc. v. Jobar Int'l, Inc., 551 F.2d 784, 787 (9th Cir. 1977), and citing AT&T v. Compagnie Bruxelles Lambert, 94 F.3d 586, 588 (9th Cir. 1996)).

C. Rule 12(b)(6)

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

III. DISCUSSION

Defendants argue that Plaintiffs' claims should be dismissed because (among other reasons) this Court lacks personal jurisdiction over the Healthcare Defendants and because Plaintiffs consented to Facebook's conduct. The Court agrees.

A. This Court lacks personal jurisdiction over the Healthcare Defendants.

Neither Plaintiffs nor the Healthcare Defendants are California residents (Compl. ¶¶ 6–9, 10–16), but Plaintiffs contend that the Healthcare Defendants are subject to personal jurisdiction in California because they participate in sending Plaintiffs' data to Facebook. Pls.' Opp'n to Defs.' Mot. to Dismiss ("Opp'n") 12, Dkt. No. 105 (arguing that the Healthcare Defendants "continuously and systematically send users' sensitive medical information to Facebook, which is headquartered in California, each and every time a user sends a GET request to the health care Defendants' respective websites").

When no applicable federal statute authorizes personal jurisdiction, a district court applies the law of the state where the court sits. Fed. R. Civ. P. 4(k)(1)(A); Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1320 (9th Cir. 1998). California's long-arm statute has the same due process requirements as the federal long-arm statute. Schwarzenegger, 374 F.3d at 801. Under the Due Process Clause, nonresident defendants must have "minimum contacts" with the forum state such that the exercise of personal jurisdiction "does not offend traditional notions of fair play and substantial justice." Int'l Shoe Co. v. Wash., 326 U.S. 310, 316 (1945). Where a defendant moves to dismiss a complaint for lack of personal jurisdiction, the plaintiff bears the burden of demonstrating that jurisdiction is appropriate. Sher v. Johnson, 911 F.2d 1357, 1361 (9th Cir. 1990).

i. Specific Personal Jurisdiction

Specific personal jurisdiction exists when (1) the non-resident defendant purposefully directs activities to the forum or purposefully avails itself of the privilege of conducting activities in the forum; (2) the claim arises out of or relates to the defendant's forum-related activities; and (3) the exercise of jurisdiction is reasonable. Schwarzenegger, 374 F.3d at 802. "If any of the three

requirements is not satisfied, jurisdiction in the forum would deprive the defendant of due process of law." Omeluk v. Langsten Slip & Batbyggeri Al S, 52 F.3d 267, 270 (9th Cir. 1995). The plaintiff bears the burden of satisfying the first two prongs. Schwarzenegger, 374 F.3d at 802.

Purposeful availment and purposeful direction are distinct concepts. Id. "A showing that a defendant purposefully availed himself of the privilege of doing business in a forum state typically consists of evidence of the defendant's actions in the forum, such as executing or performing a contract there." Id. (emphasis added) (quoting Hanson v. Denckla, 357 U.S. 235, 253 (1958)). In return for availing itself of the benefits and protections of the forum state's laws, the defendant must "submit to the burdens of litigation in that forum." Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476 (1985).

By contrast, a "showing that a defendant purposefully directed his conduct toward a forum state . . . usually consists of evidence of the defendant's actions outside the forum state that are directed at the forum, such as the distribution in the forum state of goods originating elsewhere." Schwarzenegger, 374 F.3d at 803 (emphasis added). Due process allows "the exercise of personal jurisdiction over a defendant who 'purposefully direct[s]' his activities at residents of a forum, even in the 'absence of physical contacts' with the forum." Id. (quoting Burger King, 471 U.S. at 476).

Nothing in Plaintiffs' allegations suggests that the Healthcare Defendants purposefully availed themselves of the benefits of doing business in California. Rather, Plaintiffs allege that the Healthcare Defendants "purposefully directed their activity to California" by "send[ing] users' sensitive medical communications to Facebook every time a user sends a GET request to the health care Defendants' respective websites." Opp'n 12.

To evaluate purposeful direction, courts in the Ninth Circuit apply the three-part test from Calder v. Jones, 465 U.S. 783 (1984). See Pebble Beach Co. v. Caddy, 453 F.3d 1151, 1156 (9th Cir. 2006) (applying the Calder test). To satisfy the Calder test, the defendant "must have (1) committed an intentional act, which was (2) expressly aimed at the forum state, and (3) caused harm, the brunt of which is suffered and which the defendant knows is likely to be suffered in the

forum state." Pebble Beach, 453 F.3d at 1156.

Plaintiffs have satisfied the first prong ("an intentional act"). The Healthcare Defendants acted intentionally when they embedded Facebook code on their websites.

Under the second prong ("expressly aimed at the forum state"), Plaintiffs' theory is that the Healthcare Defendants expressly aimed their conduct at California by "continuously and systematically send[ing] users' sensitive medical communications to Facebook . . . ." Opp'n 12.

Facebook's tracking is indeed continuous and systematic. Every time someone views a page containing a Facebook button on one of the Healthcare Defendants' sites (or elsewhere on the internet), Facebook logs that visit and correlates it with the visitor's other activity. Systematic tracking is the point: Facebook improves its ad targeting, and makes more money, by gathering comprehensive information about its users' browsing habits.

But the comprehensiveness of Facebook's tracking does not establish that the Healthcare Defendants "send" information to Facebook, as Plaintiffs suggest. More accurately, they embed code that creates a new connection between a visitor's browser and a Facebook server. The website's decision to embed the code allows that connection to occur, but the connection happens independently. Besides triggering a second GET request in the user's browser, the Healthcare Defendants play no part in the exchange of data between Facebook and Plaintiffs.

Plaintiffs also admit that they do not know whether the Healthcare Defendants were aware that Facebook used embedded buttons to track their visitors. Compl. ¶ 105. Personal jurisdiction cannot be based on the possibility that the Healthcare Defendants' acts could have foreseeable effects in California. See Bancroft & Masters, Inc. v. Augusta Nat'l Inc., 223 F.3d 1082, 1087 (9th Cir. 2000) (holding that Calder "cannot stand for the broad proposition that a foreign act with foreseeable effects in the forum state always gives rise to specific jurisdiction"). Personal jurisdiction requires "something more"—namely, "wrongful conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state." Id. The Healthcare Defendants cannot have "targeted" activity at known California residents if they were unaware that the activity was happening.

But even if the Healthcare Defendants knew that Facebook tracks users via "Share" and "Like" buttons, Plaintiffs' allegations do not support the conclusion that the Healthcare Defendants targeted their activities at Plaintiffs in California. Without "something more," embedding third-party code cannot confer personal jurisdiction over a website operator in the forum where the third party resides. 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. Under Plaintiffs' theory, every website operator that embeds one of these tools could be haled into court where the third-party company resides. Personal jurisdiction cannot reasonably stretch so far. This Court is aware of no other case that raises the same question, but courts have reached the same conclusion in related scenarios. See, e.g., NuboNau, Inc. v. NB Labs, Ltd, No. 10-cv-2631-LAB (BGS), 2012 WL 843503, at *6 (S.D. Cal. Mar. 9, 2012) ("the Court doesn't find that merely engaging Twitter and Facebook to promote one's business constitutes purposeful direction at California, simply because Twitter and Facebook happen to be based there"); DFSB Collective Co. Ltd. v. Bourne, 897 F. Supp. 2d. 871, 884 (N.D. Cal. 2012) (holding that the defendant did not purposefully direct activities at California by "utiliz[ing] accounts on California-headquartered Internet companies Facebook, hi5.com, DeviantArt, and 4Shared to direct traffic to his Websites"); see also CollegeSource, Inc. v. AcademyOne, Inc., 653 F.3d 1066, 1075–76 (9th Cir. 2011) ("If the maintenance of an interactive website were sufficient to support general jurisdiction in every forum in which users interacted with the website, the eventual demise of all restrictions on the personal jurisdiction of state courts would be the inevitable result.") (internal quotation marks and citation omitted).

Because they did not purposefully direct activities to California or purposefully avail themselves of the privilege of conducting business in California (Schwarzenegger, 374 F.3d at 802), this Court lacks personal jurisdiction over the Healthcare Defendants.

ii. General Personal Jurisdiction

General personal jurisdiction exists when a corporation's "affiliations with the State are so 'continuous and systematic' as to render [it] essentially at home in the forum State." Daimler AG

v. Bauman, 134 S. Ct. 746, 754 (2014). Plaintiffs argue that general personal jurisdiction arises from the fact that the Healthcare Defendants "continuously and systematically send users' sensitive medical communications to Facebook"—that is, from the same activity that Plaintiffs believe creates specific personal jurisdiction. Opp'n 12. Since that activity is insufficient to establish specific personal jurisdiction, it falls well short of establishing that the Healthcare Defendants are "essentially at home" in California. See Teras Cargo Transp. (Am.), LLC v. Cal Dive Int'l (Australia) Pty Ltd., No. 15-CV-03566-JSC, 2015 WL 6089276, at *7 (N.D. Cal. Oct. 16, 2015) ("the threshold level of contacts required for general jurisdiction is even higher than is required for specific jurisdiction").

iii. Forum Selection Clause

Plaintiffs argue that "Facebook users, including web developers and operators like the health care Defendants, submit to this Court's personal jurisdiction for the purpose of all claims related to Facebook." Opp'n 13. Their argument is based on the forum selection clause in Facebook's Terms of Service:

> You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims.

Compl. Ex. A at 3.

This clause applies only to disputes between the Healthcare Defendants and Facebook. See id. (stating that the forum shall be the Northern District of California for "any claim, cause of action or dispute . . . you have with us") (emphasis added). It does not create personal jurisdiction in California over the Healthcare Defendants when they are sued by third parties, even if Facebook is also a defendant.

B. Plaintiffs consented to Facebook's tracking activity.

Plaintiffs agreed to several Facebook policies when they signed up for accounts (Compl. ¶¶ 58–78), including Facebook's Data Policy:

> We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

Compl. Ex. A at 2. Facebook's Cookie Policy also contains several broad disclosures, including information about how Facebook tracks users to improve its ad targeting:

> Cookies are small files that are placed on your browser or device by the website or app you're using or ad you're viewing. Pixel tags (also called clear GIFs, web beacons, or pixels) are small blocks of code on a webpage or app that allow them to do things like read and place cookies and transmit information to us or our partners. The resulting connection can include information such as a device's IP address, the time a person viewed the pixel, an identifier associated with the browser or device and the type of browser being used.
>
> . . .
>
> Things like Cookies and similar technologies (such as information about your device or a pixel on a website) 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 and partners, can serve you ads that may be interesting to you on Facebook Services or other websites and mobile applications.

Compl. Ex. C at 1–2.

Plaintiffs give several reasons why they believe these policies do not adequately disclose that Facebook collects information about its users when they visit third-party websites. First, Plaintiffs argue that Facebook's disclosure is "buried in a Terms of Service or Privacy Policy that may never be viewed." Opp'n 19 (quoting Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014)). But Plaintiffs acknowledge in their complaint that the Facebook policies, including the Data Policy and the Cookie Policy, "constitute[] a valid contract." Compl. ¶ 59. Also, in their cause of action against Facebook for fraud, Plaintiffs allege that they relied on Facebook's assertions in the very same contracts. Compl. ¶¶ 366–67 ("Facebook violated § 1572, actual fraud, through its suppression, with the intent to deceive its users, of the facts that it . . .

tracks and intercepts user communications with health-care related websites. . . . Plaintiffs relied on Facebook's false assertions in contracting with and using Facebook."). Having alleged that they understood and agreed to Facebook's policies, Plaintiffs cannot now claim to be ignorant of their contents.

Plaintiffs also argue that Facebook's policies are too "vague" and "broad" to be enforceable. Opp'n 19–20. Yet Facebook's Data Policy discloses the precise conduct at issue in this case: "We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button . . .)." Compl. Ex. A at 2 (emphasis added). The meaning of "information" might be broad—it could include any data transmitted when the visitor's browser connects to Facebook's servers, including cookies, referer headers, and all the parts that combine to form a browser fingerprint. But, as Defendants point out, "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); see MTD 17. Several courts have held that similar disclosures constitute adequate notice of tracking activity. See, e.g., Mortensen v. Bresnan Commc'n, L.L.C., No. CV 10-13-BLG-RFC, 2010 WL 5140454, at *5 (D. Mont. Dec. 13, 2010) (holding that customers agreed to allow their internet service provider to send all of their network traffic to a third party, because the provider disclosed that customers' "electronic transmissions would be monitored and would in fact be transferred to third-parties for the purposes of providing 'content or services' "); Del Vecchio v. Amazon.com, Inc., No. C11-366RSL, 2012 WL 1997697, at *6 (W.D. Wash. June 1, 2012) (holding that the defendant "notif[ied] visitors that it will take the very actions about which Plaintiffs now complain: place browser and Flash cookies on their computers and use those cookies to monitor and collect information about their navigation and shopping habits"); Perkins, 53 F. Supp. 3d at 1214 (holding that LinkedIn adequately disclosed that it collected email addresses from users' contact lists when they created accounts, because it told users that "LinkedIn.com is asking for some information from your Google Account," including the users' "Google Contacts").

Plaintiffs suggest that because "sensitive medical information" is involved, Facebook must

meet a stricter disclosure standard under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§ 1320d–1320d-8 (and under similar state-law provisions in Cal. Civ. Code § 1798.91). Opp'n 14–17. Under HIPAA, "protected health information" is defined as "individually identifiable" information that is "created or received by a health care provider" (or similar entities) that "[r]elates to the past, present, or future physical or mental health or condition of an individual." 45 C.F.R. § 160.103. To disclose protected health information about a person, a the disclosing party must obtain the person's signed, written consent (among other requirements). 45 C.F.R. § 164.508. According to Plaintiffs, the disclosures in Facebook's policies do not meet HIPAA's heightened authorization requirements.

Plaintiffs' argument fails because Facebook did not collect "protected health information." As discussed above, requests to Facebook's servers can include several types of information about the user, including browser settings, language, operating system, IP address, and the contents of cookies that Facebook has set. But that same information is transmitted to Facebook every time a user visits any page on the internet that contains a Facebook button. Nothing about that information relates specifically to Plaintiffs' health. The only difference between those requests is the referer header, which contains the URL of the page where the Facebook button is embedded. The URLs at issue in this case point to pages containing information about treatment options for melanoma,[4] information about a specific doctor,[5] search results related to the phrase "intestine transplant,"[6] a wife's blog post about her husband's cancer diagnosis,[7] and other publicly available medical information. See MTD Ex. A (compiling a list of the URLs that Plaintiffs allege were disclosed to Facebook). These pages contain general health information that is accessible to the public at large. The same pages are available to every computer, tablet, smartphone, or automated crawler that sends GET requests to these URLs. Nothing about the URLs, or the content of the

[4] http://www.cancer.net/cancer-types/melanoma/treatment-options (Compl. ¶ 132).
[5] http://www.shawneemission.org/find-adoctor?doctor=Scott-E-Ashcraft-MD-1407822869#.U77dgKhRa-k (Compl. ¶ 161).
[6] http://my.clevelandclinic.org/search/results?q=intestine%20transplant (Compl. ¶ 188).
[7] https://www.mdanderson.org/publications/cancerwise/2012/06/ metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnos.html (Compl. ¶ 202).

pages located at those URLs,[8] relates "to the past, present, or future physical or mental health or condition of an individual." 45 C.F.R. § 160.103 (emphasis added). As such, the stricter authorization requirements of HIPAA (as well as Cal. Civ. Code § 1798.91) do not apply.

Plaintiffs' consent bars their statutory causes of action against Facebook. Plaintiffs' claim under the Wiretap Act fails because "consent of one of the parties to the communication [is] sufficient to preclude liability under the Wiretap Act." Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1045 (N.D. Cal. 2014); see also 18 U.S.C. § 2511(2)(d) (stating that no liability exists where "one of the parties to the communication has given prior consent" to interception). Similarly, Plaintiffs cannot state a claim under the California Invasion of Privacy Act because that statute imposes liability only for interception "without the consent of all parties." Cal. Penal Code §§ 631(a), 632; see also Faulkner v. ADT Sec. Servs., Inc., 706 F.3d 1017, 1019 (9th Cir. 2013) (holding that a communication is confidential under § 632 only when a party "has an objectively reasonable expectation that the conversation is not being overheard or recorded") (quoting Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95, 117 n.7 (2006)).

Plaintiffs' consent also bars their common-law tort claims and their claim for invasion of privacy under the California Constitution. See Cal. Civ. Code § 3515 ("He who consents to an act is not wronged by it."); Kent v. Microsoft Corp., No. SACV13-0091 DOC ANX, 2013 WL 3353875, at *6 (C.D. Cal. July 1, 2013) (granting defendant's motion to dismiss because "plaintiffs generally may not assert a wrong arising out of an action which they consented to"); Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1, 26 (1994) ("[T]he plaintiff in an invasion of privacy case must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant. If voluntary consent is present, a defendant's conduct

[8] Plaintiffs note that Facebook "knows the contents of communications between users and websites" because, every 30 days, it scrapes the contents of pages containing Facebook buttons. Compl. ¶ 86. This allegation only highlights the fact that the Healthcare Defendants' websites do not contain individualized health care information: Facebook's scraper only collects publicly available information on the Healthcare Defendant's websites, regardless of whether Plaintiffs (or others) visited those sites.

will rarely be deemed 'highly offensive to a reasonable person' so as to justify tort liability."); In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1037–38 (N.D. Cal. 2014) (holding that a plaintiff asserting a privacy claim under the California Constitution "must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant," and granting defendant's motion to dismiss).

IV. LEAVE TO AMEND

Courts "should freely give leave [to amend] when justice so requires." Fed. R. Civ. P. 15(a)(2); In re Korean Air Lines Co., Ltd., 642 F.3d 685, 701 (9th Cir. 2011). Absent a showing of prejudice, delay, bad faith, or futility, there is a strong presumption in favor of granting leave to amend. Eminence Capital, LLC v. Aspeon, Inc., 316 F.3d 1048, 1052 (9th Cir. 2003). However, courts can dismiss without leave to amend if "allegation of other facts consistent with the challenged pleading could not possibly cure the deficiency." Swartz v. KPMG LLP, 476 F.3d 756, 761 (9th Cir. 2007) (quoting Albrecht v. Lund, 845 F.2d 193, 195 (9th Cir. 1988)); see also Chappel v. Lab. Corp. of Am., 232 F.3d 719, 725–26 (9th Cir. 2000) ("a district court acts within its discretion to deny leave to amend when amendment would be futile").

In this case, no consistent amendment could support a finding of personal jurisdiction over the Healthcare Defendants. Both the Plaintiffs and the Healthcare Defendants reside in other states. Plaintiffs' theory of personal jurisdiction is that the Healthcare Defendants embedded Facebook tools on their websites, which allowed some of Plaintiffs' browsing data to be sent to Facebook. This activity is insufficient as a matter of law to confer jurisdiction over the Healthcare Defendants in California. No further allegations consistent with the original complaint could change this conclusion.

Likewise, no amendment could change the fact that Plaintiffs consented to Facebook's conduct. Facebook's policies disclose the precise activity at issue in this case. See, e.g., Compl. Ex. A at 2 ("We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement

and advertising services).”); id. Ex. C at 1–2 (disclosing that Facebook uses a variety of techniques to track users on third-party sites, and explaining that the “resulting connection [to Facebook’s servers] can include information such as a device’s IP address, the time a person viewed the [site], an identifier associated with the browser or device and the type of browser being used”). Plaintiffs admit that they understood and agreed to Facebook’s policies. No further allegations could allow Plaintiffs to bring claims “arising out of conduct which they consented to.” Kent, 2013 WL 3353875, at *6.

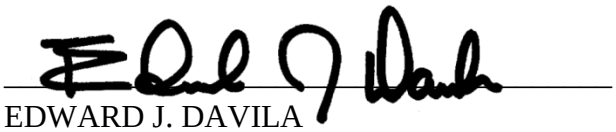
Because amendment would be futile, the Court will dismiss the complaint without leave to amend.

V. CONCLUSION

This Court lacks personal jurisdiction over the Healthcare Defendants because Plaintiffs have not established that the Healthcare Defendants have minimum contacts with California. Plaintiffs’ claims against Facebook fail because Plaintiffs consented to Facebook’s conduct. As such, Defendants’ motion to dismiss is GRANTED. Plaintiffs’ complaint is dismissed without leave to amend. The Clerk shall close this file.

IT IS SO ORDERED.

Dated: May 9, 2017



EDWARD J. DAVILA
United States District Judge