United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE META PIXEL HEALTHCARE LITIGATION	Case No. 22-cv-03580-WHO **ORDER DENYING MOTION FOR PRELIMINARY INJUNCTION** Re: Dkt. No. 46

INTRODUCTION

This case is about defendant Meta Platform, Inc.'s alleged use of proprietary computer code to obtain certain healthcare-related information of Facebook users. According to plaintiffs, the Meta Pixel allows Meta to intercept personally identifiable medical information and the content of patient communications for Facebook users, which Meta then monetizes for its own financial gain. Plaintiffs have brought several federal and state law claims to vindicate the harms that they have allegedly experienced. They ask me to enjoin Meta from intercepting and disseminating their patient information.

Our nation recognizes the importance of privacy in general and health information in particular: the safekeeping of this sensitive information is enshrined under state and federal law. The allegations against Meta are troubling: plaintiffs raise potentially strong claims on the merits and their alleged injury would be irreparable if proven. To secure a mandatory injunction, however, plaintiffs need to show "that the law and facts *clearly favor* [their] position, not simply that [they are] likely to succeed." *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (emphasis in original). Meta's core defense is that it has systems in place to address the receipt of the information at issue and that it would be unfairly burdensome and technologically infeasible for them to take further action. Without further factual development, it is unclear where the truth lies, and plaintiffs do not meet the high standard required for a mandatory injunction. At this early stage of the case, I **DENY** the motion for a preliminary injunction.

FACTUAL BACKGROUND

Plaintiffs are four Facebook users who are proceeding anonymously due to the sensitive nature of this litigation. First Amended Complaint ("FAC") [Dkt. 22] ¶¶ 32–35. They allege that Meta[1] improperly acquires their confidential health information in violation of state and federal law and in contravention of Meta's own policies regarding use and collection of Facebook users' data. *Id.* ¶¶ 1–2, 12. Each of plaintiffs' healthcare providers—MedStar Health System, Rush University System for Health, and UK Healthcare—allegedly installed the Meta Pixel on their patient portals.[2] *See id.* ¶¶ 3–9. Plaintiffs claim that when they logged into their patient portal on their medical provider's website, the Pixel transmitted certain information to Meta. *Id.* ¶¶ 4–9; *see also e.g.*, *id.* ¶¶ 86, 122, 146 (describing types of data transmitted by the Pixel). They contend that this information, which is contemporaneously redirected to Meta, revealed their status as patients and was monetized by Meta for use in targeted advertising. *Id.* ¶¶ 2, 17–18, 71.

The issues raised in plaintiffs' motion for a preliminary injunction involve Meta's alleged receipt of certain health information through the Meta Pixel; the scope and meaning of certain terms in Meta's policies; the strength of plaintiffs' legal claims; and Meta's systems to prevent receipt of this information. I describe the relevant facts below.

A. The Meta Pixel's Technology

The Meta Pixel is a free and publicly available piece of code that Meta allows third-party website developers to install on their websites. *See* Declaration of Tobias Wooldridge

[1] Meta was previously known as Facebook, Inc. In late 2021, the company changed its name to Meta Platforms, Inc. but the social media platform itself is still known as Facebook. Opp. at 3 n.2.

[2] Some of the medical providers, which are not defendants to the lawsuit, may have since removed the Pixel: Meta asserts that as of November 23, 2022, the Pixel is not integrated into the patient portals for either Rush University System for Health or UK HealthCare. *See* Supplemental Declaration of Tobias Wooldridge ("Supp. Wooldridge Decl.") [Dkt. 143-3] ¶¶ 3, 5–6.

("Wooldridge Decl.") [Dkt. 77-4] ¶ 3.[3] The Pixel is customizable: website developers choose which types of user action to measure, and program the Pixel accordingly. *Id.* ¶¶ 3–4. Website developers in a range of industries use the Pixel. *Id.* ¶ 3. In a nutshell, the Meta Pixel allows website developers to learn: (1) if and when website users take certain actions on a website, and (2) generalized information about website users, which can be used for targeting advertising. *Id.* ¶¶ 3–4.

To understand how the Meta Pixel typically works, imagine the following scenario. A shoe company wishes to gather certain information on customers and potential customers who visit its website. The shoe company first agrees to Meta's Business Tools Terms (discussed below), which govern the use of data from the Pixel. Wooldridge Decl. ¶ 6. The shoe company then customizes the Meta Pixel to track, say, every time a site visitor clicks on the "sale" button on its website, which is called an "Event." *Id.* ¶ 4. Every time a user accesses the website and clicks on the "sale" button (*i.e.*, an "Event" occurs), it triggers the Meta Pixel, which then sends certain data to Meta. *Id.* Meta will attempt to match the customer data that it receives to Meta users—Meta cannot match non-Meta users. *Id.* The shoe company may then choose to create "Custom Audiences" (*i.e.*, all of the customers and potential customers who clicked on the "sale" button) who will receive targeted ads on Facebook, Instagram, and publishers within Meta's Audience Network. *Id.* Meta may also provide the shoe company with de-identified, aggregated information so the shoe company understands the impact of its ads by measuring what happens when people see them. *Id.* Meta does not reveal the identity of the matched Meta users to the shoe company. *Id.*

Now, imagine that same process occurring but instead of a shoe company, substitute MedStar Health System, plaintiff John Doe's medical provider. Plaintiffs' expert, Richard Smith, who submitted a lengthy declaration in conjunction with the preliminary injunction motion, asserted that MedStar Health System has the Meta Pixel on various pages of its website, www.MedStarHealth.org. *See* Declaration of Richard M. Smith ("Smith Decl.") [Dkt. 49] ¶ 19;

[3] With apologies to the public, all citations are to the sealed versions of the relevant materials. I address the motions to seal in a separate order issued concurrently.

FAC ¶¶ 3–5; *see also* Supplemental Declaration of Tobias Wooldridge ("Supp. Wooldridge Decl.") [Dkt. 143-3] ¶ 4 (explaining that the Pixel is integrated into the MedStar page that allows users to navigate to the login page). Plaintiffs allege that when John Doe or any other patient of MedStar presses the login button to enter their MedStar patient portal using their username or email address and password, the Meta Pixel source code causes Doe's and all other patients' computing devices to re-direct the contents of their respective patient portal login communications to Meta and then to MedStar, rather than just to MedStar. *See* Smith Decl. ¶¶ 27–28. Meta allegedly redirects the patient portal login information to itself via a "SubscribedButtonClick" transmission that includes, among other things:

- The patient's identity in the form of cookies, IP address, and User-Agent identifiers;
- Content of the button ("Log in");
- Contents of the page from which the patient clicked to log in to the patient portal; and
- Content of the page the patient will land as a result of clicking "Log in" to the patient portal.

Id. ¶¶ 31–33. As a patient browses through the MedStar website, the Meta Pixel allegedly continues to transmit information to Meta, including information about doctors, medical conditions, and appointments associated with a patient's session. Motion for Preliminary Injunction ("Mot.") [Dkt. 46] at 4; Smith Decl. ¶¶ 97, 130–31.[4]

Plaintiffs assert that Meta monetizes the information that it receives through the Meta Pixel by using it to generate highly-profitable targeted advertising on- and off–Facebook. Notice of Motion ("Not. of Mot.") at 1; FAC ¶ 17. They claim that Meta can target ad campaigns to patients based on patients' browsing behavior on their medical providers' website. FAC ¶¶ 18–19; *see*

[4] According to Meta, the Pixel is not integrated into the MedStar login page itself. *See* Supp. Wooldridge Decl. ¶ 4. Meta acknowledges, though, that as of November 2022 the Meta Pixel was integrated into the https://www.medstarhealth.org/mymedstar-patient-portal page, and that website users may click the "log in" button on this page to navigate to the patient portal. *Id.* Meta does not address plaintiffs' contentions that the Pixel transmits information to Meta on other pages of the MedStar website.

also Wooldridge Decl. ¶ 4 (explaining that website developers can target ads on Facebook, Instagram, and other sites based on data transmitted by the Pixel). Meta may, for instance, target ads to a person who has (1) used the patient portal and (2) viewed a page about a specific condition, such as cancer. FAC ¶ 19. These allegations appear to be borne out by plaintiffs' expert's experiences: after Smith visited five hospital websites which employ the Meta Pixel, he allegedly received many new health-related advertisements. Smith Decl. ¶ 187; *see also* ¶ 188 (providing over a dozen examples of health-related advertisements). In particular, Smith noticed that within two hours of searching for information on ulcerative colitis on one of the hospitals' websites, he was shown an advertisement related to ulcerative colitis in his Facebook video feed. *Id.* ¶¶ 189–90.

According to plaintiffs, they have identified more than 660 entities covered under the Health Insurance Portability and Accountability Act ("HIPAA"), from which Meta is receiving information. Mot. at 2; FAC ¶ 15.

B. Meta's Data Policies

Meta has several policies governing how it collects and uses data, including through the Pixel. When individuals sign up for a Facebook account, they agree to Meta's Terms of Service, Data Policy, and Cookies Policy. FAC ¶ 49. These policies are contractually binding on both Meta and its users. *Id.* Because these policies bear on the important question of whether plaintiffs knew and consented to Meta's use of the Meta Pixel to receive health-related information, I describe each policy below.

1. Terms of Service

The Terms of Service govern the "use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software" that Meta offers. *See* Declaration of Abigail Barrera ("Barrera Decl.") Ex. A (Terms of Service) [Dkt. 76-3] at 1. Meta informs users that it "use[s] data about the connections you make, the choices and settings you select, and what you share and do on and off our Products – to personalize your experience." *Id.* at 2. The Terms of Service explain that Meta shows users "personalized ads, offers, and other sponsored or commercial content to help [them] discover content, products, and services that are offered by the many businesses and organizations that use Facebook and other Meta Products." *Id.* To provide these services, Meta's terms explain, Meta "collect[s] and use[s] your personal data." *Id.* at 4. The Terms of Service include several links to the Data Policy. *Id.* at 1, 3, 4.

2. Data Policy

The Data Policy[5] "describes the information" that Meta "process[es] to support Facebook, Instagram, Messenger and other products and features offered by Meta." Barrera Decl., Ex. B (Data Policy) [Dkt. 76-4] at 1. Among other things, the Data Policy tells users that:

> Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. **We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.**
>
> Partners receive your data when you visit or use their services or through third parties they work with. **We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us.**

Id. at 4–5 (emphasis added). The Data Policy also notifies users that Meta uses this information "to personalize features and content (including your ads, Facebook News Feed, Instagram Feed, and Instagram Stories) and make suggestions for you . . . on and off our Products." *Id.* at 5; *see also id.* at 6 ("We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services."). Meta does

[5] At some point, Meta renamed the Data Policy as the Privacy Policy. *See* Opp. at 3 n.3.

not, however, "share information that personally identifies" users with advertisers unless users allow Meta to do so. *Id.* at 9.

3. Cookies Policy

Cookies are "small pieces of text used to store information on web browsers." Barrera Decl., Ex. C (Cookies Policy) [Dkt. 76-5] at 1. They "store and receive identifiers and other information on computers, phones and other devices," and they can serve a number of different functions, such as "personalizing content, tailoring and measuring ads, and providing a safer experience." *Id.* at 1.

Meta's Cookies Policy explains that Meta "use[s] cookies if you have a Facebook account, use the Meta Products, including our website and apps, or visit other websites and apps that use the Meta Products (including the Like button)." *Id.* Meta notes that cookies allow it to "understand the information that we receive about you, including information about your use of other websites and apps, whether or not you are registered or logged in," and that it "use[s] cookies to help us show ads and to make recommendations for businesses and other organisations to people who may be interested in the products, services or causes they promote." *Id.* at 1–2. Cookies allow Meta "to provide insights about the people who use the Meta Products, as well as the people who interact with the ads, websites and apps of our advertisers and the businesses that use the Meta Products." *Id.* at 3. The policy also describes the cookie used to enable the Meta Pixel ("_fbp") and explains that Meta's "business partners may also choose to share information with Meta from cookies set in their own websites' domains, whether or not you have a Facebook account or are logged in." *Id.* at 4; *see also id.* at 4–5 ("Meta uses cookies and receives information when you visit [websites and apps that use the Meta Products], including device information and information about your activity, without any further action from you. This occurs whether or not you have a Facebook account or are logged in.").

4. Business Tools Terms and the Pixel Creation Process

Meta also has policies which govern third-party website developers' use of the Meta Pixel. Before a website developer can integrate the Pixel on a website, the developer must agree to Meta's Business Tools Terms and create a Meta Pixel ID. Wooldridge Decl. ¶ 6.

The Business Tools Terms require developers to "represent and warrant that you (and any data provider that you may use) have all of the necessary rights and permissions and a lawful basis (in compliance with all applicable laws, regulations and industry guidelines) for the disclosure and use of Business Tool Data." Barrera Decl., Ex. D (Business Tools Terms) [Dkt. 76-6] at 1. Developers must also "represent and warrant that [they] have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage," including a "clear and prominent notice on each web page where [Meta] pixels are used that links to a clear explanation [of] . . . how users can opt-out of the collection and use of information for ad targeting []." *Id.* at 3. As a condition of using the Pixel, developers specifically agree that they will "not share Business Tool Data . . . that [they] know or reasonably should know . . . includes **health**, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines)." *Id.* at 2 (emphasis added); *see also* Barrera Decl., Ex. E (Commercial Terms) [Dkt. 76-7] at 2 (similar provision in Commercial Terms).

During the Meta Pixel ID creation process, Meta reminds developers not to send sensitive user data to Meta. Wooldridge Decl. ¶ 7. Meta has published several articles that explain and give examples of the kinds of information (including health information) that developers should not send to Meta, provide steps that developers can take to avoid sending such information, and describe how to address instances in which sensitive information may have been sent. *Id.*

C. User Control and Meta's Filtering Mechanism

Finally, outside of the policies discussed above, there are two technological tools that bear on the matter at hand.

First, Meta gives users the ability to control the use of information about their off-Facebook activity (such as activity on third-party websites) for advertising purposes. Wooldridge Decl. ¶ 11. The Off-Facebook Activity tool allows users to view a summary of information that Meta has received about their activity from third parties through the Business Tools, including the Pixel. *Id.* Users can "disconnect" the off-Facebook activity that has been associated with their account—which prevents the data from being used for personalized advertising—and can turn off storage of any future connections for all third-party websites (or on a website-by-website basis). *Id.* The "Data About Your Activity From Partners" tool also allows users to opt out of receiving personalized advertisements based on their activities on other websites and apps. *Id.* ¶ 12; *see also* Barrera Decl., Exs. F, G, H, I (collecting screenshots and articles regarding these tools). Importantly, Meta does not assert that these tools allow users to prevent their information from being sent to Meta in the first place. *See* Reply at 3 ("[N]owhere in Meta's Opposition does it represent that patients can prevent Facebook from receiving [their data].").

Second, Meta uses a filtering mechanism[6] which attempts to screen out potentially sensitive health data that Meta receives. Wooldridge Decl. ¶ 8. It developed the filter to detect data—including health data—sent through the Pixel that Meta categorizes as potentially sensitive. According to Meta, the filter prevents any such data that it detects from being ingested into its ads ranking and optimization systems. *Id.* When it filters out data, it notifies the developer that Meta detected and blocked data that may not comply with Meta's policies. *Id.* ¶ 9. These notifications provide details about the affected data, including the URL where the events occurred, the location of the potentially violating information, steps that the developer can take to address the issue, and an email address to contact with questions. *Id.*

PROCEDURAL BACKGROUND

This case is one of seven consolidated putative class actions involving the Meta Pixel that are currently before me. Plaintiffs in the present case filed suit in June 2022. Dkt. 1. On July 15, 2022, plaintiffs filed the FAC, which is currently the operative pleading. *See* FAC. They bring eight claims: (1) breach of contract, *id.* ¶¶ 108–23; (2) breach of the implied warranty of good faith and fair dealing; *id.* ¶¶ 124–30; (3) intrusion upon seclusion and constitutional invasion of privacy; *id.* ¶¶ 131–38; (4) violation of the Electronic Communications Privacy Act ("ECPA"); *id.* ¶¶ 139–55; (5) violation of the California Invasion of Privacy Act ("CIPA"); *id.* ¶¶ 156–65; (6) negligent misrepresentation; *id.* ¶¶ 166–73; (7) violation of California's Unfair Competition Law;

[6] The details of this filtering mechanism have been filed under seal. *See, e.g.*, Wooldridge Decl. ¶ 8; Supp. Wooldridge Decl. ¶¶ 13–14, 19–20, 24–25. As discussed in the concurrently filed order granting the sealing requests, I will maintain this information under seal because Meta's sealing requests are justified at this early stage in the litigation.

id. ¶¶ 174–87; and (8) trespass, *id.* ¶¶ 188–99.

On August 25, 2022, plaintiffs filed the instant motion for a preliminary injunction, which rests on plaintiffs' claims under the ECPA, CIPA, and California tort law. *See* Mot. at 1. As part of their motion, they seek an order that: (1) "[p]rohibits Meta from intercepting patient information and communications from HIPAA-covered entities through its use of the Meta Pixel" and (2) "[p]rohibits Meta from disseminating and/or using patient information and communications that it has intercepted from HIPAA-covered entities through its use of the Meta Pixel." Not. of Mot. at 1. In conjunction with the opening motion, they submitted declarations by plaintiff John Doe and their expert Richard Smith, a legal consultant who specializes in the analysis of software systems. Dkts. 47, 49. Plaintiffs also submitted copies of five decisions from state courts that have found that similar claims may lie against medical providers based on their use of the Pixel. *See* Declaration of Jason Barnes ("Barnes Decl.") [Dkt. 48] ¶¶ 5–10.[7]

In opposition, Meta included a declaration by Tobias Wooldridge, a senior software engineer at Meta, which addressed technical aspects of the Pixel and described Meta's filtration system, among other things. *See* Wooldridge Decl. ¶¶ 4, 8–9. With their reply, plaintiffs included a declaration by Christopher Wilson, a computer sciences professor who holds positions at Northeastern University and Harvard University, who opined that Meta could, with slight modifications, use its existing filtering system and other tools to comply with an injunction of the sort that plaintiffs seek. *See* Declaration of Christopher Wilson ("Wilson Decl.") [Dkt. 98] ¶¶ 1, 6–8, 10–20. Meta objected that the Wilson Declaration was new evidence improperly submitted on reply. *See* Meta's Objections [Dkt. 111] at 1. At the hearing, I allowed Meta the opportunity to submit a supplemental declaration that addressed the issues raised in the Wilson Decl. *See* November 14, 2022 Order [Dkt. 133] at 1. Meta then filed the Supp. Wooldridge Decl., and

[7] These claims include: (1) a claim under the Maryland Wiretap Act, (2) a claim under the Massachusetts Wiretap Act; (3) claims under the California Invasion of Privacy Act; (4) intrusion upon seclusion; (5) publication of private facts; and (6) *Biddle* claims. Barnes Decl. ¶¶ 5–10. (*Biddle* claims refer to the Ohio Supreme Court decision, *Biddle v. Warren Gen. Hosp.*, 86 Ohio St. 3d 395 (1999), which established a common law tort under Ohio law for the unauthorized, unprivileged disclosure to a third party of nonpublic medication information that a physician or a hospital learned within a physician-patient relationship. *Id.* ¶ 7 n.1.)

plaintiffs subsequently submitted supplemental authority consisting of new guidance issued by the Office for Civil Rights at the U.S. Department of Health and Human Services on December 1, 2022, regarding the obligations of HIPAA on certain entities when using online tracking technologies, including the Meta Pixel. *See* Supp. Wooldridge Decl.; Plaintiffs' Notice of Supplemental Authority [Dkt. 148] at 2.

After full briefing and argument, my ruling follows.

LEGAL STANDARD

"A preliminary injunction is an extraordinary remedy never awarded as of right." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008) (citation omitted). "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Id.* at 20. In each case, courts "must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief." *Id.* at 24 (quoting *Amoco Prod. Co. v. Vill. of Gambell, AK*, 480 U.S. 531, 542 (1987)).

Mandatory injunctions, which require affirmative action rather than maintaining the status quo, are "particularly disfavored." *Garcia*, 786 F.3d at 740 (quoting *Stanley v. Univ. of S. California*, 13 F.3d 1313, 1320 (9th Cir. 1994)). To succeed, the plaintiff "must establish that the law and facts *clearly favor*" his or her position, not simply that the plaintiff "is likely to succeed." *Id.* (emphasis in original).

DISCUSSION

My decision to deny the pending motion is based on Meta's evidence that it is doing all it can to minimize the problems raised by plaintiffs, and the need for discovery to clarify both the scope of the problems and potential solutions for them. But as the discussion below suggests, it appears that plaintiffs have plausible claims that may well succeed on the merits if that hurdle is overcome, and that the injury alleged is irreparable.

Before I address Meta's substantive challenges to the motion, I will dispense with a procedural issue it raised. Meta objects that the planned consolidated complaint, which will be filed at some point in the future, moots plaintiffs' motion. *See* Opposition ("Opp.") [Dkt. 77-3] at 10–11. It cites authority standing for the unremarkable principle that "[i]t is well-established" in the Ninth Circuit "that an amended complaint supersedes the original, the latter being treated thereafter as non-existent." *Ramirez v. Cnty. of San Bernardino*, 806 F.3d 1002, 1008 (9th Cir. 2015) (internal citation and quotation marks omitted). It also cites my order establishing that the consolidated complaint shall be the operative complaint in the consolidated action. Opp. at 10 (citing October 12, 2022 Order) [Dkt. 73] at 3.

Meta is missing the point. Yes, at some point a consolidated complaint will be filed and at that point, the FAC will no longer be the operative pleading. That has not happened yet. None of Meta's cases support its novel theory that a motion for a preliminary injunction based on a *currently operative* complaint is mooted by a *currently non-existent* consolidated complaint. I note, too, that all of the plaintiffs from the consolidated and soon-to-be consolidated cases agreed that the preliminary injunction briefing and hearing should proceed despite the cases being consolidated. *See* Dkts. 65, 94, 95. I need to address plaintiffs' motion on the merits. Having determined that the motion is not moot, I turn to the four *Winter* factors.

I. LIKELIHOOD OF SUCCESS ON THE MERITS

Because plaintiffs' purported consent is an overarching issue that could preclude relief for all of the claims at issue, I begin with this topic.

A. Plaintiffs Did Not Consent to Meta's Acquisition of Their Health Information.

The key question at the heart of this motion is whether a reasonable user would have understood from Meta's policies that Meta collects the health information at issue here. Plaintiffs contend that the information at issue constitutes "protected health information" within the meaning of HIPAA, and as a result, HIPAA's heightened standard for consent applies. Mot. at 14. I agree that the information at issue here appears to show patient status and thus constitutes protected health information under HIPAA. But I do not reach the question of whether HIPAA's heightened standard for consent applies because, as set forth below, I do not believe that a reasonable user would have understood that Meta may intercept their health information.

1. The Meta Pixel Captures Information Showing Patient Status.

Plaintiffs contend that the Pixel sends information revealing patient status because it intercepts data relating to patient portal logins and logouts alongside identifiers for each patient. Mot. at 6. I agree.

Plaintiffs have put forward evidence that the Pixel transmits "the patient status of individuals logging into the 'patient portals' of their providers through click data, including the Meta Pixel 'SubscribedButtonClick' . . ." Smith Decl. ¶ 4; *see also id.* ¶¶ 31–32, 164 (describing "at least five" protected health information identifiers that are "routinely sent to third-parties in tracking pixels when a MedStar Health patient is communicating with a MedStar Health hospital at a MedStar Health Web site"). Meta concedes that plaintiff John Doe's medical provider MedStar Health, for instance, has integrated the Pixel into the webpage located at https://www.medstarhealth.org/mymedstar-patient-portal. *See* Supp. Wooldridge Decl. ¶ 4. Using the MedStar Health page as an example, this means that when a website user clicks on the "Log in" button on that webpage, the Pixel transmits: (1) the https://www.medstarhealth.org/mymedstar-patient-portal URL; (2) the content of the "Log in" button; (3) the destination URL (*i.e.* the URL of the webpage that the user is directed to after clicking the "Log in" button, which here is the patient portal); and (4) cookies which uniquely identify a Facebook user. *See* Smith Decl. ¶¶ 31–37.

With the MedStar Health page as an example, I conclude that the Pixel transmits information showing patient status. That is, the act of clicking the "Log in" button, when coupled with the MedStar Health patient portal URL and the other information transmitted by the Pixel, sufficiently identifies the website user as a patient. Next, I consider whether patient status constitutes protected health information under HIPAA.

2. Patient Status Is Protected Health Information.

HIPAA defines "protected health information" 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" or the "provision of health care to an individual." 45 C.F.R. § 160.103. At least one court has previously found that information which shows patient-status constitutes protected health information. *See Arvidson v. Buchar*, No. ST-16-cv-410, 2018 WL 10613032, at *10 (V.I. Super. Ct. June 6, 2018) (ruling that patient names and a patient list were PHI which were therefore subject to special disclosure requirements under HIPAA). And the Department of Health and Human Services has issued guidance—including as recently as this past month—instructing that information which connects an individual with a healthcare provider "is indicative that the individual has received or will receive health care services," and thus "relates to the individual's past, present, or future health or health care or payment for care." *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Health & Human Services (content current as of Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html;[8] *see also* 78 Fed. Reg. 5642 (Jan. 25, 2013) (observing that it would be a HIPAA violation for a covered entity to disclose a list of patient names, addresses, and hospital identification numbers because "the protected health information is obviously identifiable").

Meta does not challenge plaintiffs' assertion that patient status is protected information under HIPAA, but instead relies on *Smith v. Facebook*, 262 F. Supp. 3d 943 (N.D. Cal. 2017). But *Smith* does not forestall my conclusion that patient status is protected health information. It dealt with the question of whether Facebook users had consented to Facebook collecting information about them via their browsing through certain health-related websites (such as http://www.cancer.net) that had an embedded Facebook "Like" button. *Smith*, 262 F. Supp. 3d at 948. *Smith* concluded that there was no protected health information because the information transmitted to Facebook when a user visited the http://www.cancer.net page was the same kind of information transmitted to Facebook any time a user visited any page on the internet that contained a Facebook button. *Id.* at 954. In other words, the URLs did not "relate[] specifically to Plaintiffs' health." *Id.* at 954. *Smith* further explained:

> The URLs at issue in this case point to pages containing information about treatment options for melanoma, information about a specific

[8] Plaintiffs submitted the December 2022 guidance as part of their supplemental authority. *See* Dkt. 148-2.

> 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. 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 pages located at those URLs, 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.

Id. at 954–55 (underline in original).

This case is different than *Smith.* Unlike the "general health information that is accessible to the public at large," the URLs and other information transmitted through the Pixel establish that a user is about to log in to a healthcare provider's website. Smith Decl. ¶¶ 31–37. Unlike in *Smith*, then, the Pixel captures information that connects a particular user to a particular healthcare provider—*i.e.*, patient status—which falls within the ambit of information protected under HIPAA. *Smith* involved users browsing through websites providing healthcare information to the public at large, not users navigating to patient portals on healthcare providers' websites. The act of navigating to a patient portal on a healthcare provider's website is not the general internet browsing contemplated in *Smith*. As a result, *Smith* does not bear on the question of whether the information at issue here constitutes patient health information.

3. Meta Has Not Established Consent to the Conduct at Issue.

Meta's policies notify Facebook users that Meta collects and uses their personal data, including data about their browsing behavior on some third-party websites, at least in part for targeted advertising. *See* Terms of Service at 4 (providing that Meta "collect[s] and use[s] your personal data"); Data Policy at 4–5 (explaining that third-parties which are partnered with Meta "provide information about your activities off of our Products"); Cookies Policy at 4 (providing that Meta's "business partners may also choose to share information with Meta"). Meta's policies do not, however, specifically indicate that Meta may acquire *health data* obtained from Facebook users' interactions with their *medical providers' websites*. Its generalized notice is not sufficient to establish consent.

Consent "can be explicit or implied, but any consent must be actual." *In re Google, Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013) (citation omitted). "In order for consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue." *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) (internal quotation omitted); *see also Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 847–48 (N.D. Cal. 2014) (explaining that, for a finding of consent, the disclosures must have given users notice of the "specific practice" at issue). As the Restatement explains, "[i]n order to be effective, the consent must be to the particular conduct of the actor, or to substantially the same conduct." Restatement (Second) of Torts § 892A (1979). In other words, "consent to a fight with fists is not consent to an act of a very different character, such as biting off a finger, stabbing with a knife, or using brass knuckles." *Id.* The test is whether a reasonable user who viewed Meta's disclosures would have understood that Meta was collecting the information at issue. *See Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014). Meta has the burden to show consent. *Calhoun*, 526 F. Supp. 3d at 620.

First, I am skeptical that a reasonable user who viewed Meta's policies would have understood that Meta was collecting protected health information.[9] The nature of the data collection that plaintiffs agreed to is akin to the general internet browsing at issue in *Smith*; the collection of protected health information from a medical provider is a different matter entirely.

Second, *even if* a reasonable Facebook user would have understood that Meta's data collection included health information from their medical provider, that must still be squared with its representation that it "requires" any third-party to have "lawful rights to collect, use and share your data before providing any data to us." Data Policy at 5. For purposes of the likely forthcoming motion to dismiss, I note that Meta's policies "must have only one plausible interpretation for a finding of consent." *Calhoun*, 526 F. Supp. 3d at 620 (citation omitted); *see*

[9] This is especially true because other Meta policies (such as the Business Tool Terms) expressly provide that website developers will not share data that they "know or reasonably should know . . . includes health, financial or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines." Business Tool Terms at 2, *see also* Commercial Terms at 2 (using similar language).

also In re Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019) (internal citation omitted) (hereinafter "*Facebook Consumer Priv. Litig.*") (denying Facebook's motion to dismiss based on plaintiffs' purported consent where there were multiple plausible interpretations of the term "allowed"). In Meta's view, the Data Policy provision is satisfied because any third party that wishes to use the Pixel must "represent and warrant" to Meta that the third party has "all of the necessary rights and permissions and a lawful basis (in compliance with all applicable laws, regulations, and industry guidelines) for the disclosure and use" of the data. Opp. at 19 (citing Business Tool Terms at 1). But "require" is susceptible to multiple meanings. It *could* mean, for instance, that all developers using the Meta Pixel have told Meta that they may lawfully share this information with them. This is, of course, Meta's preferred interpretation. But it could also mean that—in the context of the health information at issue here—Meta required a HIPAA-compliant authorization before receiving such information. In light of the multiple plausible interpretations of "require," it is unlikely that Meta will be able to establish that plaintiffs consented to the data collection at issue here.

In sum, it does not appear to me that consent will bar plaintiffs' claims. I go on to consider the strength of plaintiffs' claims under the Wiretap Act, CIPA, and California law.

B. Wiretap Act Claim

There are two questions that I must answer to determine whether plaintiffs are likely to prevail on their Wiretap Act claim. First, I must examine whether plaintiffs have shown that each of the five elements are met. Second, I must consider whether any of the Wiretap Act's exceptions could exempt Meta from liability. I address each question below.

1. Elements of a Wiretap Act Claim

"The Wiretap Act prohibits the unauthorized 'interception' of an 'electronic communication.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 606–07 (9th Cir. 2020), *cert. denied sub nom. Facebook, Inc. v. Davis*, 141 S. Ct. 1684 (2021) (quoting 18 U.S.C. § 2511(1)(a)–(e)). Plaintiffs must show that Meta (1) intentionally (2) intercepted (3) the contents of (4) plaintiffs' electronic communications (5) using a device. *See In re Pharmatrak, Inc.*, 329

F.3d 9, 18 (1st Cir. 2003) (listing elements for a Wiretap Act claim). Meta challenges only the "contents" element.

a. Meta's "Intentional" "Interception"

"Intercept" is defined under the Wiretap Act as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Although the statute does not define "acquisition," the Ninth Circuit has construed the term according to its ordinary meaning as the "act of acquiring, or coming into possession of [.]" *United States v. Smith*, 155 F.3d 1051, 1055 n.7 (9th Cir. 1998). "Such acquisition occurs when the contents of a wire communication are captured or redirected in any way." *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (internal citation and quotation marks omitted).

According to plaintiffs, the Pixel is "designed for the very purpose of intercepting communications on third-party websites by surreptitiously and contemporaneously redirecting these communications to Meta." Mot. at 11 (citing Smith Decl. ¶¶ 7–14). Plaintiffs have put forward evidence that Meta receives information through the Pixel. *See, e.g.*, Smith Decl. ¶¶ 4–5, 32–33. Meta does not dispute that the intentional or interception elements are met. *See* Opp. at 20–21. Plaintiffs appear likely to succeed on these two elements of their claim.

b. "Contents" of "Electronic Communications" on "Devices"

Of the remaining three elements, only "contents" is in dispute. Meta says that the names of buttons clicked on websites and their associated URLs are not "content" within the meaning of the statute. I disagree. As set forth below, because the "Log in" button and full-string URLs concern the "substantive, purport, or meaning of a communication," these transmissions likely constitute "contents."

The statute broadly defines "content" to include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). "Contents" refers to the "intended message conveyed by the communication"—it does not include record information regarding the characteristics of the message that is generated in the course of the communication. *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). For instance, contact information provided as part of a sign-up process constitutes "content" because this information is the subject of the communication. *Id.* at 1107 ("Because the users had communicated with the website by entering their personal medical information into a form provided by the website, the First Circuit correctly concluded that the defendant was disclosing the contents of a communication."). And while a URL that includes "basic identification and address information" is not "content," a URL disclosing a "search term or similar communication made by the user" "could constitute a communication" under the statute. *Id.* at 1108–09.

In my view, the log-in buttons and the kinds of descriptive URLs identified in the Smith Decl. are "contents" within the meaning of the statute. Unlike in *Zynga*, the URLs at issue here would not merely reveal the name of a Facebook user or group—as Smith explained, the transmitted URLs include both the "path" and the "query string."[10] Smith Decl. ¶¶ 50–51; *see also id.* ¶ 189 (showing hardfordhospital.org/services/digestive-health/conditions-we-treat/colorectal-small-bowel-disorders/ulcerative-colitis URL). These items are content because they concern the substance of a communication. *See Zynga*, 750 F.3d at 1107; *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015) ("If an address, phone number, or URL is . . . part of the substantive information conveyed to the recipient, then by definition it is 'content.'"); *see also In re Google RTB Consumer Priv. Litig.*, No. 21-cv-2155-YGR, 2022 WL 2165489, at *10 (N.D. Cal. June 13, 2022) (finding that categories of the website, categories that describe the current section of the website, and referrer URL that caused navigation to the current page constituted "content").

As noted above, Meta does not challenge plaintiffs' assertion that the Pixel transmits "electronic communications" through the use of "devices." And plaintiffs' internet communications on their healthcare providers' websites appear to fall squarely within the statutory definitions. *See* 18 U.S.C. §§ 2510(5), (12) (defining "device" and "electronic communication").

[10] The "path" identifies where a file or resource can be found on a website. Smith Decl. ¶ 50. Take the https://www.medstarhealth.org/doctors/paul-a-sack-md URL: here, the "path" is doctors/dr-paul-a-sack-md. *Id.* A "query string" provides a list of parameters. An example of a URL which includes a query string is https://www.medstarheatlh.org/sxa/search/results/?q=diabetes. *Id.* The query string parameters in this search indicate that a search was done at the MedStar Health website for information about diabetes. *Id.*

In sum, plaintiffs have made a strong showing as to each of the elements of their Wiretap Act claim. But to ultimately succeed, plaintiffs must also overcome Meta's arguments regarding the applicability of the Wiretap Act exceptions.

2. Wiretap Act's Exceptions

Importantly, the Wiretap Act exempts liability in certain circumstances. The statute provides that:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d). In other words, the Wiretap Act allows interception where the interception is made by a "party" to the communication or where a "party" has consented to the interception. *Id.* This exception does not apply, however, where the interceptor acts "for the purpose of" committing any crime or tort in violation of state or federal law. *Id.*

Putting the question of plaintiffs' consent to the side, the healthcare providers who configured the Pixel on their websites presumably consented to Meta's receipt of the information. Because the Wiretap Act is a one-party consent statute, *see Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021), this means that whether or not plaintiffs consented, Meta is exempt from liability—so long as Meta did not act "for the purpose of" committing any crime or tort. 18 U.S.C. § 2511(2)(d). Plaintiffs' Wiretap Act claim rises and falls with this exception to the exception.

The Ninth Circuit has explained that the crime-tort exception to the Wiretap Act's consent defense focuses on whether "the *purpose* for the interception—its intended use—was criminal or tortious." *Sussman v. Am. Broad. Companies, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999) (emphasis in original) (quotation marks and citation omitted). The existence of a lawful purpose does not sanitize an interception that was also made for an illegitimate purpose. *Id.* Under this exception, plaintiffs must allege that either the "primary motivation or a determining factor in [the defendant's] actions has been to injure plaintiffs tortiously." *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) (quotation omitted).

To ultimately succeed on this claim, plaintiffs must show that the purpose for Meta's interception was to injure plaintiffs tortiously. Meta contends that the crime-tort exception does not apply because its purpose was merely advertising, which is neither a crime nor a tort. Opp. at 20. Multiple courts in this district have found that the crime-tort exception to the Wiretap Act is inapplicable where the defendant's primary motivation was to make money, not to injure plaintiffs tortiously. *See Rodriguez*, 2021 WL 2026726, at *6 n.8 (finding crime-tort exception inapplicable where Google's alleged interceptions occurred with the consent of app developers and were financially motivated); *In re Google Inc. Gmail Litig.*, No. 13-md-02430-LHK, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014) ("[T]he tort or crime exception cannot apply where the interceptor's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.'") (internal citation omitted).

Plaintiffs respond that the use of patient data for advertising in the absence of express written consent is criminal and tortious. Reply at 11; *see also* FAC ¶ 154 (alleging that Meta had a tortious purpose in acquiring the content of patient communications related to patient portals). Plaintiffs cite several state court decisions establishing that tort claims may lie against health care providers over their use of the Pixel. Reply at 11. And as discussed in Part I.D. *infra*, plaintiffs' tort claims against Meta appear viable. There is a not-insignificant chance, then, that plaintiffs may be able to show that the crime-tort exception applies. *Cf. Brown*, 525 F. Supp. 3d at 1067 (finding that the crime-tort exception may apply where plaintiffs had "adequately alleged that Google's association of their data with preexisting user profiles violated state law, including CDAFA, intrusion upon seclusion, and invasion of privacy").

That said, in light of the authority in this district finding that liability does not lie where a defendant's primary motivator was to make money, I am not convinced that plaintiffs have met their burden to show that the law and facts "clearly favor" their position. *Garcia*, 786 F.3d at 740.

Of course, this claim will present differently in a motion to dismiss context. The parties will have the opportunity to refine their arguments regarding Meta's purpose in intercepting the information at issue here later in the litigation.

C. CIPA Claim[11]

The California Invasion of Privacy Act ("CIPA") mirrors the federal Wiretap Act, but with a few important exceptions. "The purpose of the act was to protect the right of privacy by, among other things, requiring that all parties consent to a recording of their conversation." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 769 (2002).

Plaintiffs allege that Meta violated two provisions of CIPA: section 631(a) (the wiretapping provision), and section 632(a) (the recording provision). Mot. at 15–16. The wiretapping provision of CIPA provides:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars.

Cal. Penal Code § 631(a). Put simply, "CIPA is violated when a person reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1050 (N.D. Cal. 2018) (internal quotation marks and citation omitted).

The recording provision of CIPA states that it is unlawful for any person to "intentionally and without the consent of all parties to a confidential communication, use[] [a] recording device

[11] The parties do not dispute that California law applies. *See* Mot. at 15 (explaining why Meta is subject to California law for conduct relating to Facebook's source code); Opp. at 12–13 (analyzing substance of plaintiffs' state law claims).

to . . . record the confidential communication[.]" Cal. Penal Code § 632(a). A "confidential communication" is "any communication carried on in circumstances as may reasonably indicate that any party to the communication desired it to be confined to the parties thereto[.]" Cal. Penal Code § 632(c).

1. Elements of CIPA Claim (Wiretapping Provision)

"The analysis for a violation of CIPA is the same as that under the federal Wiretap Act." *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (quoting *Cline*, 329 F. Supp. 3d at 1051). I have already concluded that plaintiffs will likely establish the elements of a claim under the federal Wiretap Act. *See* Section I.B.1 *supra*. Meta mounts a single challenge to a single element here, arguing that plaintiffs cannot show that the intercepted information is "content" based on its arguments under the federal Wiretap Act. *See* Opp. at 21. For the reasons given above, this challenge fails.

2. Elements of CIPA Claim (Recording Provision)

As noted above, section 632(a) applies only to eavesdropping or recording of a *confidential* communication. *See* Cal. Penal Code § 632(a). Meta argues that the communications at issue here were not confidential because they were transmitted via the Internet. Opp. at 21–22. I disagree.

A communication is confidential under section 632(a) if one of the parties "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan*, 27 Cal. 4th at 777. "And in California, courts have developed a presumption that Internet communications do not reasonably give rise to that expectation." *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (citing and collecting authorities); *see also Rodriguez*, 2021 WL 2026726, at *7 (explaining that plaintiffs "must plead unique, definite circumstances" to rebut California's presumption against online confidentiality). The question is whether plaintiffs have shown that there is something unique about these particular internet communications which justify departing from the presumption. For the reasons expressed below, I conclude that they have done so.

Communications made in the context of a patient–medical provider relationship are readily distinguishable from online communications in general for at least two reasons. First, patient-status and medical-related communications between patients and their medical providers are protected by federal law. *See, e.g.*, 42 U.S.C. § 1320d-6 (providing criminal and civil penalties for disclosing protected health information without authorization); 45 C.F.R. § 164.508 (requiring a "valid authorization" for use or disclosure of protected health information); Section I.A.2 *supra* (finding that patient status is protected health information under HIPAA). Second, unlike communications made while inquiring about items of clothing on a retail website, *Revitch*, 2019 WL 5485330, at *3, health-related communications with a medical provider are almost uniquely personal. "One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up." *Norman-Bloodsaw v. Lawrence Berkeley Lab'y*, 135 F.3d 1260, 1269 (9th Cir. 1998); *see also Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994) ("Extension of the right to confidentiality to personal medical information recognizes there are few matters that are quite so personal as the status of one's health")*; cf. Facebook Consumer Priv. Litig.*, 402 F. Supp. 3d at 783 ("So, for example, if you are diagnosed with a medical condition, you can expect to conceal it completely only if you keep it between you and your doctor. But it does not follow that if you send an email to selected colleagues and friends explaining why you'll be out of commission for a while, you've relinquished any privacy interest in your medical condition, such that the email provider could disseminate your diagnosis to anyone who might be interested in your health status."). For these reasons, it seems to me that plaintiffs will likely be able to show that they had an objectively reasonable expectation that their communications with their medical providers were confidential.

Accordingly, plaintiffs will likely be able to show that the communications at issue here were confidential under the CIPA.

D. Invasion of Privacy and Intrusion upon Seclusion Claims

To prevail on these claims, plaintiffs must show that they had an objectively reasonable expectation of privacy in their medical communications and Meta's conduct was highly offensive. *See Facebook Consumer Priv. Litig.*, 402 F. Supp. 3d at 797 (describing test); *In re Google RTB*

Consumer Priv. Litig., 2022 WL 2165489, at *7 (same).

Courts are generally hesitant to decide claims of this nature at the pleading stage. *See Facebook Consumer Priv. Litig.*, 402 F. Supp. 3d at 797 ("Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is."); *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1054 (N.D. Cal. 2018) (observing that whether conduct rises to the level of highly offensive "is indeed a factual question best left for a jury") (internal quotation marks and citation omitted); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1080 (N.D. Cal. 2016) ("A judge should be cautious before substituting his or her judgment for that of the community."). At this early stage, plaintiffs' claims appear fairly strong. I address each element in turn.

1. Reasonable Expectation of Privacy[12]

I have already found that—in the context of the CIPA claim—plaintiffs will likely be able to show that they had an objectively reasonable expectation that their communications with their medical providers were confidential based on the laws and regulations protecting the confidentiality of medical information. *See* Section I.C.2 *supra*. Case law also supports plaintiffs' position that individuals maintain a reasonable expectation of privacy in detailed URLs. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 605–06 (finding plaintiffs adequately pleaded a reasonable expectation of privacy in "full-string detailed URLs" which contain "the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested").

Meta argues that plaintiffs lacked a reasonable expectation of privacy because its policies convey that it may collect and use their personal data, including data about their browsing behavior on some third-party websites, even while users are not logged into Facebook. But I have already found that the policies at issue did not adequately disclose that Meta collects the kind of sensitive health information at issue in this case, especially in light of the policy provision providing that Meta will "require" partners to obtain "lawful rights" to share user data before Meta will acquire it and Meta's directives to its partners to not send any health information. *See* Data

[12] The reasonable expectation of privacy analysis here is similar to the analysis of whether a communication is "confidential" under CIPA.

Policy at 5; Business Tool Terms at 2. As a result, Meta's policies tend to support, rather than diminish, the likelihood that a user has an objectively reasonable expectation of privacy in this specific information. *Cf. In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 603 (finding an objectively reasonable expectation of privacy existed where plaintiffs plausibly alleged that Facebook did not disclose that the information at issue would be collected).

2. Highly Offensive Intrusion

The next question is whether plaintiffs have shown that Meta's intrusion was "highly offensive." A jury will have to weigh the injury alleged, which is potentially highly offensive, against Meta's defense that it has developed comprehensive systems (discussed in Section III, below) to guard against the intrusion in the most effective manner practicable. Plaintiffs have offered support for the position that Meta's conduct is highly offensive.

In determining the "offensiveness" of an invasion of a privacy interest, courts may consider: "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994) (internal citation and quotation marks omitted). "If voluntary consent is present, a defendant's conduct will rarely be deemed 'highly offensive to a reasonable person' so as to justify tort liability." *Id.* (citation omitted).

There is support for plaintiffs' position that Meta has behaved egregiously. By enacting criminal and civil statutes forbidding the disclosure of protected health information without proper authorization, Congress has made policy decisions regarding the importance of safekeeping this information. *See, e.g.*, 42 U.S.C. § 1320d-6 (providing criminal and civil penalties for disclosing protected health information without authorization); 45 C.F.R. § 164.508 (requiring a "valid authorization" for use or disclosure of protected health information). Courts have also found that taking personal contact information without consent could be deemed highly offensive. *See Opperman v. Path*, 87 F. Supp. 3d 1018, 1060–61 (N.D. Cal. 2014) (finding that a jury must decide whether the "surreptitious theft of personal contact information" is highly offensive). Finally, I note that Meta's policies forbid the transmission of health-related information, which the

Ninth Circuit has found to be relevant in the "highly offensive" inquiry. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 606 (finding that highly offensive element was sufficiently pleaded where Facebook collected full-string detailed URLs and where "Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue."). These arguments have merit.

It is true that "[c]ourts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms." *In re Google, Inc. Privacy Pol'y Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014). But that is not the kind of information at issue here. Meta does not point to a single case where a court found that the collection of the kinds of information at issue here did not constitute a highly offensive invasion of privacy.[13]

A preliminary injunction is an extraordinary remedy that requires the movant to carry the burden of persuasion by a "clear showing." *Mazurek v Armstrong*, 520 U.S. 968, 972 (1997). It is by no means clear at this stage of the case whether plaintiffs will prevail in this litigation. Whether it is likely is a close call, and it will depend on the strength of Meta's defense, which I discuss below in sections III and IV.

II. IRREPARABLE HARM

Plaintiffs contend that they are irreparably harmed by Meta's ongoing interference with their right to confidential medical care and communications.[14] Mot. at 19. I agree that the harm itself is irreparable.

[13] Meta's reliance on *Hammerling v. Google* is misplaced. In *Hammerling*, plaintiffs alleged that Google violated California privacy laws by collecting personal information via various apps. *See* No. 21-cv-09004-CRB, 2022 WL 2812188, at *1 (N.D. Cal. July 18, 2022). But the data at issue in *Hammerling* involved "usage and engagement" data—*i.e.*, the average number of days that users were active on particular apps and a user's total time spent on non-Google apps. *Id.* at *1. *Hammerling* explicitly noted that "the plaintiffs d[id] not allege that Google can read the specific information (i.e., content) that a user inputs." *Id.* at *14. Because the kind of data collected in *Hammerling* is not analogous to the data at issue here, *Hammerling*'s conclusion that the data disclosure was not highly offensive does not bear on the present matter.

[14] Although Meta has implemented measures to prevent its receipt of health information, Meta acknowledged during the hearing that Meta still receives some health information from the Pixel. *See* Preliminary Injunction Hearing Transcript ("PI Hrg. Tr.") [Dkt. 141] at 20:23-21:5.

The legal standard for injunctive relief requires that a plaintiff "demonstrate that irreparable injury is likely in the absence of an injunction." *Winter*, 555 U.S. at 22 (emphasis removed). "Irreparable harm is traditionally defined as harm for which there is no adequate legal remedy, such as an award of damages." *Arizona Dream Act Coal. v. Brewer*, 757 F.3d 1053, 1068 (9th Cir. 2014) (citation omitted). "Because intangible injuries generally lack an adequate legal remedy, 'intangible injuries [may] qualify as irreparable harm.'" *Id.* (quoting *Rent-A-Ctr., Inc. v. Canyon Television & Appliance Rental, Inc.*, 944 F.2d 597, 603 (9th Cir. 1991)).

The invasion of privacy triggered by the Pixel's allegedly ongoing disclosure of plaintiffs' medical information is precisely the kind of intangible injury that cannot be remedied by damages. *See, e.g., Meyer v. Portfolio Recovery Assocs., LLC*, 707 F.3d 1036, 1045 (9th Cir. 2012) (finding that violation of privacy shows irreparable harm); *Brooks v. Thomson Reuters Corp.*, No. 21-cv-01418-EMC, 2021 WL 3621837, at *11 (N.D. Cal. Aug. 16, 2021) (holding that injunctive relief may be available "because the injury here is an invasion of privacy that can never be fully remedied through damages" and loss of privacy is "irreparable"); *Maxcrest Ltd. v. United States*, No. 15-mc-80270-JST, 2016 WL 6599463, at *4 (N.D. Cal. Nov. 7, 2016) ("[A]ny harm to Maxcrest's privacy interests would be irreparable because there is nothing a court can do to withdraw all knowledge or information that IRS agents may have acquired by examination of the requested information once that information has already been divulged.") (cleaned up). Plaintiffs' actions underscore the seriousness of the alleged loss of privacy. For example, plaintiff John Doe has elected to stop accessing his medical provider's online portal, except where medically necessary or where his attorneys have counseled him to do so, in order to prevent his health data from being sent to Meta. Declaration of John Doe ("Doe Decl.") [Dkt. 47] ¶ 7.

Meta does not challenge the severity of the harm that plaintiffs have articulated. Instead, Meta argues that there is no irreparable harm because: (1) plaintiffs purportedly delayed in seeking injunctive relief, and (2) Meta is purportedly not causally connected to the irreparable harm. Opp. at 11. Those arguments are meritless.

A. Plaintiffs Did Not Delay Before Seeking a Preliminary Injunction.

Meta points out that plaintiffs waited more than two months before seeking a preliminary injunction, which—according to Meta—undermines their claim of irreparable harm.[15] Opp. at 11. A "long delay before seeking a preliminary injunction implies a lack of urgency and irreparable harm." *Oakland Trib., Inc. v. Chron. Pub. Co.*, 762 F.2d 1374, 1377 (9th Cir. 1985) (citation omitted); *see also Garcia*, 786 F.3d at 746 (waiting "months to seek an injunction . . . undercut[s] Garcia's claim of irreparable harm"). But "delay is only one factor among the many that we consider in evaluating whether a plaintiff is likely to suffer irreparable harm absent interim relief." *Cuviello v. City of Vallejo*, 944 F.3d 816, 833 (9th Cir. 2019).

The two month period at issue here is readily distinguishable from the situations where courts have found that a delay in seeking an injunction weighs against irreparable harm. In *Oakland Tribune*, for instance, the Ninth Circuit affirmed the denial of a preliminary injunction where "the exclusivity provisions which plaintiff seeks to enjoin have been in effect for a number of years." 762 F.2d at 1377. And in *Garcia*, the plaintiff moved for a preliminary injunction approximately four months after the film (which formed the basis for her copyright claim) was posted on the internet. 786 F.3d at 737–38. In addition to the cases cited by Meta, other Ninth Circuit decisions suggest that waiting two months before seeking an injunction does not lessen a claim of irreparable harm. *See Arc of California v. Douglas*, 757 F.3d 975, 990 (9th Cir. 2014) (challenging a law which "was passed only months before the initiation of this lawsuit" weighed against finding delay); *cf. Cuviello*, 944 F.3d at 822, 834 (finding that plaintiff delayed by seeking preliminary injunction almost two years after learning of restraint on speech but that plaintiff had still shown irreparable harm); *Lydo Enterprises, Inc. v. City of Las Vegas*, 745 F.2d 1211, 1213–14 (9th Cir. 1984) (finding that a five year delay before "taking any action" weighed against finding of irreparable harm).

The issues in this case are factually, technologically, and legally complex. The two month period between the complaint and the motion for a preliminary injunction does not undermine plaintiffs' showing of irreparable injury.

[15] Plaintiffs sought a preliminary injunction within forty-one days of filing the FAC.

B. Plaintiffs Allege Irreparable Harm Causally Connected to Meta's Conduct.

Meta also contends that there is no irreparable harm because "plaintiffs have not shown that their alleged harm is caused by the defendant." Opp. at 12. It claims that it is not responsible because (1) plaintiffs can purportedly avoid injury by disconnecting their off-Facebook activity, and (2) third party website developers, not Meta, are to blame. *Id.* Neither argument defeats plaintiffs' showing of irreparable harm.

Meta says that plaintiffs can "avoid" their injuries by disconnecting their off-Facebook activity from their accounts, which they can do—according to Meta's senior software engineer—for all third-party websites, or on a website-by-website basis. Opp. at 12; *see also* Wooldridge Decl. ¶ 11 (explaining that Meta users can control or disconnect their off-Facebook activity). Its misunderstanding of plaintiffs' claim is laid bare with this statement from its opposition brief: "Meta gives users the ability to control the use of information about their off-Facebook activity (such as activity on third-party websites) *for advertising purposes*." Opp. at 6 (emphasis added).

Plaintiffs do not merely object to receiving targeted advertising based on their health information. The heart of plaintiffs' complaint—and the core injury asserted therein—is that Meta is accessing their health information in violation of state and federal law. During the hearing, Meta conceded that it does not enable Facebook users to prevent Meta from accessing their information. *See* PI Hrg. Tr. at 7:23–8:23. Because Meta does not enable plaintiffs to "opt out" of using the Pixel, Meta's argument and authorities regarding "self-inflicted" harm are irrelevant.

Meta's other argument hinges on the premise that Meta cannot stop website developers from sending it health information. Opp. at 12–13. But Meta conceded that it "has the ability to block *all* data coming in from a specific website or specific Pixel ID," which Meta has done in certain circumstances. *See* Supp. Wooldridge Decl. ¶ 51 (emphasis in original). Putting aside the appropriateness of such a measure, which is discussed in the balance of the equities section below, the fact stands that Meta is capable of turning the Pixel off for certain websites. Plaintiffs have alleged that Meta is causally connected to their injury. That website developers may also be liable does not mean, of course, that Meta is exempt from liability. And Meta's efforts to prevent receipt of health information do not diminish the irreparable invasion of privacy that plaintiffs have experienced.

III. BALANCE OF EQUITIES

The balance of equities factor requires me to weigh the "competing claims of injury" and "consider the effect on each party of the granting or withholding of the requested relief." *Winter*, 555 U.S. at 24 (citation omitted). To succeed in securing an injunction, plaintiffs must show that the balance of equities tips in their favor. *Id.* at 20. For the reasons set forth below, I find that plaintiffs have not done so.

As noted above, plaintiffs describe a weighty injury. Privacy is "a most fundamental human right" that is "older than the Bill of Rights[.]" *See Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 487 (1974); *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965). And while privacy is important, it is also fragile: with a mere click of the mouse, one's personal information may be disseminated to the world. There is no way to undo a loss of privacy.

Without minimizing the gravity of plaintiffs' injury, though, two points merit caution. First, Meta contends that plaintiffs' recommendations for how Meta could modify its existing filtration systems to comply with an injunction are either already implemented or are infeasible in light of Meta's existing systems. *See* Supp. Wooldridge Decl. ¶¶ 16, 23–26, 31, 33–39. The Supp. Wooldridge Decl. describes the resources[16] that Meta has already invested in its filtration systems and contextualizes the technological issues implicated by an injunction of the sort that plaintiffs seek. *Id.* ¶ 46. Wooldridge explained that Meta designed its existing filtering mechanism to detect and filter out potentially sensitive data transmitted via the Pixel in light of the vast quantity of data that floods Meta every day. *Id.* ¶ 8. According to Meta, Meta's existing filtration systems are "the most effective and feasible methods" for Meta to detect and prevent the receipt of potentially sensitive information at scale. *Id.* ¶ 47. At this point, I have no reason not to credit Meta's assertions regarding the design of the filtration systems or the feasibility of Wilson's

[16] There are currently 15 Meta employees (including four dedicated engineers) working on improving the integrity systems used to detect and filter out potentially sensitive health data sent via the Meta Pixel, and 80 employees who are involved in other aspects of Meta's filtration systems. Supp. Wooldridge Decl. ¶¶ 9–10.

recommendations.

Second, at this early stage of litigation, many of the facts are unknown or still developing. It is not clear to me, for instance, how many hospital systems currently use the Pixel on their patient portals.[17] Nor do I know how successfully Meta's filtration systems flag and block the health information at issue in this case. Plaintiffs claim that the filtration systems are "ineffective," *see* Reply at 6 n.4, but without the benefit of discovery, plaintiffs must rely on anecdotal evidence from their expert. *See* Smith Decl. ¶¶ 187–90. And while Wilson described steps that Meta purportedly already has available to comply with an injunction based on the filings from this case so far, Meta's senior software engineer contends that these steps are infeasible in light of how Meta's systems actually function. *See* Supp. Wooldridge Decl. ¶¶ 16, 23–26, 31, 33–39. All this is to say: plaintiffs have described what is potentially a serious problem. But at this point, the precise contours of this problem—the number of HIPAA-entities currently sending patient information to Meta, the amount of data that seeps through the filtration systems, and the feasibility of other technological solutions—remain unknown.

Discovery will eliminate some of these unknowns. Once plaintiffs learn more about Meta's filtration systems and develop an understanding of the kinds of data that are or are not blocked, plaintiffs will be on stronger footing regarding both the feasibility and necessity of technological changes. Should plaintiffs learn that Meta's filtration system is indeed ineffective or that Meta can readily refine its systems to block the patient information at issue here, the balance of equities may at that point tilt in favor of an injunction. In the meantime, I expect Meta to continue to refine its filtration systems to address the issues raised by this case.[18]

The record is not sufficiently developed at this stage to make a judgment regarding the

[17] Plaintiffs allege that they "have identified at least 664 hospital systems or medical provider web properties where Facebook has received patient data via the Facebook Pixel." FAC ¶ 15. But the extent to which these entities *currently* use the Pixel is unclear. Smith observed that after plaintiffs had filed suit, the Pixel was removed "from a number of" hospital websites. Smith Decl. ¶¶ 192–97. And Meta contends that the three hospital systems used by plaintiffs do not currently feature the Pixel on the patient portal webpage. *See* Supp. Wooldridge Decl. ¶¶ 3–6.

[18] Meta is currently working on additional measures with the goal of blocking the kinds of data at issue in this case. Supp. Wooldridge Decl. ¶¶ 28–30.

equities in this case. I suspect it will be clearer after discovery.

IV. PUBLIC INTEREST

The balance of equities focuses on the parties, but "the public interest inquiry primarily addresses impact on non-parties rather than parties," and takes into consideration "the public consequences in employing the extraordinary remedy of injunction." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1202 (9th Cir. 2022) (quoting *Bernhardt v. Los Angeles Cnty.*, 339 F.3d 920, 931–32 (9th Cir. 2003)). For the reasons set forth in the preceding section, I find that the public interest factor does not—at this point—favor an injunction.

To be sure, the public has an interest in privacy in general and health information in particular. But I must also consider the "public consequences" of imposing injunctive relief under these circumstances. *See hiQ Labs.*, 31 F.4th at 1202. Although key information remains unknown, plaintiffs ask me to impose a mandatory injunction against a company that has already gone to some lengths to address these issues. Putting the efficacy of Meta's filtering system to the side, the fact remains that Meta has designed and implemented the systems which it believes are the "most effective and feasible methods" to address the receipt of sensitive information. Supp. Wooldridge Decl. ¶ 47. Against this backdrop, I am not convinced that the public interest would support imposing an injunction against companies in Meta's position.

In light of the systems in place that Meta has created to block receipt of this sensitive information and the factual uncertainties described above, it is too early to find that the public interest supports a mandatory injunction. Of course, my perspective may evolve as the factual record develops in the case.

CONCLUSION

My analysis of the *Winter* factors shows that neither the equities nor the public interest currently supports an injunction. Although plaintiffs have potentially strong arguments on both the merits and irreparable injury, they cannot meet the high standard required for a mandatory

United States District Court
Northern District of California

injunction. Their request for a preliminary injunction is **DENIED.**

IT IS SO ORDERED.

Dated: December 22, 2022

William H. Orrick
United States District Judge