Paul R. Kiesel, State Bar No. 119854
kiesel@kiesel.law
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel: 310-854-4444
Fax: 310-854-0812

Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (admitted *pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (admitted *pro hac vice*)
atruong@simmonsfirm.com
Jennifer Paulson (admitted *pro hac vice*)
jpaulson@simmonsfirm.com
SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: 212-784-6400
Fax: 212-213-5949

Stephen M. Gorny (admitted *pro hac vice*)
steve@gornylawfirm.com
GORNY DANDURAND, LC
4330 Belleview Avenue, Suite 200
Kansas City, MO 64111
Tel.: 816-756-5071
Fax: 816-756-5067

Amy Gunn (admitted *pro hac vice*)
agunn@simonlawpc.com
Elizabeth S. Lenivy (admitted *pro hac vice*)
elenivy@simonlawpc.com
THE SIMON LAW FIRM, P.C.
800 Market St., Ste. 1700
St. Louis, MO 63101
Tel.: 314-241-2929
Fax: 314-241-2029

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE, on behalf of himself and all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 3:22-cv-3580-WHO

CLASS ACTION

PLAINTIFFS' NOTICE OF MOTION AND MOTION FOR PRELIMINARY INJUNCTION

Date: October 5, 2022
Time: 2:00 p.m.
Crtrm.: 2, 17th Floor
Judge: Hon. William H. Orrick

TO THE COURT, ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on October 5, 2022, at 2:00 p.m., or as soon thereafter as the matter may be heard, in the courtroom of the Honorable William H. Orrick of the United States District Court of the Northern District of California, located at 450 Golden Gate Avenue, San Francisco, CA 94102, 17th Floor, Courtroom 2, or via Zoom platform as circumstances require, Plaintiffs John Doe, Jane Doe I, Jane Doe II, and John Doe II, on behalf of themselves and others similarly situated ("Plaintiffs"), will and hereby move the Court for a preliminary injunction.

At the time and place set forth above, Plaintiffs will request that the Court, pursuant to Rule 65 of the Federal Rules of Civil Procedure and Civil Local Rules 65-2 and 7-2, issue an order for a preliminary injunction against Defendant Meta Platforms, Inc., formerly known as Facebook ("Meta"), and all other persons acting in concert with it, requiring it to immediately cease the collection, dissemination, and retention of patient information collected via the Meta Pixel tracking tool employed on hospital webpages. Specifically, Plaintiffs seek an Order:

1. Prohibiting Meta from intercepting patient information and communications from HIPAA-covered entities through its use of the Meta Pixel; and
2. Prohibiting 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.

On a daily basis, Meta intercepts personally identifiable medical information and the content of patient communications which it then monetizes for its own financial gain. Meta's conduct is unlawful and will continue to affect patients of medical providers around the country without this Court's intervention. As demonstrated below, Plaintiffs and the putative class they represent (hereinafter, the "Class") will suffer irreparable harm if Meta is allowed to continue tracking, collecting, and intercepting users' communications. Moreover, the balance of equities strongly favors Plaintiffs and the Class, and the requested injunctive relief serves the public interest because the innocent and unnamed parties in this action – namely, the Class – have been deprived of their right to privacy in their medical information and communications. This Motion is supported by this Notice of Motion, the Memorandum of Points and Authorities in Support thereof, the Declarations of Richard M. Smith, Plaintiff John Doe, and Jason

"Jay" Barnes, filed herewith, all records and papers on file in this action, and such other materials and argument as may be presented before or at the hearing.

DATED: August 25, 2022

SIMMONS HANLY CONROY LLC

By: */s/ Jason 'Jay' Barnes*

Jason 'Jay' Barnes (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Jennifer Paulson (admitted *pro hace vice*)

KIESEL LAW LLP
Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

GORNY DANDURAND, LC
Stephen M. Gorny (admitted *pro hac vice*)

THE SIMON LAW FIRM, P.C.
Amy Gunn (admitted *pro hac vice*)
Elizabeth S. Lenivy (admitted *pro hac vice*)

Attorneys for Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Codes

Other Authorities

Regulations

I. STATEMENT OF ISSUES TO BE DECIDED

Plaintiffs respectfully request that the Court decide the following issues such that an order granting Plaintiffs' Motion for Preliminary Injunction may issue:

1. Whether Plaintiffs are sufficiently likely to succeed on the merits of their claims for violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511 (the "Wiretap Act") (Count IV), violations of the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632 ("CIPA") (Count V), and intrusion upon seclusion and violations of Article I, section 1 of the California Constitution (Count III), to issue a preliminary injunction order;
2. Whether Plaintiffs will likely suffer irreparable harm in the absence of injunctive relief;
3. Whether the balance of equities tips in Plaintiffs' favor; and
4. Whether an injunction is in the public interest.

II. PRELIMINARY STATEMENT

The technology is new and may seem complicated, but the law is old and simple. A third party (like Defendant Meta Platforms, Inc. ("Meta")) may not acquire or use personally identifiable information relating to a patient's status as a patient or communications with their medical provider, without the patient's knowledge and express authorization. Further, a third party may not re-direct the content of electronic communications (to which the third party is not a party) to itself without authorization, regardless of whether patient status or patient communications are the subject of the communication.

Plaintiffs bring this action against Meta for violating both these simple rules. More specifically, Plaintiffs seek redress for Meta's acquisition and use of Plaintiffs' (and the Class's) medical information, particularly the content of their actions and communications relating to their logins and logouts from online patient portals, via the Meta Pixel, without their knowledge or consent.

There is unlikely to be any dispute of material fact regarding the underlying technology that allows Meta to acquire and use the healthcare information described above. Meta designed its Pixel to re-direct the content of user communications with non-Facebook websites, like MedStar Health's ("MedStar") website, to Meta in real-time. Because these patient communications and information are

personally identifiable, particularly in the hands of Meta, Meta then uses it for targeted advertising. Plaintiffs offer evidence of both the acquisition of such information and its use in targeted advertising in the Declaration of Richard M. Smith[1] ("Smith Decl.").

Plaintiffs anticipate that Meta will claim it garnered consent for its actions. But Meta has not. As explained in further detail below, the communications at issue identify the Plaintiffs as patients of their respective medical providers – and Meta is able to connect their status as patients to the content of other communications that Plaintiffs exchanged with their medical providers, giving Meta unauthorized access to users' patient status, doctors, medical appointments, and medical conditions. Further, even if medical information were not at issue, Meta promises users, like Plaintiffs, that it "requires" its partners to have lawful rights to collect, use, and share data before providing any data to Meta. Yet, it permits the Meta Pixel to be deployed and acquire medical information on medical websites, without enforcing its requirement that such medical websites have the lawful right to share such information (by way of a HIPAA-compliant authorization[2]) before providing patient data to Meta.

Because the medical privacy rights of Plaintiffs and millions of other Americans continue to be routinely violated by Meta, Plaintiffs seek Court intervention to prohibit this practice so they may enjoy private communications with their healthcare providers. To that end, Plaintiffs seek an Order that will: (1) prohibit Meta from acquiring patient information and communications from HIPAA-covered entities through the Meta Pixel; and (2) prohibit 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. As alleged in the First Amended Complaint ("FAC"), Plaintiffs have identified more than 660 HIPAA-covered entities from which Meta is receiving information and in discovery have provided Meta with their list of those entities. Plaintiffs are also confident that Meta is able to identify all web properties from which it is currently acquiring such patient information – and to immediately stop the data flow. Plaintiffs further request the Court retain jurisdiction over this matter to ensure that Meta complies with its obligations.

[1] Specific identifying information associated with Mr. Smith have been removed from his declaration.

[2] HIPAA refers to the Health Insurance Portability and Accountability Act of 1996.

III. STATEMENT OF FACTS

A. How the Technology Works

As described by Meta, the "Meta Pixel is a snippet of JavaScript code that … track[s] visitor activity" on non-Meta websites.[3] The Meta Pixel itself is "invisible to the human eye." Smith Decl. ¶ 16. Nevertheless, Meta admits that it uses the invisible pixel to collect: (1) "HTTP headers," including "IP addresses, information about the web browser, page location, document, referrer and person using the website"; (2) "Pixel-specific Data," i.e. a "Pixel ID and the Facebook Cookie"; (3) "Button Click Data," which "[i]ncludes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of button clicks"; and, in some circumstances, (4) optional values and form field names, including emails and addresses. *Id*. at ¶ 9. The "Button Click Data" is called a "SubscribedButtonClick Event," which "fire[s] on every click a user performs" on a web property where the Meta Pixel is present, "sending the button text as a pairameter (buttonText)." *Id*. at ¶ 14.

As used by Meta at Plaintiff John Doe's ("Doe") medical provider, MedStar, at www.MedStarHealth.org, when Doe and any other MedStar patient presses the login button to enter their Medstar patient portal account 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 content of their respective patient portal login communications to Meta rather than just to MedStar. *Id.* at ¶¶ 27-28. Meta re-directs the patient portal login communications to itself via a "SubscribedButtonClick" transmission that includes, among other things: (1) the patient's identity in the form of cookies, IP address, and User-Agent identifiers;[4] (2) content of the button ("Log in"); (3) content of the page from which the patient clicked to Login to the patient portal; and (4) content of the page the patient will land as a result of clicking to Login to the patient portal. *Id.* at ¶¶ 31-33.

[3] https://developers.facebook.com/docs/meta-pixel

[4] Meta cannot dispute this is personally identifiable to Meta. The c_user cookie is a Meta ID. Mark Zuckerberg's c_user cookie value is 4 – because his Meta ID is 4. In addition, Meta maintains a record of every datr cookie ever associated with a Facebook user's account. Thus, a Meta user utilizing Meta's Access Your Information tool can view information about the datr cookies Meta directly associates with the user.

As patients continue to exchange communications with their medical providers, the Meta Pixel re-directs the contents of any other communications to itself. For example, Meta re-directs communications about doctors, conditions, and appointments associated with a patient's session that includes a patient portal login. *Id.* at ¶¶ 97, 130-131 (acquiring communication regarding Dr. Paul Sack).

Meta's actions are by design. In fact, it has designed the Meta Pixel not only to send personally identifiable information and the content of patient communications to itself, but also to do so when a person has attempted to block third-party cookies. *Id.* at ¶¶ 96, 148.

Meta's actions on www.MedStarHealth.org are not an aberration, but just one example of a uniform practice affecting hundreds of medical provider websites from across the United States impacting likely millions of Americans. Meta re-directs patient information on medical provider websites anytime a patient clicks to: (a) register for a supposedly "secure" patient portal; (b) log-in or log-out of their patient portal. *Id.* at ¶¶ 27, 173, 174, 176, 179, 182, 185. The Pixel also redirects to Meta patients' personally identifiable information, including Internet Protocol addresses, browser attribute information sufficient to fingerprint[5] the patient's device, and cookies that Meta can use to identify the patient and his or her device. *Id.* at ¶¶ 31-37. This disclosure, tracking, and use of Plaintiffs' sensitive medical information for marketing is all done without Plaintiffs' knowledge or consent, in violation of their privacy rights, and in violation of Meta's Terms of Use. Indeed, Meta represents to its users that it requires medical providers using the Pixel to have the right to collect and share the data at issue. In reality, Meta does not require any such thing – and receives patient medical information via the Meta Pixel in the absence of patient consent.

B. Allegations Relating to Consent

Meta does not disclose anywhere that it acquires its users' patient portal logins, logouts, or associated communications with their medical providers. To the contrary, Meta promises users that it "require[s] each of [its] partners to have lawful rights to collect, use, and share your data before providing any data to [Meta]." Meta's Data Policy, available at https://www.facebook.com/privacy/policy/version/20220104. This promise is present in the Facebook Data Policy that is one of the

[5] Device fingerprinting is the process of combining information such as IP address, browser information, device information, cookie values, etc. to uniquely identify a user. Smith Decl. ¶ 31.

documents that Meta requires users to state that they have agreed to via a checkbox on the account sign-up page. *Id.* Thus, it is a binding contractual promise from Meta to all of its users.

Plaintiffs anticipate that Meta will argue that its general statements about collection of user information on non-Facebook websites is sufficient to garner consent to the collection of patient portal logins, logouts, and associated communications. However, that argument is contrary to Meta's own express promises set forth above. Equally important, the type of medical information at issue here is not subject to consent via casual notice. Patient-status and medical-related communications between patients and their medical providers are expressly protected by federal law, long-standing common law, and basic rules of human dignity. Thus, even if Meta did not promise that it requires partners to have the lawful rights to collect, use, and share data with Meta, general statements of Meta's activity would not be sufficient notice of the very specific activity at issue here.

IV. LEGAL ARGUMENT

Pursuant to Federal Rule of Civil Procedure 65 and Civil Local Rules 65-2 and 7-2, Plaintiffs seek an order from this Court requiring Meta to stop its unlawful interception, dissemination, and misappropriation of sensitive medical information that it has intercepted through the Meta Pixel. The general basis for injunctive relief is irreparable injury to the moving party and the inadequacy of legal remedies. *See Weinberger v. Romero-Barcelo*, 456 U.S. 305, 312 (1982); *Stanley v. Univ. of So. Calif.*, 13 F.3d 1313, 1320 (9th Cir. 1994). Injunctive relief is appropriate where the plaintiff establishes: (1) it is likely to succeed on the merits of its claims; (2) it will likely suffer irreparable harm in the absence of injunctive relief; (3) the balance of equities tips in its favor; and (4) an injunction is in the public interest. *Winter v. Natural Res. Def. Council*, 555 U.S. 7, 20 (2008). All four of these elements are met here.

A. Plaintiffs Will Likely Succeed on the Merits of their Claims

To show "likelihood of success on the merits," a plaintiff need not show with absolute certainty that he will prevail. *See Drakes Bay Oyster Co. v. Jewell*, 747 F.3d 1073, 1085 (9th Cir. 2014). Rather, a reasonable probability of success, not an overwhelming likelihood, is all the law requires. *See Gilder v. PGA Tour, Inc.*, 936 F.2d 417, 422 (9th Cir. 1991); *see also Leiva-Perez v. Holder*, 640 F.3d 962, 966 (9th Cir. 2011) (likelihood of success does not require showing success is "more likely than not.").

Plaintiffs move for a preliminary injunction under their causes of action for violations of the Wiretap portion of the ECPA and CIPA and for intrusion upon seclusion and violations of Article I, section 1 of the California Constitution. Plaintiffs' allegations and their supporting evidence demonstrate a likelihood of success on the merits of these claims as described below.

1. Plaintiffs Did not Consent to Meta's Acquisition or Use of their Patient Status and Communications

Patient status and associated healthcare communications are protected by federal law. Under HIPAA, a company like Meta may not "obtain[] individually identifiable health information relating to an individual" without express authorization as prescribed by federal law. 42 U.S.C. § 1320d-6. Federal law is also clear that patient-status alone is protected information. *See* FAC ¶¶ 46-47. "If [patient identifiers are] listed with health condition, health care provision or payment data, such *as an indication that the individual was treated at a certain clinic*, then this information would be PHI."[6] HHS Guidance Regarding Methods of De-identification of PHI in Accordance with the HIPAA Privacy Rule. The only exception to this rule is found in 45 C.F.R. § 164.510(1) which provides that patient status may be revealed or acquired through a "directory of individuals" undergoing treatment in a facility when disclosed or acquired by "members of the clergy" or "other persons who ask for the individual by name." Even then, patients must be provided an opportunity to object to third-party acquisition of their status as a patient. 45 C.F.R. § 164.510(2).

Here, by re-directing data relating to patient portal logins and logouts, and associated communications, to Meta alongside identifiers for each patient, the Meta Pixel provides clear indications that Plaintiffs and other patients are, in fact, patients of the medical providers whose websites contain the Meta Pixel.

Plaintiffs anticipate that Meta will cite *Smith v. Facebook*, 745 F. App'x 8 (9th Cir. 2018) ("*Smith*"), an unpublished opinion from the Ninth Circuit, to argue that the information at issue here is not PHI. However, other courts have expressly rejected this argument – because *Smith* involved different factual allegations. *See Doe v. Virginia Mason*, 2020 WL 1983046, at *2 (Wash. Super. Feb. 12, 2020);

[6] Under HIPAA, PHI stands for Protected Health Information.

Declaration of Jason "Jay" Barnes ("Barnes Decl."), Ex. A (*Doe v. Medstar*, Case No. 24-C-20-000591 (Baltimore City, Maryland)); Ex. B (*Doe v. Mercy Health*, Case No. A 2002633 (Hamilton County, Ohio)); Ex. D (*Doe v. Partners*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts)). In *Virginia Mason*, the Court explained that *Smith* was not dispositive, and found (because of factual differences) "that the potential disclosure of a specific patient's logging in to the private portal, possibly coupled with searches of medical providers and conditions immediately prior to the log-in, state a claim to a violation of" the Washington Health Care Information Act, the state-based analog to HIPAA. 2020 WL 1983046, at *2.

Further, there are four key differences between this case and *Smith*. First, *Smith* was not limited to patients and the putative class representatives did not allege that they were patients. Here, Plaintiffs are patients of their respective medical providers and the class is limited to patients of medical providers with websites from which Meta re-directs patient data to itself by way of the Meta Pixel. Second, the "medical" websites at issue in *Smith* were not limited to HIPAA-covered entities. Here, Plaintiffs only seek redress for Meta's actions on medical provider websites relating to patients of those medical providers. Third, in *Smith*, the plaintiffs did not allege transmission of patient portal logins, logouts, appointments, or associated communications. Thus, there was some logic to the Ninth Circuit's ruling that *Smith* had not distinguished the data at issue as *patient*-data. Here, Plaintiffs allege (and demonstrate) a class that is tied to actions that specifically identify them as patients, not just members of the public browsing health-related websites. Fourth, as discussed in more detail below, Meta's current contract and promises to users are different than they were in *Smith*. Meta's express promise that it "require[s]" its "partners to have lawful rights to collect, use and share your data before providing any data" to Meta was not at issue in *Smith* because it was not part of the contract when *Smith* was filed and never considered by any court.

In light of the foregoing, the Court should eventually rule as a matter of law that Plaintiffs did not consent to Meta's acquisition of patient status information in the form of patient portal registrations, logins, logouts, and associated patient communications. Additionally, even in the absence of "personal health information," it is a defendant's "burden to prove consent." *Calhoun v. Google*, 526 F. Supp. 3d 605 (N.D. Cal. 2021) (Koh, J). "Consent 'can be explicit or implied, but any *consent must be actual*."

Id. (emphasis added). To be actual, "the disclosures must 'explicitly notify' users of the practice at issue" and "must have only one plausible interpretation" – that being in favor of the party claiming consent. *Id*. (*citing Facebook Consumer Priv. User Prof. Litig*., 402 F. Supp. 3d 767, 789-94 (N.D. Cal. 2019)). "Moreover, consent is not an all-or-nothing proposition. Rather, a party may consent to the interception of only a part of a communication or to the interception of only a subset of its communications." *Id*. Thus, "a reviewing court must inquire into the dimensions of the [purported] consent and then ascertain whether the interception exceeded those boundaries." *Id*. As explained by the Ninth Circuit, "[t]o be effective, consent must be … to the particular conduct, or substantially the same conduct." *Tsao v. Desert Palace, Inc*., 698 F.3d 1128, 1149 (9th Cir. 2012).

For example, in *Norman-Bloodsaw v. Lawrence Berkeley Lab*., 135 F.3d 1260, 1264-65 (9th Cir. 1998), the court found that, despite plaintiffs expressly consenting to periodic health examinations that included the taking of blood and urine samples and answering specific questions about venereal disease, sickle cell anemia, and menstruation, they had not consented to *testing* those same blood samples about those same topics: STDs, sickle cell, and pregnancy. *Id.* at 1270.

Plaintiffs again anticipate that Meta will point to *Smith* for support. But *Smith* is inapposite for non-PHI consent as well. The reason: the Meta contract is different now than it was in *Smith*. In *Smith*, the Meta contract contained a general disclosure without any countervailing promise that Meta would take action to impose limits on the data that it acquires from "partners" that incorporate Meta Business Tools, such as the Pixel, on their websites. On April 19, 2018, Meta amended its binding consumer contract by expressly promising, "We require each of these partners to have lawful rights to collect, use, and share your data before providing any data to us."

This express promise cannot be ignored. When interpreting a contract, "[t]he whole of a contract is to be taken together, so as to give effect to every part, if reasonably practicable, each clause helping to interpret the other." *Int'l Brotherhood of Teamsters v. NASA Servs., Inc*., 957 F.3d 1038, 1042 (9th Cir. 2020) (citing Cal. Civ. Code § 1641). Here, that means that any provision Meta points to in its defense must be interpreted in light of its promise to require partners to obtain "lawful rights" to "share" user data before doing so. Thus, any general disclosure that Meta collects user information on non-Facebook websites is circumscribed to those situations where Facebook's partner indeed has "lawful

rights" to share. To Plaintiffs' knowledge, the only evidence that Meta makes any effort to enforce its promise is that it includes a provision in its form contract with developers stating that the developer asserts it has permission to send Meta data. https://www.facebook.com/legal/terms/businesstools/update.

But an unenforced provision in a form contract is not enough for Meta to keep its promise that it "requires" partners to have lawful rights to collect, use, and share user data. In a consumer contract of adhesion, any ambiguity is interpreted in favor of the consumer, not the drafter of the document. *Penthouse Int'l Ltd. v. Barnes*, 792 F.2d 943, 948 (9th Cir. 1998) (citing Cal. Civ. Code § 1654; Restatement (Second) of Contracts § 206). The word "require" means more than simply inserting a sentence in Meta's form contract with developers. By stating that it requires such actions, Meta promises that it will, in fact, enforce the promise it makes to its own users. Put simply, a requirement is not a requirement when it is willfully ignored and purposefully not enforced.

Further, the law is clear that courts in the Ninth Circuit are to grant "no refuge" to a defendant who purports to gain consent through mistake that the defendant knew, or, in the exercise of reasonable care, should have known about that relate to the nature and quality of the invasion intended. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2003). Accordingly, even purported express consent is not valid where the defendant knowingly invites a mistake about "the essential character of the act itself," such as "that which makes it harmful or offensive." *Id*. Determining whether something goes to the "essential nature of the invasion" turns "on the extent to which the intrusion" impacts the specific interests that the claim seeks to protect. *Id*. "Even when no restriction is specified, the reasonable interpretation of consent may limit it to acts at a reasonable time and place, or those reasonable in other respects." Restatement (Second) of Torts § 852A(3), cmt. 3. Prosser & Keeton explain: a boxer "consent[s] to the defendant's striking at him" even "if death unexpectedly results" but does not "consent to being hit with brass knuckles, which is the same invasion by an act of a different character." Keeton, supra § 18, at 118. Similarly, "[c]onsent produced by material non-disclosures is no consent at all." *Johnson v. Jones*, 344 P.3d 89, 95 (Ore. Ct. App. 2015); *see also Sanchez-Scott v. Alaza Pharms.*, 86 Cal. App. 4th 365 (2001).

/ / /

Here, the activity in question is not Meta's general tracking on the website of a shoe seller. The communications at issue are between patients and their medical providers and that identify Plaintiffs and other patients – as patients – alongside their appointment requests, doctors, and medical conditions and concerns. In Mark Twain's words, it is like the difference between lightning and a lightning bug. To put this in a real-world context, the Meta Pixel is the digital equivalent of Meta placing cameras inside each patient's medical facility to observe, in real-time, where the patient goes and when they enter their provider's office. So too, if Meta placed a bug inside its users' phones that caused those phones to notify Meta each time that the user called a specific medical provider and then also disclosed that the user had identified themselves as a patient alongside of specific providers, treatments, and appointment information, there would be no question that Meta had violated the patient's privacy rights.

The technology may be slightly different here, but the conduct is the same. In signing up for Meta, neither Plaintiffs nor any other Meta user agreed that Meta could obtain communications with medical providers that identified them as patients in addition to their appointments, providers, and medical interests. To the contrary, Meta assured Plaintiffs and all of its users that it would protect their privacy by requiring any partners to obtain lawful consent before Meta acquired their medical information. As shown by the Smith Declaration, Meta routinely breaks this promise at www.MedStarHealth.org and hundreds of other medical provider websites.

2. Plaintiffs Are Likely to Prevail on their Claim Under the Wiretap Act

"The Wiretap Act prohibits the unauthorized 'interception' of an 'electronic communication.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 606 (9th Cir. 2020) (quoting 18 U.S.C. § 2511(1)(a)-(e)). A claim under the Wiretap Act requires Plaintiffs to establish the following elements: that Meta (1) intentionally (2) intercepted (3) the contents of (4) Plaintiffs' electronic communications (5) by using an electronic, mechanical, or other device. *In re: Pharmatrak*, 329 F.3d 9, 18 (1st Cir. 2003). There are exceptions to liability where a "party" to the communication has consented to the interception or the alleged interception is made by a "party" to the communication. 18 U.S.C. § 2511(2)(d). However, there is also an exception to those exceptions where a "communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d).

/ / /

"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(f). The Ninth Circuit has defined "acquisition" 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). The Meta Pixel is designed for the very purpose of intercepting communications on third-party websites by surreptitiously and contemporaneously redirecting those communications to Meta. *See* Smith Decl. ¶¶ 7-14. There is no question that Meta intentionally acquires Plaintiffs' communications. Meta designed its Pixel to redirect specific communications which are of value and utility to its business model, including the content of buttons the patient clicked, detailed URLs including subcategories, IP addresses, user agent information, and the referrer header.

Also, there is no serious dispute that Meta acquired the "contents" of Plaintiffs' electronic communications, which ECPA defines as "*any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added). Here, Meta acquires the literal content of patient communications with their medical providers, including the names of buttons they click on the website as well as their associated URLs. Specifically, Meta receives an event report, called a "SubscribedButtonClick", every time a patient clicks to enter a patient portal that uses the Meta Pixel:

/ / /

/ / /

/ / /

/ / /

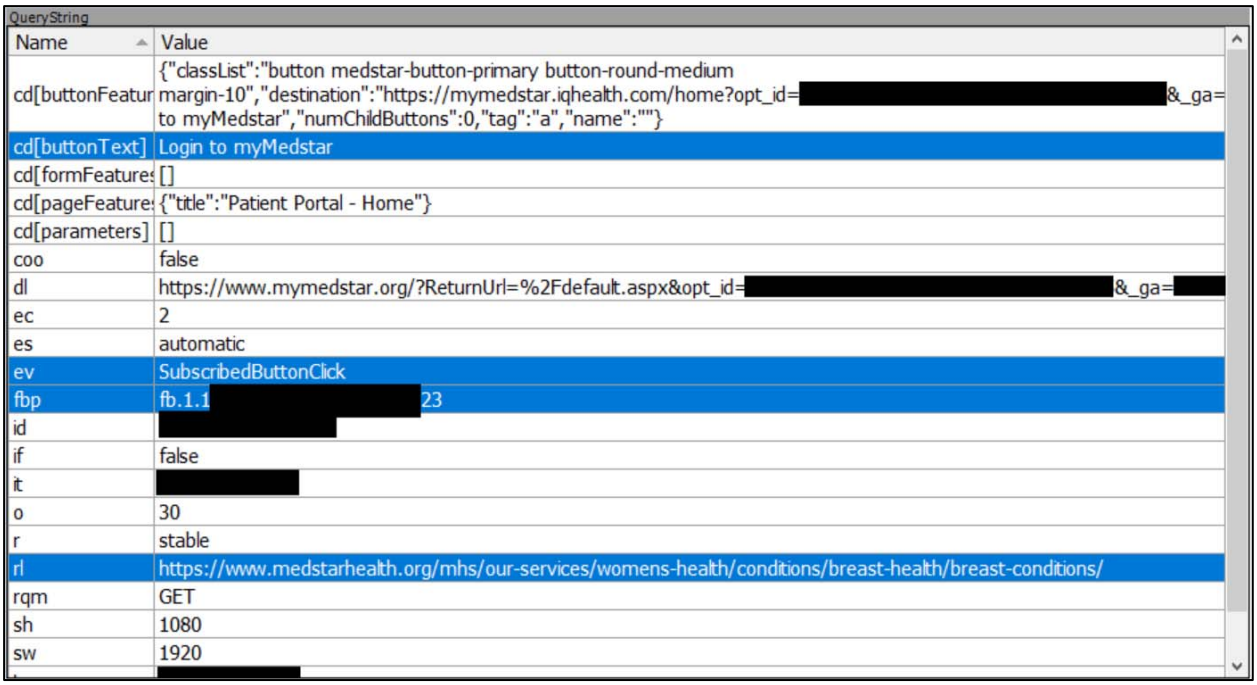
/ / /

/ / /

/ / /

/ / /

/ / /



QueryString

Name	Value
cd[buttonFeatur	{"classList":"button medstar-button-primary button-round-medium margin-10","destination":"https://mymedstar.iqhealth.com/home?opt_id=[redacted]&_ga= to myMedstar","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]	Login to myMedstar
cd[formFeature	[]
cd[pageFeature	{"title":"Patient Portal - Home"}
cd[parameters]	[]
coo	false
dl	https://www.mymedstar.org/?ReturnUrl=%2Fdefault.aspx&opt_id=[redacted]&_ga=[redacted]
ec	2
es	automatic
ev	SubscribedButtonClick
fbp	fb.1.1[redacted]23
id	[redacted]
if	false
it	[redacted]
o	30
r	stable
rl	https://www.medstarhealth.org/mhs/our-services/womens-health/conditions/breast-health/breast-conditions/
rqm	GET
sh	1080
sw	1920

FAC at ¶¶ 5(b), 8(b), 9. These interceptions not only explicitly reveal the content of the patient's communications by disclosing the "buttonText" of the clicked button (namely, "Login to myMedstar") but also reveal the patient's HIPAA-protected patient status by way of the fact that they are a registered portal user.

However, Meta's interceptions of patient communications are not limited to the contents of the webpage they are actively using, they also include additional content regarding the prior page the patient visited. In the above example, Meta's interception includes both the exact content of the "Login to myMedstar" communication transmitted by the patient as well as detailed URL information for the webpage the patient visited immediately preceding logging into the portal, including sub-sub-category information, indicating the patient visited the "breast conditions" sub-subcategory within the "Women's health" sub-category of the website. These invasive interceptions are exactly the type of detailed information courts have routinely found to be "content" under the Wiretap Act. *In re Google RTB Consumer Priv. Litig.*, No. 21-CV-2155-YGR, 2022 WL 2165489, at *10 (N.D. Cal. June 13, 2022); *In re Google Inc. Cookie Placement Consumer Privacy 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.'"); *Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995); *App. of U.S. for Pen Register*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005); *Declassified Opinion at* https://www.dni.gov

/files/documents/1118CLEANEDPRTT%202.pdf; *In re: Pharmatrak*, 329 F.3d at 18; *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 605 ("URLs could divulge a user's personal interests, queries, and habits on third-party website operating outside of Facebook's platform.").

Likewise, Meta cannot dispute that "electronic communications" are at issue here. The ECPA defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interest or foreign commerce" with exceptions that do not apply here. 18 U.S.C. § 2510(12). Plaintiffs' Internet communications on their healthcare providers' websites fall squarely within this broad definition.

Next, Meta's actions occur through the use of several "devices" within the meaning of 18 U.S.C. § 2510(5). These include: cookies; the patients' browsers; the patients' computing devices; Meta's web-servers; the web-servers of the properties of the medical providers where the Meta Pixel was present; and the Meta Pixel source code deployed by Facebook to effectuate its acquisition of patients' communications. Each of these constitute "devices" under the Wiretap Act. *United States v. Szymuszkiewicz,* 622 F.3d 701, 707 (7th Cir. 2010); *In re: Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1067 (N.D. Cal. 2015).

Finally, Meta's interception of the contents of Plaintiffs' communications was without authorization or consent. Meta is not a party to patients' communications with their medical providers and only receives the content of these communication through the surreptitious and secret redirection of them from patients' computing devices to Meta. The Ninth Circuit has explained that the "simultaneous, unknown duplication and communication" of an Internet user's requests to a website "do not exempt a defendant from liability under the party exception." *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607-08 (9th Cir. 2020). Thus, mere secret deployment of the Meta Pixel on a healthcare providers' website does not make Meta a "party" to Plaintiffs' confidential communications with their healthcare providers.

Further, Plaintiffs did not consent to Meta's acquisition of their communications with their medical providers. By the terms of Meta's own contract, it did not obtain "adequate consent" to obtain the content of patient communications with their medical providers. As explained above, this is because

Meta does not enforce its requirement that medical providers have the lawful right to share such information (via a proper HIPAA authorization) before providing it to Meta. The information Meta intercepted is PHI under HIPAA that is prohibited from disclosure to third parties. *See* 45 C.F.R. § 164.514(b)(2)(i) (stating health information is not individually identifiable only if it is scrubbed of a list of identifiers, including geographic subdivisions smaller than a state, IP addresses, device identifiers, serial numbers, and any other unique identifying number, characteristic, or code); *see also* California Civil Code § 1798.91 ("medical information" means "any individually identifiable information," which in turn means "any element of personal identifying information sufficient to allow identification of the individual…that, alone or in combination with other publicly available information, reveals the individual's identity."). Therefore, "adequate consent" in the context of communications with a medical provider regarding medical information can only mean a HIPAA-compliant authorization. Given that Meta did not obtain such authorization from Plaintiffs and the Class, it was precluded from obtaining Pixel interceptions from the medical providers' websites.

But even if Meta had obtained consent from a party to the communication, consent is not a defense where the "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 *Sussman v. ABC*, the Ninth Circuit explained this exception to the exceptions focuses "upon whether the purpose for the interception—its intended use—was criminal or tortious….Where the taping is legal, but is done for the purpose of facilitating some further impropriety…section 2511 applies." 186 F.3d 1200, 1202 (9th Cir. 1999).

Here, Meta acquires Plaintiffs' private medical information with the intent to commit a knowing intrusion upon seclusion; violation of 42 U.S.C. § 1320d-6; violation of state unfair business practices statutes; violation of HIPAA; violation of Article I, section 1 of the California Constitution; and trespassing upon Plaintiffs' personal and private property via the placement of cookies associated with the domains and patient portals for Plaintiffs' medical providers on Plaintiffs' personal computing devices within their homes and businesses. Thus, even where a medical provider may have consented to such conduct, that consent is not sufficient under (2)(d).

/ / /

To Plaintiffs' knowledge, every court to have ever considered the specific question at issue in this action has agreed with Plaintiffs that deployment of the Meta Pixel on a medical provider website associated with a patient portal sets forth a viable claim against the medical provider for violation of state criminal laws. *See Doe v. Virginia Mason*, 2020 WL 1983046, at *2 (Wash. Super. Feb. 12, 2020) (actionable for Identity Theft; Intrusion Upon Seclusion, and others); Barnes Decl. ¶ 9, Ex. D (*Doe v. Partners*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts) (actionable for violation of state Wiretap Act, Intrusion Upon Seclusion, and other claims)); ¶ 6, Ex. A (*Doe v. Medstar*, Case No. 24-C-20-000591 (Baltimore City, Maryland) (actionable for violation of state Wiretap Act, Intrusion Upon Seclusion, and other claims)); ¶ 8, Ex. C (*Doe v. University Hospitals*, Case No. CV-20-9333357 (Cuyahoga County, Ohio) (actionable for state-based tort involving disclosure or acquisition of medical information)); ¶ 7, Ex. B (*Doe v. Mercy Health*, Case No. A 2002633 (Hamilton County, Ohio)); ¶ 10, Ex. E (*Doe v. Sutter Health*, Case No. 34-2019-00258072-CU-BT-GDS (Sacramento County, California) (Mot. J. Pleadings Order, June 9, 2022) (actionable under CIPA)).[7] Meta has had knowledge of these actions for years – and yet, it has continued to deploy the Meta Pixel on medical provider websites to intercept information related to patient-status and healthcare communications without making any attempt to actually require that medical providers obtain lawful consent for their own or Meta's actions.

3. Plaintiffs Are Likely to Prevail on their Claim Under CIPA

Meta is headquartered in California, directs its Internet tracking activities from California, receives tracked Internet communications in California, and utilizes a binding Terms of Use adopting California law to govern all disputes with Meta members. FAC ¶ 31. Upon information and belief, it also required the web-developers for all of the healthcare providers that deploy the Meta Pixel to agree to its Terms of Use adopting California law to govern disputes with developers and websites utilizing Meta code. As such, Meta is subject to California law for conduct relating to Facebook's source code.

The California Invasion of Privacy Act ("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

[7] Counsel for the Doe Plaintiffs here represent the putative Plaintiff classes in each of the cited cases.

> 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).

CIPA further provides that it is unlawful for any person to "intentionally and without the consent of all parties to a confidential communication, use[] [a] recording device to … record the confidential communication." Cal. Penal Code § 632. "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[.]" *Id.*

CIPA mirrors the federal Wiretap Act with a few important exceptions. First, California is an all-party consent state, which requires Meta to obtain the consent of all parties to a communication before it "in any unauthorized manner, read, attempt[] to read, or to learn the contents or meaning of any message, report, or communication[.]" Cal. Penal Code § 631(a). In this case, Meta did not, as explained above, have the consent—let alone a HIPAA-compliant authorization—to acquire patient communications with their healthcare providers. Second, CIPA explicitly does not require the defendant to use a device. Instead, it prohibits activity "by means of any machine, instrument, or contrivance, or in any other manner[.]" Cal. Penal Code § 631(a). Third, CIPA creates liability for a defendant deemed a "party to a confidential communication" who records the communication by means of "any electronic amplifying or recording device." Cal. Penal Code § 632. Given Meta's status as an undisclosed interceptor of patient communications, it was not a "party" to the communications between Plaintiffs and their healthcare providers. However, even if Meta is considered a "party," Meta is still subject to section 632 because Plaintiffs had an objectively reasonable expectation of privacy in their conversations with their healthcare providers given the sensitive nature of the communications, Meta's promises that it "required" adequate consent before obtaining such communications, and California's recognition of a reasonable expectation of privacy in "personal information." Therefore, for all the reasons that support Plaintiffs' claim under the Wiretap Act, Plaintiffs also have a reasonable probability of success on the merits of their cause of action under CIPA. Indeed, a California state court has already

agreed that Plaintiffs could proceed with their CIPA claim against their medical provider due to it making such disclosures to Meta and others. *See* Barnes Decl. ¶ 10, Ex. E (*Doe v. Sutter Health*, Case No. 34-2019-00258072-CU-BT-GDS (Sacramento County, California) (Mot. J. Pleadings Order, June 9, 2022)).

4. Plaintiffs Are Likely to Prevail on Their Invasion of Privacy and Intrusion Upon Seclusion Claims

Invasion of privacy and intrusion upon seclusion claims are often considered in tandem given the similarity in tests.

> To state a claim for invasion of privacy under the California Constitution, a plaintiff must plead: (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is highly offensive. A claim for intrusion upon seclusion under California common law involves similar elements. Plaintiffs must show that: (1) a defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy, and (2) that the intrusion was highly offensive to a reasonable person. Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exist a reasonable expectation of privacy, and (2) the intrusion was highly offensive.

In re Google RTB Consumer Priv. Litig., No. 21-CV-2155-YGR, 2022 WL 2165489, at *7 (internal citations omitted). Here, Plaintiffs' objectively reasonable expectation of privacy is founded both in Meta's own Data Policy and the protections afforded to Plaintiffs' relationships and communications with their healthcare providers. Meta's Data Policy specifically promises that Meta will "require" partners to obtain "lawful rights" to share user data before Meta will acquire it. This promise creates a legally enforceable expectation for Meta users that their personal information and communications will not be intercepted absent such consent. In the context of Pixel deployment on a covered entity's website, HIPAA requires such covered entities to "obtain an authorization for any use or disclosure of protected health information for marketing" and "for any disclosure of protected health information which is a sale of protected health information." 45 C.F.R. § 164.508. Thus, the "critical fact" in this case is that Meta promised not to intercept the Class's personal information and communications with their healthcare providers absent authorization or "lawful rights" to do so, and then proceeded to do so anyway. *In re Google RTB Consumer Priv. Litig.*, No. 21-CV-2155-YGR, 2022 WL 2165489, at *8 (N.D. Cal. June 13, 2022) ("The 'critical fact [that] [Google] represented to the plaintiffs that their

information would not be [sold] but then proceeded to [sell] it anyways' undermines Google's argument that plaintiffs lack a reasonable expectation of privacy.").

Moreover, the type of information at issue—sensitive health communications, patient status, and patient portal use information, as well as detailed URL information, IP addresses, and user agent information—is personal information under California law and parties generally maintain a reasonable expectation of privacy in their personal information. *Id*. (citing Cal. Civ. Code § 1798.140); *see also In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d at 605 (finding plaintiffs adequately pleaded a reasonable expectation of privacy in "full-string detailed URL[s], which contains the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested," "full referral URL (including the exact subpage of the precise items being purchased)," in addition to IP address and user agent information).

Whether conduct is "highly offensive" is generally a mixed question of law and fact. *Hill v. NCAA*, 7 Cal. 4th 1, 40 (1994). By enacting criminal and civil statutes forbidding the practices at issue, Congress and every state have made policy decisions that this type of conduct is highly offensive to a reasonable person. *See* Wiretap Act, CIPA, HIPAA, Cal. Civ. Code § 1798.91. Meta's conduct in taking information without Plaintiffs' knowledge or authorization is highly offensive to a reasonable person. *See Opperman v. Path*, 87 F. Supp. 3d 1018, 1061 (N.D. Cal. 2014) (ruling that the "surreptitious theft of personal contact information" could be deemed highly offensive). Indeed, courts have agreed with Plaintiffs that the activity in question here is an actionable intrusion upon seclusion. *See Doe v. Virginia Mason*, 2020 WL 1983046, at *2 (Wash. Super. Feb. 12, 2020); Barnes Decl., Ex. A (*Doe v. Medstar*, Case No. 24-C-20-000591 (Baltimore City, Maryland)); Barnes Decl., Ex. C (*Doe v. University Hospitals*, Case No. CV-20-9333357 (Cuyahoga County, Ohio) (privacy torts merged for medical privacy)); Barnes Decl., Ex. B, (*Doe v. Mercy Health*, Case No. A 2002633 (Hamilton County, Ohio) (same)); Barnes Decl., Ex. D (*Doe v. Partners*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts)). Therefore, Plaintiffs have a reasonable probability of success on the merits of their invasion of privacy and intrusion upon seclusion claims.

/ / /

/ / /

B. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief

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 8. To show "irreparable harm," a plaintiff must demonstrate that the potential harm is imminent. *See Caribbean Marine Servs. Co. v. Baldridge*, 844 F.2d 668, 674 (9th Cir. 1988) ("a plaintiff must *demonstrate* immediate threatened injury as a prerequisite to preliminary injunctive relief").

To constitute irreparable harm, an injury must generally be certain, actual, and not merely theoretical. *Summers v. Earth Island Inst.*, 555 U.S. 488, 493 (2009) (*citing Friends of Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000)). Here, the irreparable harm Meta has caused and will continue to cause is the interference with the patient Class's right to confidential medical care and communications. These concerns are not mere platitudes. As set forth in the Declaration of John Doe ("Doe Decl."), Meta's ongoing practice of receiving unauthorized interceptions of patient communications has placed patients in the impossible post-COVID era position of being forced to choose between forgoing electronic access to their medical providers in order to avoid Meta's interceptions, or continuing to access medical care remotely only to have it shared with Meta in real-time. Doe Decl. ¶¶ 7-8. This practice will only continue to grow as more and more medical providers expand their remote e-health services and internet advertising portfolios.

Furthermore, monetary damages are not sufficient to remedy the invasions of privacy at issue in this case. While it is true that the patient Class can ultimately economically measure their damages, it is also true that the underlying privacy violation cannot be remedied by money damages. This is not a trade secret or copyright infringement case where the party seeking to enforce their singular right over the information at issue does so in order to protect its inherent economic value. No medical patient seeks to maintain their medical privacy for the purposes of preserving its financial value. Rather, they zealously guard the secrecy of such information for the purposes of the secrecy itself. Once that right to privacy has been violated, it can be compensated but never remedied. For this reason, the Ninth Circuit has recognized that it is exactly these kinds of "intangible injuries" that may qualify as irreparable harm. *Arizona Dream Act Coal. v. Brewer*, 757 F.3d 1053, 1068 (9th Cir. 2014) ("No award of damages can compensate Plaintiffs' for the myriad personal and professional harms caused by their inability to obtain

driver's licenses."); *Enyart v. Nat'l Conference of Bar Examiners, Inc.*, No. C 09-5191 CRB, 2010 WL 475361, at *7 (N.D. Cal. Feb. 4, 2010), *aff'd*, 630 F.3d 1153 (9th Cir. 2011) (finding risk of "a serious career setback" for plaintiff and resulting psychological impact sufficient to establish irreparable harm); *Doe 1 v. U.S. Dep't of Homeland Sec.*, No. 220CV09654VAPAGRX, 2020 WL 6826200, at *8 (C.D. Cal. Nov. 20, 2020), *aff'd sub nom. Does 1 through 16 v. U.S. Dep't of Homeland Sec.*, 843 F. App'x 849 (9th Cir. 2021) (holding "each of these Plaintiffs is, or will imminently be, harmed by the inability to train and practice with their teams—a critical activity in furthering their athletic careers.").

Because Plaintiffs and the members of the Class have suffered and continue to suffer imminent and irreparable harm by Meta's actions, injunctive relief is appropriate.

C. The Balance of Equities Tips Sharply in Plaintiffs' Favor

A plaintiff seeking injunctive relief must establish that the balance of equities tips in its favor. *See Winter*, 555 U.S. at 20. "A court balancing the equities will look to the possible harm that could befall the various parties." *Maxim Integrated Prods. Inc. v. Quintana*, 654 F. Supp. 2d 1024, 1036 (N.D. Cal. 2009).

An injunction preventing Meta from intercepting and utilizing patient communications on covered entities' websites merely requires compliance with HIPAA, the Wiretap Act, CIPA, Article I, section 1 of the California Constitution, and other state laws. *See, e.g.*, *Pyro Spectaculars North, Inc. v. Sousa*, No. S-12-0299, 2012 WL 968084, *11 (E.D. Cal. Mar. 21, 2012) (holding injunction would not cause significant hardship to defendant because "it would essentially only require him to abide by existing law."). It is hornbook law that the public interest and the balance of the equities favor "prevent[ing] the violation of a party's constitutional rights" such as the privacy rights protected by the California Constitution. *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012).

On the other hand, if Meta continues to unlawfully acquire and utilize Plaintiffs' personal and medical information and communications without consent, Plaintiffs and the Class will continue to face serious and substantial irreparable harm. Each day that goes by, more and more individuals unknowingly fall victim to Meta's scheme, and the Class is thereby enlarged. *See Indep. Living Ctr. of S. Cal., Inc. v. Shewry*, 543 F.3d 1047, 1049 (9th Cir. 2008) ("When the balance of harm 'tips decidedly toward the plaintiff,' injunctive relief may be granted . . . .") (quoting *Benda v. Grand Lodge of the Int'l Ass'n of*

Machinists & Aerospace Workers, 584 F.2d 308, 315 (9th Cir. 1978)).

Therefore, because the balance of equities tips sharply in Plaintiffs' favor, injunctive relief is appropriate.

D. The Injunctive Relief Sought Is in the Public Interest

The public interest weighs heavily towards granting Plaintiffs the relief they seek. Widespread recognition of privacy as a fundamental right precedes this nation's founding. *See Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) ("We deal with a right of privacy older than the Bill of Rights"); *Berger v. New York*, 388 U.S. 41, 45 (1967) (citing 4 Blackstone, Commentaries 168 (1765), describing "eaves-droppers" as "a common nuisance . . . preventable at the court, or . . . indictable at the sessions."). The value of this right to individuals is paramount. *See Kewanee Oil v. Bicron*, 416 U.S. 470, 487 (1974) ("A most fundamental human right, that of privacy, is threatened when industrial espionage is condoned or is made profitable; the state interest in denying profit to such illegal ventures is unchallengeable.").

As the Ninth Circuit has pointed out, "One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health[.]" *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d at 1269. In *Riley v. California*, a unanimous Supreme Court held that Americans have a reasonable expectation of privacy in the type of data at issue in this case. 134 S.Ct. 2473, 2490 (2014) ("[C]ertain types of data are also qualitatively different. An Internet search and browsing history … could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

American courts have long protected this right to privacy. The late Prof. Edward Bloustein explained why:

> The fundamental fact is that our Western culture defines individuality as including the right to be free from certain types of intrusions. This measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity, is part of what our culture means by those concepts. A man whose home may be entered at the will of another, whose conversation may be overheard at the will of another, whose marital and family intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account. He who may intrude upon another at will is the master of the other and, in fact, intrusion is a primary weapon of the tyrant.

Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 973-74 (1964). With its unquenchable thirst for data and unrelenting assault on the legal

underpinnings of privacy rights that protect Americans against intrusions from both private and governmental actors, Meta is creating a turn-key solution for totalitarianism. If Meta is deemed immune from this conduct, then so too would governmental actors be immune from the same or similar conduct.

As discussed above, the public's overarching interest in privacy, particularly as to matters concerning healthcare data, and even more specifically patient-healthcare provider communications, patient status, and patient portal use information, is evidenced by the statutory protections that exist for such sensitive information, including HIPAA, the Wiretap Act, and CIPA. Unless this Court issues an injunction, Meta will continue to ignore its duties under the Wiretap Act, CIPA, the California Constitution, and other state laws restricting disclosure of confidential information. Therefore, because the injunction sought is in the public interest, injunctive relief is appropriate.

V. CONCLUSION

Meta's scheme to disclose, divulge, track, and intercept the Plaintiffs' personal information combined with medical information and communications, without Plaintiffs' knowledge or consent, subjects Plaintiffs and the Class to irreparable harm in violation of the public interest. This Court should end Meta's refusal to comply with its obligations under the Wiretap Act, CIPA, the California Constitution, and other state laws restricting disclosure of confidential information, as well as Meta's own representations to users. The Court should enjoin the practices complained of and retain jurisdiction over this matter to confirm that Meta complies with its obligations under all applicable laws.

DATED: August 25, 2022

SIMMONS HANLY CONROY LLC

By: */s/ Jason 'Jay' Barnes*
Jason 'Jay' Barnes (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Jennifer Paulson (admitted *pro hace vice*)

KIESEL LAW LLP
Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

GORNY DANDURAND, LC
Stephen M. Gorny (admitted *pro hac vice*)

THE SIMON LAW FIRM, P.C.
Amy Gunn (admitted *pro hac vice*)
Elizabeth S. Lenivy (admitted *pro hac vice*)

Attorneys for Plaintiffs

CIVIL L.R. 5-1(h)(3) ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I, Jeffrey A. Koncius, hereby attest under penalty of perjury that concurrence in the filing of this document has been obtained from all signatories.

Dated: August 25, 2022

/s/ Jeffrey A. Koncius
Jeffrey A. Koncius

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE, on behalf of himself and all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 3:22-cv-3580-WHO

CLASS ACTION

[PROPOSED] ORDER GRANTING PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Date: October 5, 2022
Time: 2:00 p.m.
Crtrm.: 2, 17th Floor
Judge: Hon. William H. Orrick

This matter is before the Court on Plaintiffs' Motion for Preliminary Injunction. After full consideration of the briefs and arguments of counsel, the evidence filed in support of and opposition to this Motion, and all other matters presented, the Court finds that Plaintiffs have demonstrated a likelihood of success on the merits, the possibility of irreparable harm should an injunction not issue, the balance of equities tips in their favor, and an injunction is in the public interest.

Accordingly, Plaintiffs are entitled to injunctive relief pursuant to Federal Rule of Civil Procedure 65 and the Court grants Plaintiffs' Motion as follows:

1. The Court enjoins Defendant Meta Platforms, Inc. ("Meta") from intercepting patient information and communications from HIPAA-covered entities through its use of the Meta Pixel.

2. The Court enjoins 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.

3. The injunctions shall take effect immediately and shall remain in effect pending resolution of the merits of this case or further order of this Court.

IT IS SO ORDERED.

HON. WILLIAM H. ORRICK
UNITED STATES DISTRICT JUDGE