GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (admitted *pro hac vice*)
lgoldman@gibsondunn.com
DARCY C. HARRIS (admitted *pro hac vice*)
dharris@gibsondunn.com
200 Park Avenue
New York, NY 10166
Telephone: (212) 351-4000
Facsimile: (212) 351-4035

ELIZABETH K. MCCLOSKEY, SBN 268184
emccloskey@gibsondunn.com
ABIGAIL A. BARRERA, SBN 301746
abarrera@gibsondunn.com
555 Mission Street, Suite 3000
San Francisco, CA 94105
Telephone: (415) 393-8200
Facsimile: (415) 393-8306

ANDREW M. KASABIAN, SBN 313210
akasabian@gibsondunn.com
3161 Michelson Drive
Irvine, CA 92612 USA
Telephone: (949) 451-3800
Facsimile: (949) 451-4220

COOLEY LLP
MICHAEL G. RHODES, SBN 116127
rhodesmg@cooley.com
KYLE C. WONG, SBN 224021
kwong@cooley.com
CAROLINE A. LEBEL, SBN 340067
clebel@cooley.com
3 Embarcadero Center, 20th Floor
San Francisco, CA 94111-4004
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Defendant Meta Platforms, Inc. (formerly known as Facebook, Inc.)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE META PIXEL HEALTHCARE LITIGATION

This Document Relates To:

All Actions

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

DEFENDANT META PLATFORMS, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT

CLASS ACTION

Date: August 16, 2023
Time: 2:00 p.m.
Courtroom 2

HON. WILLIAM H. ORRICK

NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE that on August 16, 2023, at 2:00 p.m., before the Honorable William Orrick of the United States District Court for the Northern District of California, Courtroom 2, 450 Golden Gate Avenue, San Francisco, CA 94102, Defendant Meta Platforms, Inc., will, and hereby does, move this Court pursuant to Federal Rule of Civil Procedure 12(b)(6) for an order dismissing the complaint with prejudice.

The motion is based upon this notice of motion; the memorandum of points and authorities in support thereof that follows; the proposed order filed concurrently herewith; the request for judicial notice and accompanying declaration; the pleadings, records, and papers on file in this action; oral argument of counsel; and any other matters properly before the Court.

STATEMENT OF ISSUES TO BE DECIDED

Should the complaint be dismissed under Rule 12(b)(6) for failure to state a claim?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

TREATISES

REGULATIONS

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Plaintiffs' rhetoric aside, this case concerns a relatively narrow issue: the allegation that healthcare providers decided to use a commonplace internet analytics tool to send sensitive health-related information to Meta that Meta never intended, and did not want, to receive. Meta acknowledges that the Court referred to this as a "potentially serious problem" in its order denying plaintiffs' motion for a preliminary injunction, and Meta does not disagree; that is why it has built, and is constantly working to improve, the filtration systems that are designed to screen out potentially sensitive data when it is sent by web developers in violation of Meta's policies.

Two undisputed points put plaintiffs' claims in context.

First, there is nothing inherently unlawful or harmful about the pixel-based analytics technology at the heart of this case. This technology helps web developers measure certain actions users take on their websites—*e.g.*, what pages they view and what products they purchase—and use that information to grow their businesses and improve online user experiences. That ubiquitous and useful technology is offered by numerous companies (not just Meta) to web developers spanning numerous industries (not just healthcare). Meta's version of this tool, the "Meta Pixel," is of a piece with other companies' offerings: Meta makes a generic bit of code publicly available, and third-party web developers can freely customize and install it to help them improve the online services they offer.

Second, web developers—not Meta—choose whether, where, and how they will use the Meta Pixel. Meta's Business Tools Terms, which all web developers (healthcare provider or not) must agree to before integrating the Pixel code on their websites, (1) require web developers to confirm that they have the proper permissions and legal right to share any data they choose to send, and (2) tell web developers not to send *any* "health" or other sensitive information. Meta also has implemented a filtering mechanism to screen out potentially sensitive health data it detects, and to alert the developer so it can check how it has configured the Pixel and fix any issues. But it is ultimately the developer, not Meta, that controls the code on its own website and chooses what information to send. Plaintiffs attempt to distract the Court from these points by detailing the ways in which Meta allegedly encourages businesses in the healthcare sector to use its Business Tools, but these allegations miss the

point: These companies can use Meta's Pixel without sending health information to Meta, and are expected to use the Pixel in compliance with Meta's terms.

Plaintiffs have filed a grab-bag complaint asserting thirteen causes of action, ranging from "wiretap" violations to larceny to trespass. But *none* of those causes of action fits plaintiffs' theory of the case—that *Meta* should be held liable for certain *healthcare providers'* alleged misuse of a publicly available tool that Meta did not implement or configure on the providers' websites. As a result, the claims fail for a host of reasons that this Court had no occasion to consider when it evaluated plaintiffs' preliminary injunction motion.[1] Several of the claims—including the federal and state wiretapping claims—fail because plaintiffs do not allege the requisite intent by Meta to receive sensitive health information. Other claims fail because they are based on California laws that do not apply extraterritorially, and none of the plaintiffs is a California resident. Still others, like larceny and trespass, cannot be stretched to encompass the technology at issue and the facts alleged in this case. And many of the claims fail for *all* these reasons, plus element-specific reasons all their own.

The causes of action asserted in the complaint are poor vessels for the misguided theory of the case plaintiffs have advanced against Meta, and each of them should be dismissed.

BACKGROUND

A. Meta's Pixel

This case centers on the Meta Pixel, "a free and publicly available piece of code that Meta allows third-party website developers" in "a range of industries" to "install on their websites." Dkt. 159 at 2–3.[2] Developers can use the Pixel to (1) measure certain actions taken by users on the developers' own sites and apps, and (2) assess and improve the effectiveness of the developers' advertising. Compl. ¶¶ 101–03. The Pixel is "customizable," and developers "choose the actions the

[1] Meta respectfully maintains that Facebook users consented to the data-sharing practices at issue in this case based on the clear and broad disclosures users must agree to when they create a Facebook account. *See* Dkt. 76 at 15–20. But in light of this Court's contrary ruling in its order denying a preliminary injunction, Dkt. 159 at 12–17, this motion addresses the numerous other problems with plaintiffs' claims.

[2] Plaintiffs allege the Pixel is used on applications as well, but it is used only on websites. *See, e.g.*, Compl. ¶¶ 6, 63, 242; Request for Judicial Notice ("RJN") Ex. 6. Other "tracking tools," like the SDK, are used on applications. *See* Dkt. 205 (Conditional Joint Motion to Relate); Compl. ¶¶ 1, 7.

Pixel will track and measure" on their websites. Compl. ¶ 44. While Meta provides instructions on how to install the Pixel, developers decide whether, how, where, and when to use it. Compl. ¶¶ 46–47.

B. Meta's Terms

When users sign up for a Facebook account, they agree to Meta's Terms of Service (the "Terms"), which govern the relationship between Meta and its users. Meta's Terms govern the "use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software" Meta offers. RJN Ex. 1 at 1. The Terms provide that Meta's "liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms or the Meta Products" (including the Meta Pixel). *Id.* at 7. Users also agree to Meta's Privacy Policy, which notes that Meta "collect[s] and receive[s] information from" third parties, including information about "[w]ebsites you visit and cookie data, like through . . . the Meta Pixel." RJN Ex. 4 at 6–7.

Third-party web developers that use Meta's services—including the Meta Pixel tool—must agree to Meta's Business Tools Terms and Commercial Terms. The Business Tools Terms require developers to "represent and warrant" that they "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." RJN Ex. 2 at 2. 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 3–4.

To use the Pixel, developers must agree not to "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. The Commercial Terms contain similar restrictions, and require developers to agree not to "send to [Meta], or use Meta [Pixel] to collect from people . . . health, financial, biometrics, or other categories of similarly sensitive information." RJN Ex. 3 at 2.

C. Plaintiffs' Allegations

Plaintiffs are Maryland, Wisconsin, North Carolina, Ohio, and Missouri residents and Facebook users who communicate with their healthcare providers through the providers' websites. Compl. ¶¶ 24–28. They allege their providers incorporated the Meta Pixel onto their websites in a manner that resulted in the following information being sent to Meta: (1) that the plaintiffs were "communicating" with the providers' websites (without specifying what was being communicated); (2) that the plaintiffs clicked the login buttons on their providers' websites; (3) that two of the plaintiffs had "previously visited" webpages about breast health and medical records; (4) the plaintiffs' IP addresses; and (5) cookies and browser attributes. Compl. ¶¶ 79, 81–82. As a result, plaintiffs allege the providers sent information to Meta revealing their identity, that they logged into their providers' patient portals, and the pages they visited before logging in. Compl. ¶¶ 80, 82.

Plaintiffs allege Meta encourages "health" entities to use its tools, including the Meta Pixel, and to advertise on Meta's platforms. Compl. ¶ 126; *see* Compl. ¶¶ 129–46. Plaintiffs also allege Meta does not verify that developers have consent to share the data they send. Compl. ¶¶ 115–16. But the complaint acknowledges Meta has a filtration system to detect and filter out potentially sensitive health data, including "information that web developers have no right to send." Compl. ¶¶ 118, 125.

Plaintiffs bring thirteen claims against Meta, seeking monetary and injunctive relief on behalf of themselves and a putative class of "[a]ll Facebook users whose health information was obtained by Meta from their health care provider or covered entity." Compl. ¶ 274.

LEGAL STANDARD

A complaint must "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). On a motion to dismiss, the Court must first separate the complaint's legal conclusions—which are disregarded—from its factual allegations. *Id.* at 678–79. The remaining factual allegations must "raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555. If the complaint pleads facts that are "'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of entitlement to relief.'" *Iqbal*, 556 U.S.

at 678 (quoting *Twombly*, 550 U.S. at 557). Claims also may be dismissed based on a dispositive issue of law. *Seismic Reservoir 2020, Inc. v. Paulsson*, 785 F.3d 330, 335 (9th Cir. 2015).

ARGUMENT

A. Plaintiffs Do Not State a Claim Under the Federal Wiretap Act (Claim 3)

"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) (quoting 18 U.S.C. § 2511(1)(a)–(e)). Plaintiffs must plausibly allege that Meta "(1) intentionally (2) intercepted (3) the contents of (4) plaintiffs' electronic communications (5) using a device." Dkt. 159 at 17. And because the Wiretap Act is a one-party consent statute, Meta is not liable if *any* party to a communication consented to sharing it, unless Meta obtained the information for "the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Plaintiffs' claim fails to meet these requirements.

1. Plaintiffs Fail to Adequately Plead Intent

Plaintiffs' Wiretap Act claim fails because they do not allege that Meta *intentionally*—that is, "purposefully and deliberately"—intercepted their sensitive health information. *United States v. Christensen*, 828 F.3d 763, 774 (9th Cir. 2015).[3] Where a party obtains information "as a result of accident or mistake," *id.*, or an alleged interception is "the product of inadvertence," *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003), the intent element is not satisfied. Rather, the defendant must have "acted *consciously and deliberately* with the goal of intercepting wire communications." *Christensen*, 828 F.3d at 775 (emphasis added). Even a party who sells and installs a recording system, and provides instructions for its use, is not liable for another party's misuse of that system. *See Federated Univ. Police Officers' Ass'n v. Regents of Univ. of Cal.*, 2015 WL 13273308, at *7 (C.D. Cal. July 29, 2015). So too here: Meta's actions in making a standard Internet tool "free and publicly available," Compl. ¶ 39, do not give rise to liability whenever a web developer misuses that tool.

Plaintiffs assert that Meta "intentionally intercepted" their health information, *see* Compl. ¶¶ 335, 358, but offer no factual allegations in support. Developers—not Meta—control whether, how, and where to use the pixel tool. *See* Compl. ¶¶ 39, 44–46. Meta contractually *prohibits* web developers

[3] At the preliminary injunction stage, Meta did "not dispute that the intentional or interception elements are met." Dkt. 159 at 18. The Court has thus not yet assessed Meta's "intent" arguments.

from sending potentially sensitive information. *See* RJN Ex. 2 at 2. Plaintiffs acknowledge Meta's efforts to "create[] a 'filter to detect data sent through the Pixel' that Meta 'categorizes as potentially sensitive data, including health data.'" Compl. ¶ 118 (quoting Wooldridge Decl. ¶ 8); *see* Compl. ¶ 125. And they invoke Meta's "public descriptions of systems it already has in place" and Meta's position that it "d[oes] not want health information." Compl. ¶¶ 148–49. Taken separately or together, these allegations affirmatively *negate* any suggestion that Meta's "purpose[]" is to receive sensitive health information. *Christensen*, 828 F.3d at 774.

Plaintiffs allege that Meta encourages "health" companies to use the pixel tool and advertise with Meta. *See, e.g.*, Compl. ¶¶ 126–27, 131, 134–46, 231, 242–43. But those allegations do not plausibly suggest any intent to receive *sensitive* health information for a simple and commonsense reason: Just like any other entity that may possess some sensitive information about its customers, healthcare providers can use the pixel tool in any number of perfectly legitimate ways without sharing sensitive data. *E.g.*, *Smith v. Facebook, Inc.*, 745 F. App'x 8, 8–9 (9th Cir. 2018). Given the many legitimate uses of the Meta Pixel on health-related websites, the alleged existence of a Meta "Health" marketing division does not plausibly suggest any unlawful intent to receive sensitive data.[4]

The Wiretap Act claim must be dismissed due to lack of intent.

2. The One-Party Consent Exemption Applies

The Wiretap Act claim also must be dismissed because at least one party (the providers who configured the Meta Pixel on their website) consented—indeed, affirmatively chose—to share information with Meta, and Meta lacked any criminal or tortious purpose in receiving that information.

The Wiretap Act does not impose liability "where *one* of the parties to the communication has given prior consent" unless the "communication [was] intercepted for the purpose of committing any

[4] Some courts have allowed Wiretap Act claims to proceed beyond the pleadings stage where "a defendant is aware of the defect causing the interception but takes no remedial action." *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014). These decisions are inconsistent with the Ninth Circuit's decision in *Christensen*, because mere knowledge of a defect does not constitute "act[ing] consciously and deliberately with the goal of intercepting wire communications." 828 F.3d at 774. But even if those cases were correctly decided, they would not help plaintiffs here, because plaintiffs do not plausibly allege that Meta declined to take any remedial action. Rather, Meta *has* taken action to remedy the conduct of developers who violate these policies by creating a filtration system that aims to detect and filter out even *potentially* sensitive health data. *See* Compl. ¶¶ 118, 125(c).

criminal or tortious act." 18 U.S.C. § 2511(2)(d) (emphasis added); *see In re Facebook*, 956 F.3d at 607. The healthcare providers "who configured the Pixel on their websites presumably consented to Meta's receipt of the information." Dkt. 159 at 20; *see Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at *10 (N.D. Cal. Apr. 6, 2023). To state a claim, then, plaintiffs must plausibly allege that Meta intercepted their information "for the purpose of committing" a crime or tort. 18 U.S.C. § 2511(2)(d). They fail to do so.

The requisite criminal or tortious purpose "must be *separate and independent* from the act of the recording." *Planned Parenthood Fed'n of Am., Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022) (emphasis added). Plaintiffs had to allege both that Meta intended to *intercept* their communications (*see supra* at 5–6), and that Meta intended to *use* their data to commit an independent crime or tort. "[T]he focus is *not* upon whether the interception itself violated [the] law; it is upon whether the *purpose* for the interception—its intended use—was criminal or tortious." *Planned Parenthood*, 51 F.4th at 1136; *see also United States v. McTiernan*, 695 F.3d 882, 890 (9th Cir. 2012) (courts "look to the purpose" and ask whether it "directly facilitates" some *other* "criminal conduct"). And the defendant must have intended to use the recording to commit a crime or tort "[a]t the time of the recording." *Planned Parenthood*, 51 F.4th at 1136.

Plaintiffs allege that Meta's purpose in making its pixel tool available to developers is to help companies in a wide range of industries improve their online advertising and services. *See, e.g.*, Compl. ¶¶ 39–42. Acting for commercial gain is not a criminal or tortious purpose. *See* Dkt. 159 at 21; *see also Katz-Lacabe*, 2023 WL 2838118, at *10; *Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 n.8 (N.D. Cal. May 21, 2021); *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 518 (S.D.N.Y. 2001); *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014). In *Katz-Lacabe*, the plaintiffs alleged that the defendant used cookies and tracking pixels to collect personal data and then "to aggregate and synchronize the collected data to perform 'identity resolution,'" which the defendant traded and sold to third-party data brokers and clients for profit. 2023 WL 2838118, at *1–2, *10. The crime-tort exception did not apply because the defendant's purpose was commercial profit, not to commit a tort, and the court dismissed the Wiretap Act claim. *Id.* at *10.

So too here. Plaintiffs allege that Meta received sensitive data through the Meta Pixel to enhance its advertising and "to make money," not "to perpetuate torts on millions of Internet users." *Katz-Lacabe*, 2023 WL 2838118, at *10. Meta's policies prohibiting developers from sending sensitive health information confirm that Meta did not intend to use the Pixel to commit a crime or tort. And Meta's attempts to filter out any potentially sensitive health information that developers send in violation of its terms drive the point home—Meta did not have any "criminal or tortious purpose at the time the [interception] was made." *Planned Parenthood*, 51 F.4th at 1136; *see* Compl. ¶¶ 118, 125(c).

Plaintiffs present a laundry list of various crimes and torts that they allege Meta committed by receiving their sensitive health data. Compl. ¶ 347. Not one of those alleged purposes is "separate and independent from the act of recording." *Planned Parenthood*, 51 F.4th at 1136; *Sussman v. Am. Broad. Cos.*, 186 F.3d 1200, 1202 (9th Cir. 1999). Rather, the crimes and torts plaintiffs tick off "occur[] through the act of interception itself." *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 145 (3d Cir. 2015). Plaintiffs concede as much when they allege "[i]n *acquiring the contents of Plaintiffs' and Class Members' communications relating to patient portals, appointments, and phone calls*, Meta had a purpose that was tortious, criminal, and designed to violate state constitution and statutory provisions," and then list thirteen laws Meta allegedly violated through that acquisition. Compl. ¶ 347 (emphasis added). Plaintiffs thus allege that Meta's purpose was to commit a tort or crime *through the act of interception itself*.

A closer look at these allegations confirms that plaintiffs do not allege an independent crime or tort. Subparagraphs 347(a) through (c) concern the alleged "unauthorized acquisition of individually identifiable health information" under HIPAA—*i.e.*, "the act of interception itself." *In re Google Inc. Cookie Placement*, 806 F.3d at 145. Subparagraphs (d) through (h), (j), and (k) list several of plaintiffs' other causes of action, all of which also concern Meta's alleged interception of information. Subparagraph (i) alleges "[v]iolations of various state health privacy statutes," including California's "Confidentiality of Medical Information Act," "Consumer Privacy Protection Act," and "Consumer Privacy Act," without further explanation. And subparagraph (l) restates two federal wire fraud provisions, which concern devising a scheme to defraud another out of money or property without any further explanation; but plaintiffs do not allege that Meta defrauded them out of money or property.

See Compl. ¶ 348; *infra* at 24. Because plaintiffs have not alleged that Meta intercepted their sensitive information for the *purpose* of committing a crime or tort "separate and independent" of receipt itself, the crime-tort exception is inapplicable.

3. Most Of The Allegedly Intercepted Information Was Not "Content"

The Wiretap Act requires interception of "the content of a communication"—"the intended message conveyed by the communication, and [not] 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). Plaintiffs allege Meta intercepted: (1) the name of SubscribedButtonClick events; (2) previously visited provider websites; and (3) IP addresses and other identifiers that can identify plaintiffs and their devices. Compl. ¶¶ 79(c)–(h), 81(c)–(h), 339. This Court has stated that the name of SubscribedButtonClick events may be "content" that was intercepted, Dkt. 159 at 18–19, but none of the remaining items constitutes content.

First, any information used to identify plaintiffs or their devices, including IP address, is record information, not content. Record information is data "generated in the course of the communication," including the "name, address and subscriber number or identity of a subscriber or customer"; and the "origin, length, and time of a call, or geolocation data." *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021) (quoting *Zynga*, 750 F.3d at 1106). "There is no language in [the Wiretap Act] equating 'contents' with personally identifiable information." *Zynga*, 750 F.3d at 1107.

Second, plaintiffs do not allege that Meta received any content pertaining to websites they previously visited. URLs that merely contain the "address of the webpage the user was viewing before clicking on [an] icon" are not, without more, content. *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 265 (N.D. Cal. 2016); *see Katz-Lacabe*, 2023 WL 2838118, at *9. This Court has observed that *some* URL information, such as that identified in the Smith Declaration, can be sufficiently descriptive to qualify as "content" where it includes both path and query strings. *See* Dkt. 159 at 19 & n.10. But the Smith Declaration is not tethered to the named plaintiffs' claims: plaintiffs do not allege that Meta intercepted URLs that contain query strings. Instead, they allege, *e.g.*, that Meta learned that John Doe I communicated with MedStar via "www.MedStarHealth.org" and "[h]e had previously visited a MedStar page about breast health." Compl. ¶ 79(a), (e). The screenshots accompanying paragraphs

79 and 81 of the complaint confirm the lack of any "content"; there are no query strings and neither the referer header nor the destination header contain "content" information under *Zynga*. Thus, the named plaintiffs' allegations regarding information that Meta received about *their own* previously visited websites do not plausibly establish Meta received any content.[5]

B. The Complaint Does Not State a Claim Under CIPA (Claim 4)

Plaintiffs also bring a claim under the California Invasion of Privacy Act (CIPA), a state analogue to the Wiretap Act. That claim also suffers from multiple deficiencies that compel dismissal.

1. CIPA Does Not Apply Extraterritorially

Plaintiffs are Maryland, Wisconsin, North Carolina, Ohio, and Missouri residents who do not allege that the alleged misconduct took place in California. *See* Compl. ¶¶ 24–28. "Under California law, a presumption exists against the extraterritorial application [of] state law." *O'Connor v. Uber Techs., Inc.*, 58 F. Supp. 3d 989, 1004 (N.D. Cal. 2014). Courts must "presume the Legislature did not intend a statute to be operative, with respect to occurrences outside the state, . . . unless such intention is clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history." *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011) (citations omitted).

Nothing in CIPA displaces the presumption. CIPA's intent is "to protect the right of privacy of the ***people of this state***." Cal. Penal Code § 630 (emphasis added). Had the Legislature intended to provide for extraterritorial application, it would have done so expressly—as it has in other statutes. Plaintiffs are not "people of this state," and none of their providers is based in California. Nor do they allege that they accessed their providers' websites in California, that they were injured in California, or that any wiretapping or eavesdropping took place in California. They cannot bring a CIPA claim.

2. Plaintiffs Fail to Plausibly Allege Meta Had the Requisite Intent

Sections 631(a) and 632(a) of CIPA both require a showing that the defendant *intentionally* engaged in wiretapping or eavesdropping. Cal. Penal Code §§ 631(a), 632(a). Plaintiffs must plead "specific factual circumstances that make plausible [Meta's] intent to record a confidential

[5] Plaintiffs allege additional "contents" in conclusory fashion. *See* Compl. ¶ 338. But again, those generic references are not tethered to any allegations about the named plaintiffs' data. Compl. ¶¶ 79, 81; *see* Compl. ¶ 82.

communication." *Vartanian v. VW Credit, Inc.*, 2012 WL 12326334, at *2 (C.D. Cal. Feb. 22, 2012). They have not done so.

Section 632(a)'s intent requirement is satisfied only if the plaintiff proves "the person using the recording equipment [did] so with the *purpose or desire* of recording a confidential conversation, or with the *knowledge to a substantial certainty* that his use of the equipment will result in the recordation of a confidential conversation." *People v. Superior Court (Smith)*, 70 Cal. 2d 123, 134 (1969) (emphases added). It is not enough to intend to use a recording device; instead, a defendant must intend to use it *for an impermissible purpose*. This rule "provides effective protection against 'eavesdroppers' without penalizing the innocent use of recording equipment." *Id.* Section 631(a) likewise requires that a defendant "intentionally tap[ped]" or "willfully and without the consent of all parties to the communication . . . reads, or attempts to read . . . the contents or meaning of any message, report or communication." Cal. Penal Code § 631(a). The intent requirement must be interpreted the same way across both provisions. *Cal. Soc'y of Anesthesiologists v. Brown*, 204 Cal. App. 4th 390, 403 (2012).

Because CIPA requires an *affirmative desire* to eavesdrop on or intercept a confidential communication, the "deploy[ment of] recording devices that *might* happen" to record such information is insufficient. *Lozano v. City of Los Angeles*, 73 Cal. App. 5th 711, 727–28 (2022) (quoting *Smith*, 70 Cal. 2d at 134); *see also, e.g.*, *Federated Univ. Police Officers' Ass'n v. Regents of Univ. of Cal.*, 2015 WL 13273308, at *10 (C.D. Cal. July 29, 2015) (no liability for selling and installing a recording device). The unintentional or inadvertent receipt of information "by chance" likewise cannot support a CIPA claim. *Smith*, 70 Cal. 2d at 133. "[A] person might intend to record the calls of wild birds on a game reserve and at the same time accidentally pick up the confidential discussions of two poachers. To hold the birdwatcher punishable under [CIPA] for such a fortuitous recording would be absurd." *Id.*; *see also People v. Buchanan*, 26 Cal. App. 3d 274, 287–88 (1972) (finding no intent where switchboard operator "inadvertent[ly]" overheard a telephone conversation).

Pixels are a useful, legal, ubiquitous internet analytics tool, and creating a tool and making it freely available to others is not the intentional conduct that CIPA prohibits. *See Federated Univ.*, 2015 WL 13273308, at *10. Nor does it plausibly establish that Meta knew with "substantial certainty" that it would be receiving potentially sensitive health-related data from providers. *See Smith*, 70 Cal. 2d at

134. Given that Meta took steps to filter out such information as well as the undisputed fact that Meta contractually barred developers from sending it such data, there is no basis to conclude that Meta *intended* to receive any potentially sensitive health information.

3. Plaintiffs Do Not Plausibly Allege Data Was Sent From or Received in California

Section 631(a) applies only when a person "reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication" while it is "being sent from, or received at any place ***within this state***." Cal. Penal Code § 631(a) (emphasis added). Plaintiffs do not plausibly allege any data was sent from or received in California. *See supra* at 10. They merely allege, in conclusory fashion, that Meta "designed and effectuated its scheme to track the patient communications at issue here from California." Compl. ¶ 369. Another judge in this district recently dismissed a CIPA claim against Google on this precise basis, holding it was not enough to allege that "events and conduct giving rise to Plaintiffs' claims occurred in California" or that "California is the state from which [defendant]'s alleged misconduct emanated." *Hammerling v. Google LLC*, 2022 WL 17365255, at *11 (N.D. Cal. Dec. 1, 2022). Nor is the presence of Meta's headquarters in California, *see* Compl. ¶¶ 29, 369, enough to demonstrate where plaintiffs' information was actually "sent from" or "received." Cal. Penal Code § 631(a); *Hammerling*, 2022 WL 17365255, at *11.

4. Plaintiffs Do Not Plausibly Allege that Meta Used a "Device"

The section 632(a) claim also fails because plaintiffs do not plausibly allege Meta used any "electronic amplifying or recording device[s]." Cal. Penal Code § 632(a). A device under CIPA is "a thing made or adapted for a particular purpose, especially a piece of mechanical or electronic equipment." *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14, 2017). CIPA therefore applies to *devices* such as video recorders, *People v. Lyon*, 61 Cal. App. 5th 237, 245 (2021), but not software or apps, *In re Google Location History Litig.*, 428 F. Supp. 3d 185, 193 (N.D. Cal. 2019) (Google Maps); *Moreno*, 2017 WL 6387764, at *5 (mobile software). The CIPA claim does not identify any "device" Meta allegedly used, and the "devices" identified in the Wiretap Act claim do not qualify for devices under CIPA. *See* Compl. ¶ 340. The Pixel and cookies do not qualify because CIPA does not apply to software. *See In re Google Location History*, 428 F. Supp. 3d

at 193; *Moreno*, 2017 WL 6387764, at *5.[6] The remaining "devices" do not qualify because they are not used to "record [any] confidential communication." Cal. Penal Code § 632(a).

C. Plaintiffs Do Not State a Constitutional Privacy (Claim 6) or Intrusion Upon Seclusion (Claim 5) Claim

The "California Constitution and the common law both set a high bar for an invasion of privacy claim," *Bellumini v. Citigroup, Inc.*, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014), and courts typically assess them together. *Hernandez v. Hillside, Inc.*, 47 Cal. 4th 272, 288 (2009). A plaintiff "must demonstrate (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Lewis v. Superior Court*, 3 Cal. 5th 561, 571 (2017) (quotation marks omitted). Plaintiffs fail to plausibly allege these claims.

The California Constitution Does Not Apply Extraterritorially. The fact that none of the plaintiffs is a California resident dooms their constitutional claim. *See supra* at 10; Compl. ¶¶ 24–28. The presumption against extraterritoriality applies to California Constitution claims, *see People v. Bustamante*, 57 Cal. App. 4th 693, 699 n.5 (1997), and the privacy provision's purpose is to protect "Californians." *Williams v. Superior Court*, 3 Cal. 5th 531, 552 (2017); *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 125 (2006).

No Legally Protected Interest. This Court previously held that plaintiffs had a legally protected interest in "[c]ommunications made in the context of a patient-medical provider relationship." Dkt. 159 at 24–25. But critically, plaintiffs' complaint does not plausibly allege such communications within the meaning of *this* cause of action. A constitutionally protected informational privacy interest is limited to "*sensitive* and *confidential* information," *In re Yahoo*, 7 F. Supp. 3d at 1041, such as "symptoms, family history, diagnoses, test results and other intimate details concerning treatment," *Grafilo v. Wolfsohn*, 33 Cal. App. 5th 1024, 1034 (2019) (quoting *Lewis*, 3 Cal. 5th at 575).

There are no specific allegations about the kinds of data Meta allegedly received about John Doe II or Jane Does II and III. Compl. ¶ 82. John Doe I's and Jane Doe I's allegations are likewise

[6] Although *Moreno* and *In re Google Location History* concern a separate provision of CIPA that addresses electronic tracking devices, the term "device" should be interpreted the same way across the statute. *See Brown*, 204 Cal. App. 4th at 403.

very limited. These plaintiffs allege that Meta received information allowing it to infer that (1) they were using a device associated with a particular Facebook account and (2) they attempted to log in to their providers' patient portals. *See* Compl. ¶¶ 79–81. This data is not sensitive information on the order of medical history or "intimate details concerning treatment." *Grafilo*, 33 Cal. App. 5th at 1034. Neither plaintiff alleges that Meta received medical histories, profiles, or indeed any information about their treatment. *Id.* They have not plausibly alleged any "[c]ommunications made in the context of a patient-medical provider relationship" in which they had a legally protected interest. Dkt. 159 at 24.[7]

No Sufficiently Serious Invasion. These claims also fail because plaintiffs do not allege an invasion that is "sufficiently serious" as to "constitute an egregious breach of the social norms underlying the privacy right." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 37 (1994). This Court previously suggested that Meta did "behave[] egregiously," comparing Meta's conduct to the theft of personal information. Dkt. 159 at 26–27. But again, the named plaintiffs do not allege that Meta obtained such information about *them*, much less that it did so with the intent of committing theft.

Meta's efforts to filter potentially sensitive health information are also highly "relevant in the 'highly offensive'" inquiry, Dkt. 159 at 26–27 (quoting *In re Facebook Internet Tracking Litig.*, 956 F.3d at 606). "[N]o cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights." *Hernandez*, 47 Cal. 4th at 295. "[N]egligent conduct" or conduct such as implementing "low-budget security measures," even with an "absolute disregard of [their] consequences," and even if they result in the loss of sensitive information like social security numbers, is *not* sufficiently egregious. *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012).

Plaintiffs' failure to plausibly allege that Meta "disseminat[ed] or misuse[d]" any sensitive health information further undermines any assertion that Meta's alleged breach was "sufficiently

[7] The rest of the information allegedly sent to Meta—IP address, browser information, and previously accessed webpages, *see* Compl. ¶ 81(e)–(f), (h)—does not constitute communications, let alone legally protected communications. This information is record information and automatically generated information such as non-descriptive URLs. *See supra* at 9–10. This distinguishes the alleged information here from "detailed URLs" discussed in the preliminary injunction order. Dkt. 159 at 25. This information does not qualify as legally protected information. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *Zynga*, 750 F.3d at 1108; *see also Smith v. Facebook*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. 2017) (URLs containing general health information are not protected health information).

serious." *Hill*, 7 Cal. 4th at 35. Plaintiffs simply allege they have "an interest in precluding the dissemination and misuse of their health information by Meta," without plausibly alleging *how* Meta disseminated or misused their information. Compl. ¶ 393. "Without more allegations as to what, if anything, [Meta improperly] did with this information, [plaintiffs] ha[ve] not plausibly alleged a serious invasion of privacy." *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1092–93 (N.D. Cal. 2018); *see White v. Soc. Sec. Admin.*, 111 F. Supp. 3d 1041, 1053 (N.D. Cal. 2015).

D. Plaintiffs Fail to Plausibly Allege Violation of the CDAFA (Claim 12)

The California Comprehensive Data Access and Fraud Act (CDAFA) is a misfit for this case. CDAFA is an "anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose." *Custom Packaging Supply, Inc. v. Phillips*, 2015 WL 8334793, at *3 (C.D. Cal. Dec. 7, 2015). But this is not a "hacking" case. Plaintiffs allege Meta "knowingly accessed, used, and caused to be used" plaintiffs' devices through the Pixel and _fbp cookie in violation of several sections of the CDAFA, Compl. ¶¶ 478–79, but that shoehorn attempt falls flat.

First, CDAFA does not apply extraterritorially. CDAFA was promulgated to ensure the well-being of individuals and entities "***within this state*** that lawfully utilize" computers, computer systems, and computer data. Cal. Penal Code § 502(a) (emphasis added); *see id.* § 502(e)(3), (f). "[T]he California Penal Code"—including CDAFA—is therefore not "intended to reach . . . extra-territorial activity." *M Seven Sys. Ltd. v. Leap Wireless Int'l Inc.*, 2013 WL 12072526, at *3 (S.D. Cal. June 26, 2013). And plaintiffs fail to allege any misconduct in California. *See supra* at 10, 12.

Second, CDAFA requires alleged "damage or loss by reason of a violation," which plaintiffs do not and cannot allege. Cal. Penal Code § 502(e)(1). Plaintiffs generically allege they were precluded from communicating with their providers using their devices, *see* Compl. ¶ 484(a), (c), but this is not a damage or loss contemplated by CDAFA. *See Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021). Plaintiffs' further claim that they were damaged by "[t]he diminution in value of their protected health information," Compl. ¶ 484(b), is insufficient because "loss of the value of their data" is not "'damage or loss' within the meaning of the CDAFA," *Cottle*, 536 F. Supp. 3d at 488.

Third, plaintiffs fail to plausibly allege Meta violated sections 502(c)(1)–(3) and (6)–(8) of CDAFA. *Gonzales*, 305 F. Supp. 3d at 1090. "[W]hether there is liability under § 502 requires an

analysis of the specific 'acts' that are alleged to constitute an offense and whether there was 'permission' to engage in those acts." *San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1087 (N.D. Cal. 2018). And because CDAFA claims "sound[] in fraud," they are "subject to Rule 9(b)'s [heightened] pleading standard." *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *5 (N.D. Cal. Nov. 20, 2020). These "boilerplate allegations do not survive Rule 8," let alone Rule 9(b). *Gonzales*, 305 F. Supp. 3d at 1090.

Each of these provisions requires "*knowing*" conduct—*knowingly* accessing computer systems, taking data, using computer services, providing a means of accessing a computer system, or introducing a computer contaminant. Plaintiffs do not plausibly allege any knowing conduct. *See supra* at 5–6.

Plaintiffs also fail to plausibly allege violations of sections 502(c)(1) and (c)(8) on additional grounds. To allege a violation of section 502(c)(1), plaintiffs must plausibly allege Meta accessed or used data either (1) in furtherance of a scheme to defraud or (2) to wrongfully control or obtain money, property, or data. Cal. Penal Code § 502(c)(1). But they do not allege any such scheme nor do they plausibly allege that Meta wrongfully controlled or obtained any data, because they do not allege that Meta engaged in intentional wrongdoing. *See supra* at 5–6.

Plaintiffs' claim based on violation of section 502(c)(8) fails because they have not plausibly alleged that Meta "introduce[d] any computer contaminant." Cal. Penal Code § 502(c)(8). CDAFA is "aimed at 'viruses or worms,' and other malware that usurps the normal operation of the computer or computer system." *In re iPhone Application Litig.*, 2011 WL 4403963, at *13 (N.D. Cal. Sept. 20, 2011). Plaintiffs allege that Pixel "is designed to, and does, self-propagate to contaminate users' computers, computer systems, and computer networks," Compl. ¶ 477, but there are no allegations that the Pixel "impair[s] the integrity or availability of" systems, *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1084 (7th Cir. 2016). Nor is the Pixel anything like "viruses or worms." *In re iPhone Application Litig.*, 2011 WL 4403963, at *13. Finally, Meta did not "introduce" anything: developers customize and decide whether and where to implement the Pixel. Compl. ¶¶ 44, 46–47.

E. The Complaint Does Not State Contract-Based Claims Against Meta (Claims 1 & 2)

Plaintiffs bring claims for breach of contract and the implied covenant of good faith and fair dealing, predicated on alleged violations of Meta's Terms and Privacy Policy. Those claims are barred by Meta's limitation-of-liability provision and are meritless in any event.

1. Meta's Terms contain a clear limitation-of-liability provision: "[Meta]'s liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms or the Meta Products." RJN Ex. 1 at 7. California law enforces such clauses "unless [they are] unconscionable." *Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.*, 209 Cal. App. 4th 1118, 1126 (2012).

This clause is not unconscionable. "[U]nconscionability has both a 'procedural' and a 'substantive' element, the former focusing on 'oppression' or 'surprise' due to unequal bargaining power, the latter on 'overly harsh' or 'one-sided' results." *Armendariz v. Found. Health Psychare Servs., Inc.*, 24 Cal. 4th 83, 114 (2000). Procedurally, there is no "rule that an adhesion contract is per se unconscionable." *Poublon v. C.H. Robinson Co.*, 846 F.3d 1251, 1261–62 (9th Cir. 2017). Judge Alsup has held that because "the procedure followed by Facebook was fair," the limitation-of-liability "clause was not buried," and it "contain[s] clear enough language," the clause is not unconscionable. *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037–38 (N.D. Cal. 2019). Substantively, these clauses are routinely enforced where, as here, the complained-of conduct involves third parties. *See, e.g.*, *Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016), *aff'd*, 700 F. App'x 588, 590 (9th Cir. 2017); *Darnaa, LLC v. Google LLC*, 756 F. App'x 674, 675 (9th Cir. 2018).

2. Plaintiffs' contract claims also fail on the merits. Plaintiffs fail to identify "sufficiently definite" provisions that allow the court "to ascertain the parties' obligations and to determine whether those obligations have been performed or breached." *Sateriale v. R.J. Reynolds Tobacco Co.*, 697 F.3d 777, 789 (9th Cir. 2012). A "promise must be definite enough that a court can determine the scope of the duty[,] and the limits of performance must be sufficiently defined." *Ladas v. Cal. State Auto. Ass'n*, 19 Cal. App. 4th 761, 770 (1993). The complaint contains a chart that purports to outline four "promises and Meta's breach." Compl. ¶ 312. These provisions are not sufficiently definite to support a contract claim. *Doe v. Cal. Inst. of Tech.*, 2019 WL 8645652, at *5 (C.D. Cal. Aug. 13, 2019) (provisions stating investigators would be impartial, trained in relevant issues, not retaliate for reporting misconduct, and not tolerate intentional false reporting, were "not 'sufficiently definite'").

Plaintiffs principally rely on Meta's commitment to "require" partners to have the right to share user information with Meta. But that alleged promise does not allow "a court [to] determine the scope of [Meta's] duty" or the "limits of performance," *Ladas*, 19 Cal. App. 4th at 770. The Court's prior statement that "'require' is susceptible to multiple meanings" confirms that this statement is not sufficiently definite to provide a basis for a breach of contract claim. Dkt. 159 at 17. Analyzing a similar provision, Judge Davila held that the "data policy only represents that it would 'require'" certain conduct, which does not provide an actionable contract claim as Meta "makes no guarantees about how [it] would enforce that requirement." *In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980, 1013 (N.D. Cal. 2020). The other provisions all discuss methods by which Meta *detects* "potential misuse," but state nothing about the scope of those duties or what (if any) affirmative obligations Meta may have if potential misuse is discovered. That Meta will "take appropriate action" if there is potential misuse, Compl. ¶ 312, fails to remedy this problem: to the extent plaintiffs claim Meta's filters do not constitute "appropriate action," the terms they cite are not "sufficiently definite" to evaluate that claim.

3. Even if these provisions were sufficiently definite to support a contract claim, plaintiffs have failed to allege that they were breached. Plaintiffs simply quote the contract and say Meta "has not" or "does not" adhere to its provisions. Their claim that Meta does not "require Partners to have the right to . . . share [users'] information before giving it to" Meta is undermined by the Business Tools Terms and Commercial Terms, which *do* require exactly that. RJN Ex. 2 at 2, Ex. 3 at 2. Plaintiffs contend this contractual requirement is insufficient, but they supply no basis to demand performance over and above that or Meta's filtration efforts. *See Ladas*, 19 Cal. App. 4th at 770.

4. Plaintiffs' tagalong claims fail as duplicative. *First*, plaintiffs allege that "an implied contract also exists between Meta and Plaintiffs . . . that Meta will not conspire with others to violate Plaintiffs' . . . legal rights to privacy in their individually identifiable health information." Compl. ¶ 313. But plaintiffs acknowledge that there is a valid contract between the parties, and an implied contract claim "cannot lie where there [is] a valid and express contract covering the same subject matter." *O'Connor*, 58 F. Supp. 3d at 999–1000.

Second, plaintiffs allege Meta breached the implied covenant of good faith and fair dealing by failing to take sufficient affirmative steps and "appropriate action" to ensure providers had the right to

collect and share their data. *See, e.g.*, Compl. ¶¶ 323–27. But an implied covenant "cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement." *Rosenfeld v. JPMorgan Chase Bank*, 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010); *see Guz v. Bechtel Nat'l Inc.*, 24 Cal. 4th 317, 349–50 (2000); *Partti v. Palo Alto Med. Found. for Health Care, Rsch. & Educ., Inc.*, 2015 WL 6664477, at *5 (N.D. Cal. Nov. 2, 2015). An implied covenant "is limited to assuring compliance with the *express terms* of the contract, and cannot be extended to create obligations not contemplated by the contract." *Microsoft Corp. v. Hon Hai Precision Indus. Co.*, 2020 WL 5128629, at *8 (N.D. Cal. Aug. 31, 2020); *see Foley v. Interactive Data Corp.*, 47 Cal. 3d 654, 690 (1988). Plaintiffs cannot rewrite the terms of their contract with Meta to impose obligations the agreement itself does not impose.

Further, even if this claim extended beyond the contract claim, plaintiffs have not plausibly alleged that Meta "fail[ed] or refus[ed] to discharge contractual responsibilities . . . by a conscious and deliberate act," as required for an implied-covenant claim. *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990). Their sole suggestion—that "Meta actively solicited [providers'] further disclosures and advertising revenue," Compl. ¶¶ 325–26—is irrelevant. That Meta allegedly encourages *all* companies, including health-related companies, *e.g.*, Compl. ¶¶ 41–42, 116, to use the Pixel does not plausibly establish that Meta deliberately refused to discharge contractual responsibilities or take "appropriate action" against providers who did not have permission to share data with Meta. Compl. ¶¶ 323–27; *see supra* at 3, 6.

F. Plaintiffs' Requested Remedies and the Parties' Agreements Doom the Unjust Enrichment Claim (Claim 13)

Plaintiffs also bring a cursory unjust enrichment claim, which fails for at least two reasons.

First, plaintiffs cannot pursue an unjust enrichment claim as a quasi-contract cause of action where, as here, a "valid express contract covering the same subject matter" exists. *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231 (2014); *see* Compl. ¶¶ 304, 312, 490. Given that there is no "dispute over validity or enforceability" of Meta's Terms and Privacy Policy, dismissal "with prejudice is appropriate." *Day v. GEICO Cas. Co.*, 580 F. Supp. 3d 830, 841 (N.D. Cal. 2022); *Gardiner v. Walmart, Inc.*, 2021 WL 4992539, at *8 (N.D. Cal. July 28, 2021).

Second, plaintiffs fail to plead that they "lack[] an adequate remedy at law" to redress any alleged *past* harm, as they must to bring equitable claims like unjust enrichment. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020); *see also Sharma v. Volkswagen AG*, 524 F. Supp. 3d 891, 907 (N.D. Cal. 2021); *In re Apple Processor Litig.*, 2022 WL 2064975, at *11–12 (N.D. Cal. June 8, 2022). While the court's preliminary injunction order suggested that the "allegedly *ongoing* disclosure of plaintiffs'" potentially sensitive information "cannot be remedied by damages," Dkt. 159 at 28 (emphasis added), that says nothing about whether plaintiffs lack an adequate remedy for any alleged past harm. Because plaintiffs do not allege that legal remedies cannot make them whole for any alleged past violations, this claim must be dismissed.

G. Plaintiffs Have Not Plausibly Alleged a Negligence Per Se Cause of Action (Claim 7)

Plaintiffs' "claim" for negligence per se must be dismissed. "[N]egligence per se is a doctrine, not an independent cause of action," *Dent v. Nat'l Football League*, 902 F.3d 1109, 1117 (9th Cir. 2018), and it does not create a "private right of action for violation of a statute," *Johnson v. Honeywell Int'l Inc.*, 179 Cal. App. 4th 549, 556 (2009). Negligence per se simply establishes a presumption of negligence if the defendant (1) violated a statute; (2) the violation caused injury; (3) the injury "resulted from an occurrence the nature of which the statute . . . was designed to prevent"; and (4) the individual harmed was part of the class of persons the statute was designed to protect. *Quiroz v. Seventh Ave. Ctr.*, 140 Cal. App. 4th 1256, 1285 (2006). But plaintiffs still must plausibly allege an underlying negligence cause of action, which requires breach of a duty of care that caused injury. *See Cal. Serv. Station & Auto Repair Ass'n v. Am. Home Assurance Co.*, 62 Cal. App. 4th 1166, 1177 (1998); *Rosales v. City of Los Angeles*, 82 Cal. App. 4th 419, 430 (2000). Plaintiffs satisfy neither requirement here.

First, plaintiffs have not plausibly alleged Meta had a duty to comply with HIPAA. Compl. ¶ 403.[8] "An alleged HIPAA violation cannot form the basis of a negligence claim," because HIPAA has no private right of action. *Austin v. Atlina*, 2021 WL 6200679, at *3 (N.D. Cal. Dec. 22, 2021); *see Astra USA, Inc. v. Santa Clara Cty.*, 563 U.S. 110, 117 (2011); *Moore v. Centrelake Med. Grp.*,

[8] Outside of HIPAA, plaintiffs allege no applicable duty beyond a cursory reference to "all applicable statutes and regulations," Compl. ¶ 403, but such a reference does not "provide [Meta] with 'fair notice' of the basis of [plaintiffs'] claim," *Rashdan v. Geissberger*, 2011 WL 197957, at *10 (N.D. Cal. Jan. 14, 2011) (finding it insufficient to incorporate preceding paragraphs).

Inc., 83 Cal. App. 5th 515, 535–36 (2022). To allow "HIPAA regulations to define per se the duty and liability for breach" would allow plaintiffs to conjure up such a right despite Congress' decision not to create one. *Skinner v. Tel-Drug, Inc.*, 2017 WL 1076376, at *3 (D. Ariz. Jan. 27, 2017). HIPAA does not apply to Meta in any event. Meta is not a covered entity; nor is it a covered "business associate," which is an entity that "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA]." 45 C.F.R. § 160.103. Plaintiffs do not allege that Meta fits the bill, let alone that it does so for their specific providers.

Second, plaintiffs have not plausibly alleged causation. They make a single conclusory allegation that their purported injuries were "a direct and proximate result of Meta's violations of HIPAA," Compl. ¶ 412, but their other allegations undermine this claim. Plaintiffs admit that no data is sent to Meta unless third parties choose to install the Pixel. Compl. ¶ 39. Plaintiffs further admit that third parties control the nature of the data sent via the "customizable" Pixel. Compl. ¶ 44. Plaintiffs allege Meta encouraged *installation* of the Pixel, Compl. ¶ 41, but they do not plausibly claim Meta encouraged sending HIPAA-protected data through the Pixel. *See* Compl. ¶¶ 71–74, 138–46. By plaintiffs' own account, Meta "did nothing more than create the condition that made Plaintiffs' injuries possible," and is therefore not legally responsible for those injuries. *Modisette v. Apple Inc.*, 30 Cal. App. 5th 136, 154 (2018). To the contrary, the only affirmative actions Meta arguably takes are designed to *avoid* receipt of health information. RJN Ex. 2 at 2, Ex. 4 at 7.

H. Plaintiffs Fail to Plausibly Allege a Trespass to Chattels Claim (Claim 8)

Plaintiffs' trespass claim is another basic misfit for the facts of this case. Plaintiffs say Meta trespassed on their "computing devices" when the Meta Pixel caused the "_fbp" cookie to be placed on their devices, rendering them "useless for exchanging private communications." Compl. ¶¶ 424–25. For plaintiffs to prevail on this claim, they must plausibly allege that "(1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff." *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000); *see also Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1364 (2003). The complaint satisfies neither prong.

First, for the same reasons discussed *supra* at 5–6, plaintiffs have not plausibly alleged Meta had the requisite intent. Intent to trespass "is present when an act is done for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act." Restatement (Second) of Torts § 217 cmt. c (2023 update). Moreover, plaintiffs plainly consented to cookies being placed on their computers when they accepted the Cookies Policy. *See* RJN 5 at 1, 3, 5–6.

Second, plaintiffs fail to allege that Meta "damage[d] the recipient computer []or impair[ed] its functioning." *Intel*, 30 Cal. 4th at 1364. Plaintiffs allege their computing devices "derive substantial value from their ability to facilitate communications with their health care providers or covered entities," Compl. ¶ 423, but do not allege that this was the "intended function[]" of their devices or that any communication was "significantly reduc[ed]." *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1069. For this claim plaintiffs must, and do not, allege a *technical* impairment, like "significantly reducing [a device's] memory and processing power." *Intel*, 30 Cal. 4th at 1356; *see also In re iPhone Application Litig.*, 844 F. Supp. 2d at 1069 (allegations of reduced storage, bandwidth, and battery life did not state a claim because they did not amount to a "significant reduction in service constituting an interference with the intended functioning of the system"); *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 684–85 (N.D. Cal. 2020). "[T]respass to chattels [does] not lie to protect interests in privacy"; plaintiffs cannot "convert privacy harms into property harms." *Casillas v. Berkshire Hathaway Homestate Ins. Co.*, 79 Cal. App. 5th 755, 765 (2022).

Nor can Plaintiffs rely simply on the use of the Pixel and alleged "installation" of the _fbp cookie, *see* Compl. ¶ 424, because "installat[ion] of unwanted code" that "consume[s] portions of the memory on [a plaintiff's] mobile device" does not suffice for a trespass claim. *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15–16 (N.D. Cal. Mar. 26, 2013). Plaintiffs' trespass claim also cannot be premised on nominal damages, *see* Compl. ¶ 426(a), because trespass allows one to "recover only the *actual* damages suffered by reason of the impairment of the property or the loss of its use." *Zaslow v. Kroenert*, 29 Cal. 2d 541, 551 (1946). In the absence of any actual damage or dispossession, a trespass claim will not lie. *See Intel*, 30 Cal. 4th at 308; *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348, 359 (4th Cir. 2006). Plaintiffs do not allege that Meta impaired

the functioning of their devices, and their claim that they were no longer able to send *private* communications is an improper attempt to convert a claimed privacy interest into a property interest.

I. Plaintiffs Fail to Plausibly Allege A Statutory Larceny (Claim 11)

Plaintiffs assert a "statutory larceny" cause of action premised on Penal Code sections 484 and 496, alleging that Meta "stole, took, and fraudulently appropriated" plaintiffs' "individually identifiable health information" and "knew" that this "information was stolen." Compl. ¶¶ 460–62. But larceny is another basic misfit for the facts of this case.

First, statutory larceny does not apply extraterritorially and plaintiffs do not allege any theft occurred in California. *See supra* at 10, 15. There is no "clearly expressed" intent for section 496 to apply outside California, so California's presumption against extraterritoriality bars the application of section 496 here. *Dfinity USA v. Bravick*, 2023 WL 2717252, at *4–5 (N.D. Cal. Mar. 29, 2023).

Second, plaintiffs have not plausibly alleged a violation of section 496. They would have to allege "that (i) the property was stolen or obtained in a manner constituting theft, (ii) the defendant knew the property was so stolen or obtained, and (iii) the defendant received or had possession of the stolen property." *Switzer v. Wood*, 35 Cal. App. 5th 116, 126 (2019). Plaintiffs do not plausibly allege anything was stolen or taken in a manner constituting theft. Plaintiffs freely provided information to their providers. While those providers may have provided some information to Meta allegedly in violation of plaintiffs' *privacy* rights, that does not establish any information was stolen. And even if plaintiffs could prevail on their fraud- or contract-based claims, that is not enough because "a misrepresentation or breach of contract made innocently or inadvertently does not amount to theft." *Carreon v. Edwards*, 2022 WL 4664569, at *5 (E.D. Cal. Sept. 29, 2022); *see Siry Inv., L.P. v. Farkhondehpour*, 13 Cal. 5th 333, 361–62 (2022).

Nor do plaintiffs plausibly allege that Meta *knew* plaintiffs' information was stolen. As explained above, *see supra* at 5–6, plaintiffs have not sufficiently alleged that Meta intended to receive potentially sensitive health information; even assuming some information slipped through Meta's filter, plaintiffs have not alleged any "knowing purchase, receipt, concealment or withholding of stolen property." *Citizens of Humanity, LLC v. Costco Wholesale Corp.*, 171 Cal. App. 4th 1, 18 (2009); *see Chan v. Lund*, 188 Cal. App. 4th 1159, 1172 (2010).

Third, to the extent plaintiffs assert this claim under section 484, it must be dismissed because section 484 does not provide a private cause of action. *See Durand v. U.S. Customs*, 163 F. App'x 542, 544–45 (9th Cir. 2006); *Windham v. Davies*, 2015 WL 461628, at *6 (E.D. Cal. Feb. 3, 2015).

J. The UCL (Claim 9) and CLRA (Claim 10) Claims Fail on Multiple Counts

Plaintiffs' UCL and injunction-only CLRA claims fail for a long list of reasons.

First, neither claim applies extraterritorially, and the complaint contains no plausible allegations showing that "the liability-creating conduct" occurred in California. *Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018); *see supra* at 10, 15. "[T]he presumption against extraterritoriality applies to the UCL in full force." *Sullivan*, 51 Cal. 4th at 1207. And there is no "clearly expressed" intent that the CLRA should apply extraterritorially. *Id.*; *Terpin v. AT&T Mobility, LLC*, 399 F. Supp. 3d 1035, 1047–48 (C.D. Cal. 2019) (CLRA does not apply extraterritorially).

Second, both claims fail because plaintiffs do "not allege that [they] read and relied on a specific misrepresentation." *Haskins v. Symantec Corp.*, 654 F. App'x 338, 339 (9th Cir. 2016); *see Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1219–20 (N.D. Cal. 2014). Actual reliance requires that plaintiffs plausibly allege that they *read* the alleged misrepresentations—which plaintiffs characterize as the "requirement that businesses have the right to collect, use, and share Plaintiffs' . . . data before providing any data to Meta." Compl. ¶ 433. Plaintiffs fail to allege they read anything, let alone "when and where they" viewed any alleged misrepresentation. *In re Zoom Video Commc'ns Inc. Priv. Litig.*, 525 F. Supp. 3d 1017, 1045–46 (N.D. Cal. 2021). That is "fatal" to their claims. *In re Google, Inc. Priv. Policy Litig.*, 58 F. Supp. 3d 968, 982 (N.D. Cal. 2014.

Third, the UCL claim fails because plaintiffs do not plausibly allege the loss of "money or property." Cal. Bus. & Prof. Code § 17204. Their conclusory statements that they "have suffered injuries in fact" are insufficient when their only factual allegation is that Meta's "sale" of "individually identifiable and health data" to unspecified entities has "diminished its value to Plaintiffs." Compl. ¶ 437; *see Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 603 (N.D. Cal. 2021) (external value of data does not establish loss of money or property); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014). And "the 'mere misappropriation of personal information' does not establish

compensable damages," either. *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613, 615 (9th Cir. 2021); *see Katz-Lacabe*, 2023 WL 2838118, at *8.

Fourth, plaintiffs' request for restitution under the UCL fails because plaintiffs allege an adequate remedy at law. They will be unable to plausibly allege otherwise through amendment because the claims are all premised on the same factual predicates. Where plaintiffs' equitable claims for past harms are based on the same factual predicates as their legal claims, they are not "true alternative theor[ies] of relief but rather [are] duplicative." *Loo v. Toyota Motor Sales, USA, Inc.*, 2019 WL 7753448, at *13 (C.D. Cal. Dec. 20, 2019) (dismissing with prejudice); *see Zapata Fonseca v. Goya Foods Inc.*, 2016 WL 4698942, at *7 (N.D. Cal. Sept. 8, 2016). Nowhere do plaintiffs explain why the damages they seek for other claims are inadequate. *See supra* at 20.

Fifth, plaintiffs' claim under the "unlawful" prong of the UCL fails because it is predicated on the same theories underlying their other claims, making the failure of those underlying theories fatal. *See* Compl. ¶ 432; *Kellman v. Spokeo, Inc.*, 599 F. Supp. 3d 877, 896 & n.5 (N.D. Cal. 2022).

Sixth, plaintiffs' claim under the "unfair" prong of the UCL fails because they do not satisfy either the "balancing" or "tethering" tests. As to the "balancing" test, plaintiffs have not identified which conduct or acts by Meta were "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers," particularly since the complaint acknowledges that Meta takes substantial steps to prevent receipt of potentially sensitive information. *See Herskowitz v. Apple Inc.*, 940 F. Supp. 2d 1131, 1145–46 (N.D. Cal. 2013). Nor do they plead *any* facts alleging that any harm outweighs the utility of Meta's conduct. *Id.*; *see supra* at 2–3 (explaining the beneficial and legitimate uses of the Pixel). Plaintiffs also fail to plausibly allege Meta engaged in a practice that "threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws . . . or otherwise significantly threatens or harms competition" under the tethering test. *Kellman*, 599 F. Supp. 3d at 896. Their allegation that Meta's conduct "impaired competition within the market," Compl. ¶ 436, is not only conclusory; it does nothing to tether their claim to a legislatively declared policy or proof of some actual or threatened impact on competition. *Kellman*, 599 F. Supp. 3d at 896.

CONCLUSION

The Court should dismiss the complaint with prejudice.

Dated: May 8, 2023

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Lauren R. Goldman*
Lauren R. Goldman

COOLEY LLP

By: */s/ Michael G. Rhodes*
Michael G. Rhodes

Attorneys for Meta Platforms, Inc. (formerly known as Facebook, Inc.)

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

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

Dated: May 8, 2023

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Lauren R. Goldman*
Lauren R. Goldman