Proposed Redacted Version of Plaintiffs' Notice of Motion and Motion for Class Certification (Dkt. No. 1154-3)

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

Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Tel: 310-854-4444
Fax: 310-854-0812

Attorneys for Plaintiffs and the Proposed Classes

[Additional counsel listed on signature page]

Geoffrey Graber, State Bar No. 211547
ggraber@cohenmilstein.com
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW, Suite 800
Washington, DC 20005
Tel: 202-408-4600
Fax: 202-408-4699

Beth E. Terrell, State Bar No. 178181
bterrell@terrellmarshall.com
TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, WA 98103
Tel.: 206-816-6603
Fax: 206-319-5450

Andre M. Mura, State Bar No. 298541
amm@classlawgroup.com
GIBBS MURA LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
Tel.: 510-350-9700
Fax: 510-350-9701

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE META PIXEL HEALTHCARE LITIGATION

This Document Relates to:

All Actions.

Case No. 3:22-cv-3580-WHO (VKD)

CLASS ACTION

PLAINTIFFS' NOTICE OF MOTION AND MOTION FOR CLASS CERTIFICATION

Date: March 4, 2026
Time: 2:00 p.m.
Place: Courtroom 2 – 17th Floor
Judge: Hon. William H. Orrick III

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Plaintiffs brought this case as a proposed class action to stop Meta from collecting their communications with their healthcare providers and compensate the Facebook users whose health information was taken without their consent. Plaintiffs seek certification of three classes that focus on the information Meta collected, and a fourth class focusing on Meta's intrusion onto their devices.

This case is tailor-made for class certification—all major questions are resolvable classwide based on common or representative evidence. What Meta intended to do (or not) is a question that does not vary by Facebook user. Whether Meta broke its contractual promises to Facebook users is answerable for all in one fell swoop based on the interpretation of form contracts. Whether Meta surreptitiously collected patients' healthcare communications without consent or legal authorization depends on the way Meta's tools and systems work and the uniform promises Meta made about what information it does (and does not) collect. And whether Plaintiffs' privacy was violated depends on whether patients' expectation that Meta would not be intercepting communications with their healthcare providers online is objectively reasonable. And, if so, whether our society should countenance what Meta did. Neither of these questions depend on what any one patient said, did, or subjectively believed. Plaintiffs respectfully ask the Court to certify the proposed classes.

BACKGROUND

Discovery has uncovered that Meta obtains health information through the Meta Pixel when patients communicate with their healthcare providers on thousands of healthcare provider domains and apps. Ex. 3 (Shafiq Rep.) ¶¶ 35-41. This is no accident. An understanding of how Meta's systems work shows that Meta knowingly obtains health information about patients and their communications throughout the United States without their consent, despite its contractual promises to the contrary. So we begin by explaining how Meta's technology uniformly and systematically works to surveil patients, before describing the promises it made to Facebook users, and finally the company's persistent practice of disclaiming responsibility for its acquisition of health data to those medical partners who sounded the alarm that Meta's ad systems are collecting health information.

A. Meta's tools collect health information.

In all the ways that matter, Meta's data collection practices are uniform across the class.

Meta collects consumer data through a suite of Business Tools: the Meta Pixel, SDK, CAPI, and custom list uploads. Its primary tool, the Pixel, is computer code provided at no cost to third-party website operators, including hospitals and clinics, to improve advertising. *See* Smith Dec., ECF 49 ¶¶ 4, 7-9, 15; Ex. 10 (describing basics of Pixel installation). When a patient visits a website that has the Pixel installed, Meta's source code instructs the website to place a tracking cookie—the _fbp cookie—on the patient's device. Shafiq Rep. ¶¶ 89-90, 94. That process is invisible to the patient. Smith Rep., ECF 49 ¶ 29. Because some browsers and programs block third-party cookies to prevent tracking and protect online privacy, Meta redesigned its systems after 2018 to disguise its cookies as first-party cookies, making them appear to the browser as if the healthcare websites had installed these cookies so they could continue to function. Shafiq Rep.¶¶ 88-94, 116; Ex. 11 (Mudd Dep.) at 99:13-102:24; Ex. 12. This gave the appearance of a direct interaction between user and site to the browser, even while Pixel data continued flowing to Meta. Shafiq Rep.¶¶ 88-94.

The data the Pixel re-directs from a patient's device to Meta's servers has two important parts. *First*, it includes information Meta uses to identify the Facebook user associated with the communication. Shafiq Rep.¶¶ 78-115. The Pixel uses identifiable information, including browser cookies, device IDs, and IP address, so Meta can connect the device sending those requests to a particular user's account. Shafiq Rep.¶¶ 78-115. For example, Meta places cookies on user devices that identify which Facebook user the device belongs to, then uses that information to associate Pixel data it receives with the Facebook user to which it belongs. Shafiq Rep.¶¶ 79-94. Even without cookies, Meta uses IP address and other data to identify the Facebook user. Shafiq ¶¶ 95-97.

Second, it includes the communication itself, such as a GET or POST request (the technical terms for a browser communication), the content of a button clicked, or the information contained in a form. *See, e.g.*, Smith Dec., ECF 49 ¶¶ 5, 97, 173; Shafiq Rep. ¶¶ 27, 32. The information Meta intercepted also includes content such as the text of a button clicked to log-in to a patient portal or request an appointment, or a full-string URL that contains health information. For example, Meta's production of classwide data showed that it intercepted—and processed—the following

communications from the www.medstarhealth.org domain associated with a class member:

- medstarhealth.org/mymedstar-patient-portal and "Log In"
- medstarhealth.org/blog/heart-palpitations-emergency-care and "Request an Appointment"
- medstarhealth.org/doctors/paul-a-sack-md
- medstarhealth.org/search#globalsearch_q=diabetes [truncated URL]
- medstarhealth.org/services/diabetes
- medstarhealth.org/services/ulcerative-colitis

Shafiq Rep.¶ 135. Compare these to communications highlighted in ECF 1, ¶ 5 and ECF 159 at 19.

B. Meta then uses the collected health data for ads and other purposes.

Meta's systems and technologies ingest, process, and monetize this health data as part of its centralized ads-targeting and other pipelines. *See generally* Hashmi Rep. Part VIII.B-G. Immediately upon receipt of Pixel data, Meta seeks to identify the Facebook user whose data it received, using an internal identity-matching system called [redacted] Ex. 13 at 14; Shafiq Rep. ¶¶ 102-15. The identity-matching system relies on cookies and other identifiers—including IP address, browser fingerprint, and advertiser-supplied hashed contact information—to match data received to user profiles. Ex. 15 (Resp. to Interrog. 12) ("Meta may use hashed information transmitted with event data via the Business Tools to match events to Meta user IDs."); Shafiq Rep. ¶ 103. Once a match is made, Meta appends the user's Facebook ID to the collected data. *Id.* This enabled Meta to identify data that its Business Tools collected from Named Plaintiffs' visits to healthcare provider websites. Shafiq Rep. ¶¶ 152-53. As one 30(b)(6) witness put it, "Meta is great at identifying its users" and "strictly focuses on connecting behavior to its users." Ex. 16 (Leach Dep.) at 59:5-60:8.

After matching the collected data to the user, Meta analyzes and categorizes the data. While technologically complex, the aim is straightforward: to mine the data in real time so that it can be used for targeted ads and other business purposes. Hashmi Rep. ¶¶ 37, 109-10; Shafiq Rep. ¶¶ 107, 109, 115. Indeed, Meta uses highly detailed health classifications for health data it collects such as "skin cancer." Hashmi Rep. ¶¶ 36, 100.[1]

The interpreted events are then recorded and converted into structured "features"—i.e., [redacted]. Hashmi Rep. ¶¶ 95-107. Within Meta, Pixel Button

[1] For a more in-depth description of these pipelines and categorizations, see Hashmi Rep. ¶¶ 90-111; Shafiq Rep. ¶¶ 48-75; and Ex. 17 (Tripathi Dep.) at 37:4-18; 98:3-100:13.

Clicks are seen as particularly revealing and valuable. Internal documents describe them as the [redacted] Ex. 19, and Meta [redacted]. Hashmi Rep. ¶ 104(c). These structured features are [redacted] where they can be used by Meta in real-time for targeted advertising. Hashmi Rep. ¶¶ 108-111; Ex. 15. Meta's newsfeed personalization systems rely on these same features to influence what non-advertising content users are shown. Ex. 11 at 86:14-92:3. The entire process—from ingestion to identity resolution, to inference and storage, and to ad delivery—is automated, lightning-quick, and uniform so it can be scaled globally.[2]

C. Internal company documents reveal that Meta intended to collect health data.

This case is replete with evidence that Meta intended to collect health data.

1. Meta knew the Pixel would send health data automatically and let it do so.

Prior to 2017, the Pixel only tracked user events that were specifically selected for tracking by the website's operator. On May 20, 2017, Meta changed the Pixel so that it would automatically collect certain events—including button click events—and send them to Meta. Exs. 20-22. Meta made this change because many advertisers were not choosing to send Meta the data most profitable to it. Ex. 22 at 2 ("Many businesses, especially SMBs lack the technical ability or resources to implement the pixel correctly, resulting in passing incorrect data, or no data at all and therefore do not obtain maximum value from their Facebook ads."). So it redesigned the Pixel—calling it [redacted] or "Automatic Events"—and began capturing user actions that advertisers had not configured the Pixel to collect. Shafiq Rep. ¶ 39. By default, the [redacted] automatically listened for user interactions such as button clicks—even for patient portal login, appointment, and payment buttons. Shafiq Rep. ¶ 39; Ex. 22 at 2 ("The Facebook pixel will send button clicks, form field labels (although not the content of submitted fields), and page metadata. The page metadata that will be collected is [redacted] like the title and description of a page.).

Meta recognized that changing the Pixel to send button click events "by default" was a

[2] There are potentially [redacted] of other tables where Meta stores and uses health information. Meta has taken the position that [redacted], and its corporate designees were unable to provide full information. *See* Ex. 15; Ex. 17 at 119:1-4 ("We did some due diligence on this [redacted] table, but we couldn't figure it out.").

problem [redacted] Ex. 23 at '795. But Meta implemented the change anyway, rolling out an option that would require advertisers to manually disable automatic events—but only if they knew Meta had added that option, understood its importance, and knew how to manually reconfigure their Pixels. Ex. 20 at '903; Ex. 21 at '169. Otherwise, the events were automatic. Unsurprisingly, this was a failure: when notifying advertisers about automatic events, Meta did not even mention how advertisers could disable them. Ex. 21; Ex. 18 (Narvaez Dep.) at 79:22-80:22.

Meta recognized internally that the [redacted] was violating users' privacy: "with [redacted] Ex. 24 at '055. Thus, Meta came up with another potential solution: Meta would [redacted] Ex. 25. But the available evidence shows that Meta did not disable automatic events for healthcare provider advertisers until after this lawsuit was filed. *See* Ex. 16 at 159:8-13.

Plaintiffs' expert Richard M. Smith explains that automatic events fired on all healthcare provider websites that he examined prior to this lawsuit being filed in June 2022—including one healthcare provider for whom source code shows Automatic Events were turned off. Ex. 1 (Smith Supp. Rep.) ¶¶ 10-13. To disable automatic events for healthcare providers, Meta would have needed to identify and enforce a block on such events from regulated entities. But Meta knew it had a problem. In 2022, as public attention mounted, a Meta employee asked, [redacted] Ex. 26. And, in January 2019, an engineer raised the concern that the [redacted]. Ex. 27 at '347-348; Ex. 28 (Reza Dep.) at 29:4-30:21; 35:24-36:12. After this case was filed, Meta failed to preserve *both* the data tables that contained the button clicks that Meta received prior to this lawsuit being filed *and* the [redacted] that contained the websites where Meta supposedly disabled automatic events prior to this lawsuit being filed. ECF 880, Hashmi Rep. ¶ 17(d)-(e); Ex. 9 at page 8.

2. Meta pushed Healthcare Providers to use its tools while disclaiming responsibility.

Meta did not tell healthcare providers that the Pixel was automatically configured to send data Meta itself considered sensitive health information. Instead, Meta's sales teams pressured providers to send patient health data to improve their advertising performance, avoided questions about ethics and compliance, pushed back against healthcare providers' well-founded concerns, and routinely pushed healthcare providers to use the Pixel to target patients. For example, Meta encouraged hospitals to use the Pixel to target advertisements based on "current patients." Ex. 29 at '31-32. Meta emphasized that hospitals should send medical appointment scheduling information to Meta. *See, e.g.*, Exs. 29-36. Meta explained that it was "important" to track these events so that the hospital could "optimize" their advertisements to target users who would be interested in scheduling specific types of medical appointments. Ex. 30; *see also* Ex. 31 at '84.

Rather than working with healthcare providers to prevent Pixels from transmitting health information, Meta adopted an internal policy of not telling healthcare providers the full truth about how the Pixel worked, and then letting healthcare providers decide on their own *both* whether the information their Pixels were tracking was health information *and* whether the advertisers were violating Meta's own policies. Meta acknowledged in 2017, "Advertisers may send sensitive data (HIPAA, VPPA, PII, etc.) through the pixel, app SDK . . . in violation of our terms or their legal obligations. Automatic Setup (aka [redacted]) [redacted] . . . [W]e've determined that the risk is assumed by the advertiser, not Facebook." Ex. 37; Ex. 38 ("[I]t's up to the client to interpret their requirements around HIPAA, PII, etc. [redacted]); Ex. 39 (Deckard Dep.) at 129:13-130:24 (admitting Meta [redacted] it's "up to them"); *id.* at 200:17-205:04 (Meta leaves it to advertisers to determine compliance with Meta policies). Meta's sales managers openly discussed that healthcare providers did not have the right to send the health information the Pixel sent to Meta. *See* Ex. 40 ("I didn't realize that what [health clients] were doing was technically not Hipaa compliant . . . using the pixel isn't either.").

When Meta sales team members raised concerns, Meta leadership reiterated the policy: the

healthcare providers would decide whether they had the right to share users' health information. In January 2021, Meta account manager Rebecca Reza asked, "Is there a way to pressure test HIPAA compliance?" Ex. 41. One week later, Meta's Business Product Marketing team provided Reza with guidance. Reza testified that, "[t]he guidance that I was provided . . . [was] it is *up to the advertiser to determine* whether the data they are sending back or how to send back data in a HIPAA compliant manner." Ex. 28 at 226:10-15 (emphasis added); *see also id.* at 134:24-135:20, 144:14-146:21, 224:2-226-5; Ex. 42 ("it's the advertisers job to determine whether the info they're tracking is compliant to hipaa or not"); Ex. 43 at '8035. Reza testified that she would "defer" to the healthcare providers' judgment if they wanted to send Meta data that indicated an individual's patient status. Ex. 28 at 207:1-24. As one health account manager put it when responding to a provider's request for more information: "We don't have any documentation on HIPAA Compliance because we, as Facebook, are not required to be HIPAA compliant." Ex. 44.

Meta also does not train its health sales team on health privacy requirements. Ex. 39 at 34:1-21. Nor does it train its advertisers about how the Pixel may send health information to Meta. Instead, Meta provides formulaic guides to health clients that describe health information in a way that is abstracted from the way the Pixel operates. *See* Ex. 45 (Health Data Best Practices); Ex. 46 (Health CAPI One-Pager); Ex. 47 at '965 (quoting these same categories to client concerned about a campaign with a button click conversion). The guides did not explain that certain events, like button clicks, may transmit patient status, much less that pixels were set up by default to send that information or even that Meta tracks the content of all communications, not just those that an advertiser has configured for conversion tracking or special treatment. It also [redacted] Even when Meta's systems detected health information, its employees did not report misuse or escalate the issue. Instead, the Pixel continued to fire, even after repeated flags. *See* Ex. 45 at '865 (explaining advertisers will just receive a notice); *e.g.*, Ex. 48 (email re multiple violations and appeals); Ex. 39 at 249:13-251:18.

Some advertisers made an independent determination that the Pixel was capturing health information and informed Meta that they wished to stop using the Pixel or limit what information was being sent. *E.g.*, Ex. 49 at '316 (noting that provider was "at-risk of violating HIPAA

compliance" by including "provider page URLs [in] … conversion data"); Ex. 47 at '968 ("due to enterprise level privacy concerns around PII and PHI tracking risk," provider wants to remove all pixels from campaign focused on tracking when users schedule an appointment). But Meta did not alert other healthcare providers, and an account manager even suggested it would not be appropriate to do so. Ex. 39 at 221:9-236:11; 252:1-256:20. Meta even encouraged healthcare providers with concerns to keep using the Pixel. *Id.* at 243:17-246:16; Ex. 49 at '316 (requesting to limit information sent by Pixel); *id*. at '294 (Meta responds by recommending use of "Pixel and CAPI at the same time"); Ex. 47 at '968 (asking to remove all pixels); *id*. at '963 ("It is our recommendation that we do not completely remove the pixel in this situation.").

As Meta stayed silent, other providers remained unaware the Pixel was sending health information. When they learned, some issued breach notifications to their patients. *E.g.*, Ex. 50 (WakeMed Letter). Once The Markup published its article, Meta belatedly contacted its clients—but still put the burden fully on the healthcare providers, telling account managers to "make sure they review what data is being sent via Meta Business Tools to ensure they are not sharing any sensitive information with us." Ex. 51. Meta did not tell advertisers that, when the Pixel is set up by default as Meta instructs, it automatically shares patient identifiers, all full-string URLs, and all button clicks that they made on the healthcare provider's website—including data that Meta internally recognized as health information through its inclusion on Meta's Filter block list.

3. Meta employees proposed solutions that senior executives rejected.

Meta could have protected privacy. But its leaders, including its CEO, chose not to.

In 2019, Meta's products team [redacted]. Management overruled them. On February 22, 2019, the Wall Street Journal ran a story about Meta Pixel's interception of health information, reporting that "at least 11 popular apps, totaling tens of millions of downloads, have . . . been sharing sensitive data entered by users" with Facebook. Ex. 52. Meta's executives took note: that same day, a Facebook employee circulated a document among high-level Meta executives on the Ads Leadership Team identifying the story and commenting, [redacted] and noting that Meta's [redacted]

[redacted] Ex. 53; Ex. 11 at 179:18-180:1.

Three potential solutions were proposed to Meta leadership. *See* Exs. 53, 54. First, Meta could [redacted] Ex. 53 at 2; Ex. 11 at 182:6-10. Second, Meta could [redacted] Ex. 53 at 2; Ex. 11 at 183:5-6. Third, Meta could create a filter to "[d]etect and drop just blacklist of terms." Ex. 53 at 2; Ex. 11 at 184:18-22. Former Meta VP Graham Mudd testified "[t]hese [were] mutually exclusive options," and the first was "the one that was recommended, and . . . the most conservative of the approaches." Ex. 11 at 189:3-4, 23-25; *see also id*. at 190:8-13 (agreeing option one was "most aggressive in eliminating data from restricted sources"). Meta chose the "filter" despite knowing it would [redacted] Ex. 53 at 2. Mr. Mudd testified that "if I could make this decision myself today, I would [redacted] and choose option one. Ex. 11 at 200:23-25.

In 2021, another important privacy decision was elevated to Mark Zuckerberg. Since 2019, Mr. Zuckerberg was obligated under a consent decree with the FTC to certify quarterly that Facebook was complying with its privacy obligations. ECF 966 at 2-3; ECF 965 at 16-17. The Ads Leadership Team told Mr. Zuckerberg that it recommended, as an important step to improve user privacy, that Meta should stop collecting users' data from third-party websites (including through the Pixel) without opt-in consent. Ex. 11 at 229:5-233:15; 241:24-242:18; 247:15-249:10; Ex. 55. Even though Facebook employees told Zuckerberg that "[o]btaining consent for [third-party data] is a worthwhile privacy improvement," the proposal was never fully implemented. Ex. 56; Ex. 11 at 248:9-252:16.[3]

In June 2022, Meta looked again. On June 16, 2022—the same day the publication *The Markup* published an article titled "Facebook Is Receiving Sensitive Medical Information from Hospital Websites"—Mr. Wooldridge suggested (1) [redacted]

[3] The Ninth Circuit has indicated oral argument on Meta's mandamus petition to block Mr. Zuckerberg's deposition about his executive decisions and knowledge may be in December 2025.

[redacted] which he said was "very low hanging fruit;" and (2) [redacted] which he called "medium hanging fruit" for which [redacted] in [redacted] Ex. 57. Mr. Wooldridge sent a memo to other engineers directing them to [redacted] in [redacted] including [redacted] Ex. 58.

By July 5, 2022, Meta was considering four options: (1) [redacted] (2) [redacted] (3) [redacted] or (4) "[redacted] Ex. 59. On July 7, 2022, a decision was announced in a chat, "Overall steer from leadership convo: [redacted] Ex. 85. In short, do nothing right away.

It wasn't until February 2023 that Meta began [redacted], and not until July 2024 did Meta begin truncating URLs that the Pixel sends to Meta on health websites (for example, www.hospital.org/cancer-treatment would be truncated to www.hospital.org). Shafiq Rep. ¶ 175. Yet, even with these changes, Meta still (i) places _fbp cookies on patient devices; (ii) uses the computing resources of patient devices; (iii) collects detailed URLs in a form that is so easy to un-hash that Plaintiffs' expert did it from publicly available data; (iv) runs and uses a [redacted] processor to interpret the remaining data for ads use. Shafiq ¶ 176. In short, Meta is still collecting health data to match to its users to serve them ads.

D. Meta's contract and public statements contradict its data practices, which violate reasonable expectations of privacy and state and federal laws, including HIPAA.

Meta doesn't tell Facebook users any of this. Instead, its Terms of Service, starting in April 2018, promise that the company "require[s]" each of its partners to have the "lawful rights to . . .

share your data before providing any data" to Meta. Ex. 61 (Apr. 2018 Data Policy). According to Meta, in 2022, it removed the word "lawful" to adopt "a more expansive requirement" that partners "have to respect industry norms or other kinds of rights. That's the clarification." Ex. 16 at 49:22-51:7. Second, Meta promises that it "employ[s] dedicated teams around the world, work[s] with external service providers, partners, and other relevant entities and develop[s] advanced technical systems to detect potential misuse of our products." Ex. 63 (July 2022 Terms of Service).

Meta also published documents and made public statements implying it did not collect health information. Meta purports to prohibit advertisers from sharing health information in its Commercial Terms. Ex. 64. It further claims in its About Prohibited Information disclosure that it does not "want or permit advertisers to use the Meta Business Tools to share . . . data that is based on or includes, directly or otherwise, health . . . or other categories of sensitive information." Ex. 65.

Recall that instead of preventing advertisers from sending health information—option #1 that the product team recommended—Meta went with the filter, which allows it to receive health information and decide what to do with it behind closed doors. Meta publicly promised that:

> If Meta's signals filtering mechanism detects Business Tools data that it categorizes as potentially sensitive health-related data, the filtering mechanism is designed to prevent that data from being ingested into our ads ranking and optimization systems.

Ex. 81; Ex. 86. It then listed examples, including diseases, conditions, injuries, sexual and reproductive health, mental health, medical procedures/treatments/testing, prescription medications, and information to identify a place of treatment or counseling. But Meta's filter was [redacted]. First, the filter [redacted]. Hashmi Rep. ¶¶ 15-16, 76-77, 81, 93-94; *see also* Ex. 66 (Wooldridge Dep. I) at 198:14-15. Instead, the filter was only [redacted] Ex. 67 (Anand Dep.) at 91:8-18. The filter also included a specific exception that [redacted]. Hashmi Rep. ¶¶ 76-77, 81, 85, 87 ([redacted] from Filter treatment); Ex. 68 [redacted] Dr. Shafiq analyzed the classwide data produced by Meta to demonstrate that, despite Meta's opposition to Plaintiffs' initial motion for

preliminary injunction, the filter [redacted] referenced in the Court's order. *See* ECF 76-1 at 2 (Wooldridge Decl.); ECF 159 at 19 n.10 (PI Order); Shafiq Rep. ¶¶ 166-69. Thus, Meta's Filter promises were false.

Shortly after this lawsuit was filed, Meta launched a public-relations campaign assuring the public that advertisers could not target them based on health topics. In September 2022, Senator Jon Ossoff asked Meta's Chief Product Officer, Chris Cox, "whether or not Meta is collecting, has collected, has access to, or is storing, medical or health data for U.S. persons." Ex. 69 at '983. Meta's CPO responded, "Not to my knowledge." *Id*. In October 2022, Meta filed a declaration in this case describing its "filtering mechanism" as a tool what will "screen out potentially sensitive data it detects"—failing to mention that the filter was not designed to block the majority of data in this case. ECF 77-4 ¶ 8. In December 2022, Meta repeated this claim to Senator Mark Warner. Ex. 14. And in the spring of 2023, it said the same things to its FTC auditor, claiming that if the filter "detects that a domain classified as health-related . . . [is sending] data to Meta that matches a list of . . . health-related terms on the 'Block List,' Meta will filter that term or associated values from the dataset." Ex. 70. It provided the New York Attorney General with the same information in February 2023. Ex.71. And just last month, Mr. Wooldridge repeated this in sworn testimony in a jury trial before Judge Donato. Jury Trial Tr., *Frasco v. Flo Health*, No. 3:21-cv-00757 (N.D. Cal. Aug 4, 2025), ECF Nos. 747-753 at 998:1-12, 999:23-1000:13. But all of these claims were false. The filter [redacted]

As this Court preliminarily found, Meta's Pixel is collecting "protected health information under HIPAA." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 791 (N.D. Cal. 2022). Healthcare providers violated HIPAA by sending Meta protected health information without valid HIPAA authorizations. 42 U.S.C. § 1320d-6; *see also* Ex. 4 (Cohen Rep.) ¶¶ 141, 126–27. Meta further violated HIPAA by receiving and using protected health information without signing Business Associate Agreements with the healthcare providers. *See* Ex. 39 at 47:2-19; Ex. 44 ("I've confirmed [redacted] *see also* Cohen Rep. ¶¶ 129-31, 141; *Business Associate Contracts*, U.S. Dept. of Health and Human Services (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-

associate-agreement-provisions/index.html.

LEGAL STANDARD

"[T]he ultimate goal of Rule 23 is to determine whether efficiency and justice are best served by plaintiffs pursuing their claims on behalf of a class." *Fitzhenry-Russell v. Dr. Pepper Snapple Grp., Inc.*, 326 F.R.D. 592, 607 (N.D. Cal. 2018). A "proposed class action must satisfy all four elements of Rule 23(a), and at least one of the sub-sections of Rule 23(b)." *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. 535, 541 (N.D. Cal. 2018). Merits questions should be considered "only to the extent that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Amgen Inc. v. Conn. Ret. Plans & Trust Funds*, 568 U.S. 455, 466 (2013) (cleaned up). A court has broad discretion in deciding whether to grant or deny class certification. *Weston v. DocuSign, Inc.*, 348 F.R.D. 354, 362 (N.D. Cal. 2024) (Orrick, J.).

CLASS DEFINITIONS[4]

Plaintiffs seek to certify four classes for a Class Period of June 17, 2018 to the present.

1. ***The Patient Status Button-Click Class*** – All Facebook users who had at least one patient portal, medical appointment, bill payment, or diagnostic assessment button click[5] obtained by Meta from Class Healthcare Providers.

2. ***The Patient Health Information Class*** – All Facebook users who had at least one communication or fact identifying a doctor, condition, or treatment acquired by Meta from Class Healthcare Providers, excluding Button-Click events described above.

3. ***The Prescription Drug Information Class*** – All Facebook users whose communications with a prescription drug website for which they have a prescription, were obtained by Meta.

4. ***The Patient Device Intrusion Class*** – All Facebook users for whom Meta placed an _fbp cookie and/or used computing resources by sending data to Meta through their device and/or by computing Core Setup logic on their device while at a Healthcare Provider property.

The Class Healthcare Providers listed in Exhibit 72 and Exhibit 60 apply to both the Patient Status Button Click and Patient Health Information classes. The at-issue prescription drug domains

[4] These proposed class definitions are, together, narrower than (if not coextensive with) the class definition in the operative complaint, ECF 335 ¶ 353, and thus the Court can consider certifying them without requiring an amendment to the complaint. *Abdeljalil v. General Elec. Capital Corp.*, 306 F.R.D. 303, 306 (S.D. Cal. 2015).

[5] A "patient portal, medical appointment, bill payment, or diagnostic assessment button click" is a button click on or navigating to a patient portal login, logout, or signup; scheduling or checking-in for an appointment for a doctor/provider; bill payment, bill lookup, or signing up for bill payment; and accessing/completing a health risk assessment/quiz. Shafiq Rep. ¶ 137-53.

are listed in Exhibit 73. The entities in the Patient Status Button Click and Health Information classes are healthcare providers covered by HIPAA. And the entities in the Prescription Drug class are all prescription drug companies, which are covered by the CMIA. The types of entities at issue are all HIPAA or CMIA covered entities, and the Collection Tools at-issue are limited to the Meta Pixel, SDK, CAPI, and Custom Uploads. Jane Doe I, Jane Doe IV, Jane Doe V, Jane Doe IX, Jane Doe X, John Doe II, and John Doe III seek to represent the Patient Status Button-Click Class; Jane Doe I, Jane Doe IV, Jane Doe V, Jane Doe X, John Doe II, and John Doe III seek to represent the Health Information Class; Jane Doe IV seeks to represent the Prescription Drug Information Class, and all named plaintiffs seek to represent the Device Intrusion Class.

The specific communications at-issue in the Patient Status Button Click and Health Information classes can be objectively identified. Shafiq Rep. ¶¶ 81-91. Plaintiffs' expert Dr. Shafiq demonstrated a methodology to identify Patient Status Button Clicks in Meta's data and applied his methodology to the data produced by Meta. *Id.* ¶¶ 126-53. For the Patient Health Information class, Meta had an internal classification system called [redacted] that identified at-issue communications in health categories at "the heart of this case" until it was deprecated and spoliated in the middle of this case. The Prescription Drug Information class includes all communications at those properties because all identified properties contain the name of the prescription drug in the domain itself. And the Patient Device Intrusion class applies to all patients who exchanged a communication with their healthcare provider regardless of the specific content of the communication because the alleged common actionable conduct is Meta's unauthorized placement of the _fbp cookie and use of their computing device. Class Members can be identified through Meta's records and class member declarations. *See Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1126 (9th Cir. 2017).

With respect to the Patient Status Button Click Class, the class includes all healthcare providers that had the Pixel or CAPI on their website. This is appropriate because, as discussed above, the available evidence shows that Meta did not disable button clicks being automatically sent to Meta by healthcare provider advertisers with the Pixel until after this lawsuit was filed. *See supra* at 5. Further, any argument by Meta that these automatic configurations may have been changed by

the healthcare providers should be foreclosed because Meta spoliated any such evidence. As this Court already found, Meta "knew or consciously disregarded that there was key data" in two tables [redacted] and [redacted] "that contained data showing the healthcare provider websites that used Meta's Pixel and where individuals clicked on website buttons on those sites." ECF 880. At this stage, an appropriate remedy would be to foreclose Meta from arguing that there were healthcare providers that had installed the Pixel or CAPI, and yet somehow were not transmitting button click data to Meta. *Id.; see also* ECF 1120 at 2:5-11 (confirming no remediation for this loss of data).

All classes seek certification of the breach of contract, implied covenant of good faith and fair dealing, intrusion upon seclusion, and Comprehensive Computer Data Access and Fraud Act ("CDAFA") claim. The Patient Status Button Click, Patient Health Information, and Prescription Drug Classes also seek certification of their claims under the federal Electronic Communications Privacy Act (ECPA) and the California Invasion of Privacy Act (CIPA).

California law applies nationwide for each proposed class because Meta's Terms expressly select California law. Ex. 63 ("[T]he laws of the State of California will govern these Terms and any claim, cause of action, or dispute without regard to conflict of law provisions"). Under California's choice-of-law rules, which govern this diversity action, *Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1187 (9th Cir. 2001), courts ask whether the claims fall within the scope of that agreement and whether California has a substantial relationship with the parties. *Wash. Mutual Bank, FA v. Superior Ct.*, 24 Cal. 4th 906, 916 (2001). This case easily satisfies both requirements. *First*, courts construe Meta's choice-of-law clause broadly. *Cabrera v. Google LLC*, 2023 WL 5279463, at *36 (N.D. Cal. Aug. 15, 2023) ("[T]he specific choice-of-law used here ('governed by California law') is an especially 'broad one signifying a relationship of absolute direction, control, and restraint.'" (quoting *Nedlloyd Lines B.V. v. Sup. Ct. of San Mateo County*, 3 Cal. 4th 459 at 469 (1992)). In the Ninth Circuit, courts regularly construe choice-of-law provisions like this one as selecting California law for any claim that "does not have limitations on its geographical scope . . . even if parts of the contract are performed outside of the state." *Gravquick A/S v. Trimble Navigation Int'l Ltd.*, 323 F.3d 1219, 1223 (9th Cir. 2003); *see also Cabrera*, 2023 WL 5279463, at *36

(Google's clause applied California UCL nationwide).

Here, all class members are Facebook users, and every Facebook user is legally deemed to have agreed to the Terms of Service, Privacy Policy, and Cookie Policy via a checkbox on the sign-up page. As the Court previously noted, "Meta's policies do not . . . specifically indicate that Meta may acquire *health data* from Facebook users' interactions with their *medical providers' websites*." ECF 159 at 15 (emphasis in original). By their express terms, these documents "make up the entire agreement between [each user] and Meta" and govern the relationship between Meta, *see* Ex. 63 (Terms), including the information Meta will collect, what Meta can access on user devices, and under what conditions—the precise conduct that gave rise to Plaintiffs' contract, common law, and statutory claims.

California also has a "substantial relationship to the parties or their transaction," *Wash. Mut. Bank*, 24 Cal. 4th at 916, because Meta is headquartered in California. *See Nedlloyd*, 3 Cal. 4th at 467 ("substantial relationship present when 'one of the parties is domiciled' in the chosen state" (internal quotations omitted)); *see also Forcellati v. Hylands, Inc.*, 2014 WL 1410264, at *2 (C.D. Cal. Apr. 9, 2014) ("Given that [the defendant is] headquartered in California, . . . application of California law poses no constitutional concerns in this case."). Accordingly, the Court can apply California law nationwide absent a showing from Meta that foreign law should apply due to "*conflicts* in *fundamental* policy." *Maldonado v. Apple, Inc.*, 2021 WL 1947512 at *8 (N.D. Cal. May 14, 2021) (Orrick, J.) (emphasis in original).

ARGUMENT

A. This case meets Rule 23(a)'s requirements.

1. Each proposed class is sufficiently numerous.

Each class has millions of members. *See* Shafiq Rep. ¶¶ 137-53. That is more than enough.

2. Legal and factual issues are common to the classes.

Rule 23(a)(2)'s requirement that there be "questions of law or fact common to the class" is also satisfied here. This requirement is met if "even a single common question" exists, *Alcantar v. Hobart Service*, 800 F.3d 1047, 1052 (9th Cir. 2015), so long as "determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke," *Wal-Mart*

Stores, Inc. v. Dukes, 564 U.S. 338, 350 (2011); *see also Castillo v. Bank of America, NA*, 980 F.3d 723, 728 (9th Cir. 2020). As will be discussed in more detail in the section addressing Rule 23(b)(3)'s predominance requirement, which "supersed[es]" commonality, *Amchem Products Inc. v. Windsor*, 521 U.S. 591, 609 (1997), the most important questions in this case are all common: Did Meta knowingly or intentionally intercept communications from healthcare providers websites? Did Meta's leadership reject protective measures? Do Meta's Terms "require" advertising partners to have the "right" to share information? Does Meta use advanced tools to detect and deter misuse? Were class members' communications with their providers "confidential"? Is it objectively reasonable for class members to expect that Meta would not intercept their health information communications at healthcare provider websites? These questions and more are answerable based on classwide proof, including Meta's uniform Terms of Service and data-collection and ad-business practices.

3. The named Plaintiffs' claims are typical of the class.

Under Rule 23(a)(3)'s "permissive standards," typicality is met because the named plaintiffs' claims "are reasonably co-extensive with those of absent class members." *Castillo*, 980 F.3d at 729 (citation omitted). Plaintiffs are typical because "other members have the same or similar injury," "the action is based on conduct which is not unique to the named plaintiffs," and "other class members have been injured by the same course of conduct." *James v. Ubert Techs., Inc.*, 338 F.R.D. 123, 132 (N.D. Cal. 2021). And none are "subject to unique defenses which threaten to become the focus of the litigation." *Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992). Here, the named plaintiffs—and all class members—were injured by Meta using its Business Tools to intercept plaintiffs' health information without plaintiffs' consent when plaintiffs were communicating with their healthcare providers. *See* Doe I Decl. ¶¶ 2-4; Doe II Decl. ¶¶ 2-6; Doe III Decl. ¶¶ 2-3; Doe IV Decl. ¶¶ 2-3; Doe V Decl. ¶¶ 2-3; Doe IX Decl. ¶¶ 2-3; Doe X ¶¶2-3 Decl.; Exs. 74-80 (Plaintiffs' Interrogatory Responses); Shafiq Rep. ¶¶ 152-153. Critically, Meta's means of interception and the agreements plaintiffs formed with Meta are the same classwide.

4. The named Plaintiffs and counsel are adequate representatives.

Plaintiffs and class counsel "will fairly and adequately protect the interests of the class."

Fed. R. Civ. P. 23(a)(4). Neither has conflicts of interest with the proposed class, and both have and will continue to vigorously prosecute this action. *In re Hyundai & Kia Fuel Econ. Litig.*, 926 F.3d 539, 556 (9th Cir. 2019) (en banc); *see* Doe I Decl. ¶¶ 9-12; Doe II Decl. ¶¶ 11-14; Doe III Decl. ¶¶ 8-11; Doe IV Decl. ¶¶ 8-11; Doe V Decl. ¶¶ 8-11; Doe IX Decl. ¶¶ 8-11; Doe X Decl. ¶¶ 8-11; Barnes Decl. ¶¶ 5, 13; Graber Decl. ¶¶ 5-6; Koncius Decl. ¶¶ 7,10; Mura Decl. ¶¶ 5-6; Terrell Decl. ¶¶ 5-6. The Named Plaintiffs have proven adequacy by investing many hours in the case, responding to Meta's extensive and intrusive discovery, permitting forensic imaging of their devices, collecting documents, and testifying in depositions. They will continue to safeguard the interests of class members going forward. Likewise, proposed Class Counsel have extensive experience litigating privacy cases and will continue to pursue the case vigorously. *See* Barnes Decl. ¶¶ 8-11, 13; Graber Decl. ¶¶ 4, 6; Koncius Decl. ¶ 8, 10; Mura Decl. ¶¶ 4, 6; Terrell Decl. ¶¶ 3, 6.

B. This case meets Rule 23(b)(3)'s requirements.

1. Common questions predominate over any individual issues.

The Court can certify a damages class where "the common, aggregation-enabling, issues in the case are more prevalent or important than the non-common, aggregation-defeating, individual issues." *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 664 (9th Cir. 2022) (quoting *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016)). The Court may certify a class "even if just one common question predominates." *In re Hyundai*, 926 F.3d at 557. Predominance, in short, "is not a counting game." *In re JUUL Labs, Inc., Mktg. Sales Pracs. and Prods. Liab. Litig.*, 609 F. Supp. 3d 942, 967 (N.D. Cal. 2022). "'Rather, more important questions apt to drive the resolution of the litigation' carry greater weight than less significant individualized questions." *Id*. (citation omitted). Plaintiffs meet this standard for each claim.

ECPA. The ECPA makes it unlawful for any person to "intentionally intercept[] . . . any . . . electronic communication." 18 U.S.C. § 2511(1)(a). "Intercept" means to acquire the "contents" of an electronic communication through use of a "device," *id.* at § 2510(4), and "contents" means "any information concerning the substance, purport, or meaning of" the communication. *Id.* § 2510(8). The ECPA provides an affirmative defense if "one of the parties to the communication has given prior consent," but this defense does not apply if 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." *Id*. at § 2511(2)(d). Common questions predominate for each class.

Determining Meta's intent will focus entirely upon Meta's knowledge, conduct, and systems. *E.g.*, *supra* Background Sec. C.3 (discussing Meta's awareness that it was receiving data it shouldn't and rejection of more protective measures). Plaintiffs will show Meta "acted consciously and deliberately with the goal of intercepting … communications." *See United States v. Christensen*, 828 F.3d 763, 775 (9th Cir. 2015). Intent focuses on Meta's conduct and will be proven with evidence common to the classes. *See Allen v. Conagra Foods, Inc.*, 331 F.R.D. 641, 662 (N.D. Cal. 2019) (Orrick, J.) ("[I]ntent . . . can be shown on a representative basis.").

Whether Meta acquired "contents" through a "device" will be resolved with common evidence of how Meta's source code worked and, where available, records of the interceptions. This Court previously reasoned that both "the log-in buttons and the kinds of descriptive URLs [at-issue] are 'contents' within the meaning of the [ECPA]," and that "plaintiffs' Internet communications on their healthcare providers' websites appear to fall squarely within the statutory definitions" of "electronic communication" and "device." ECF 159 at 19; ECF 316 at 5-6, 10. Discovery has confirmed and expanded upon the early evidence. Dr. Shafiq explains how he and Meta identified Patient Status Button Click and Health Information from the data Meta produced, which includes Button Click text, full-string URLs, and "microdata" that Meta intercepted and analyzed in the middle of the communication. *See* Shafiq Rep. ¶¶ 126-57. To the extent Meta argues certain transmissions do not include "contents," that question will be uniformly decided within each respective class because the type of information conveyed within each class is uniform.

Common questions will also predominate over Meta's affirmative consent defense. Consent "can be express or implied, but any consent must be actual"—"to be actual, the disclosures must 'explicitly notify' users of the conduct at issue." *Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024). The factfinder must view the disclosures through the view of a "reasonable user" with "the level of sophistication attributable to the general public," not someone with "the skill of an experienced business lawyer" or a "technical expert." *Id.* at 1149, 1151. This is an objective measure that the Court can resolve for each class with one answer. And consent to some tracking is

not enough to sanction tracking of everything—the Court must also consider whether Meta "exceed[ed] the scope of that consent," which again will be resolvable classwide for each class. *Id*.

As discussed above, whether Plaintiffs consented to this tracking is an objective question that will not be outweighed by any individual-specific facts. *See Johnson v. CoreCivic*, 2018 WL 7918162, at *10 (W.D. Mo. Sept. 18, 2018) (certifying ECPA claim because whether defendant's disclosures established consent "applies to the class as a whole"); *Raffin v. Medicredit, Inc*., 2017 WL 131745, at *9 (C.D. Cal. Jan. 3, 2017) (certifying parallel CIPA claim, "because every putative class member was subject to [defendant's] policy on a uniform basis, determining consent [] can be accomplished without resort to individualized proof"). To determine whether class members consented, the Court will look to Meta's uniform contract promises and disclosures, the pre-existing reasonable expectations of privacy that patients enjoy with their healthcare providers, and Meta's public assurances that it would filter even "potentially sensitive health information." *See* ECF 159 at 12-17 (previewing the consent analysis and finding it unlikely that class members consented); *see generally* Ex. 5 (Vohs Rep.) (patient privacy expectations); Ex. 6 (Barasz Rep.) (general consumer privacy expectations); Cohen Rep. ¶¶ 135-36 (website privacy policies cannot authorize healthcare providers to send HIPAA protected health information to third parties); 45 C.F.R. § 164.508.

And to decide whether healthcare providers consented to share this information with Meta, the Court will also look to common evidence, including: what Meta uniformly told healthcare providers in its binding contracts and statements about the purported filter compared to what Meta actually did with the data that it intercepted. *See* ECF 76-1 at 3 (explaining the documents Meta makes available to advertisers). Again, Meta must show not only that healthcare providers were subject to a form contract when using the pixel, but that they "*actually* consented" to share this information with Meta and that Meta did not exceed the scope of any alleged consent. *See* ECF 316 at 7-8 (emphasis in original). Here, Meta will not be able to do so for any healthcare provider because it did not disclose to any healthcare provider how the Business Tools may send sensitive health information to Meta. It also failed to disclose that it uses that data to make health information inferences about their patients—data that Meta uses for its own purposes, including to help *other* advertisers. These are facts that Meta has fought to keep secret in this case. *See* Hashmi Rep. at

Part VIII.F (describing how ingested data is interpreted into [redacted] for broad use).

Even if Meta could show any healthcare provider *actually* consented, Meta's interceptions were for a common "purpose of committing [a] criminal or tortious act[.]" This exception-to-the-exception will rise or fall on common evidence in this case because it is satisfied where, as here, a defendant intercepts data for use in pre-existing user profiles or to commit a further invasion of privacy. *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) (user profiles); *Planned Parenthood v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016) (further invasion). It is met even if a defendant has other motives (such as a profit motive) for its actions. *Riganian v. LiveRamp*, 2025 WL 2021802, at *8-9 (N.D. Cal. July 18, 2025). In addition to these tortious purposes, common evidence will show that, despite its lack of proper authorization, Meta chose to keep taking that data for use in advertising, which violates HIPAA. *See* 42 U.S.C. 1320d-6. Ultimately, whether Meta's purpose was tortious or criminal is resolvable classwide because Meta's purpose and conduct was uniform.

CIPA. As with the federal statute, common questions predominate for Plaintiffs' § 631 and § 632 CIPA claims. Inasmuch as CIPA tracks the ECPA, its elements are provable classwide for the reasons discussed above. *Supra* at 18-21. CIPA, unlike its federal counterpart, requires all parties to consent. *See Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *2 (9th Cir. 2022). Under § 631, Plaintiffs must show that Meta (1) "willfully" and (2) "without the consent of all parties to the communication, or in any unauthorized manner;" (3) "reads, or attempts to read, or to learn the contents or meaning of any . . . communication;" (4) "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" Cal. Pen. Code § 631(a). Under § 632, Plaintiffs may show a violation by proving that Meta, (1) "intentionally" and (2) "without the consent of all parties" (2) "to a confidential communication," (3) used a "recording device to . . . record the confidential communication." Cal. Pen. Code § 632.

Whether Meta acquired class member communications while "in transit . . . while passing over any wire, line, or cable, or being sent or received . . . from" California will be determined by common evidence. *See Romero v. Securus Techs., Inc.*, 331 F.R.D. 391, 411 (S.D. Cal. 2018) (certifying CIPA claim and noting that "how" defendant recorded calls in California was subject to

common proof). With respect to timing, there is no variation among class members. The source code allowing Meta to acquire communications instantaneously works the same for everyone. For the location question, it is sufficient that Meta "is headquartered in California" and "manages" its ad delivery program from this state. *In re Google RTB Consumer Priv. Litig.*, 2024 WL 2242690, at *10 (N.D. Cal. Apr. 4, 2024) (rejecting "the novel proposition that plaintiffs must demonstrate the precise processor from where [the defendant] allegedly intercepted the contents of plaintiffs communications to meet [their] class certification burden"). Moreover, there is undisputed classwide evidence that Meta adopted California law by choice, its employees (including executives) who made the key decisions are in California, and all intercepted data is available to employees in California.[6] Ex. 63; Ex. 11 at 229:5-233:15; 241:24-242:18; 247:15-249:10 (key decision made by Mark Zuckerberg, who is based in California).

Meta collected "confidential communications" under § 632 if "a party to the conversation [had] an *objectively reasonable* expectation that the conversation is not being overheard or recorded." *In re Google Ass't Priv. Litig.*, 457 F. Supp. 3d 797, 828 (N.D. Cal. 2020) (emphasis added) (quoting *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 117 n.7 (2006)). This element is objective and therefore can be determined classwide for each class, taking into account the circumstances of the types of communications Meta intercepted. This Court preliminarily found plaintiffs will "likely to be able to show that the communications at issue here were confidential under CIPA" because "patient status and medical-related communications between patients and their medical providers are protected by federal law," and "health-related communications with a medical provider are almost uniquely personal." ECF 159 at 23-24. Nothing is different at this stage.

Breach of Contract. Plaintiffs will need to show (1) "the existence of the contract," (2) "plaintiff's performance or excuse" (3) Meta's "breach," and (4) "the resulting damages to the plaintiff." *Oasis W. Realty, LLC v. Goldman*, 51 Cal. 4th 811, 821 (2011). "Courts routinely certify class actions regarding breaches of form contracts." *Ellsworth v. U.S. Bank, N.A.*, 2014 WL

[6] If the Court declines to certify § 631(a) nationwide, it should still certify subclasses of patients who either communicated from California or exchanged a communication with a California-based healthcare provider. Meta's records can identify these individuals. Shafiq Rep. ¶¶ 186-89.

2734953, at *20 (N.D. Cal. June 13, 2014); *see also, e.g.*, *Williams v. Apple, Inc.*, 338 F.R.D. 629, 638 (N.D. Cal. 2021); *Frasco v. Flo Health, Inc.*, 349 F.R.D. 557, 586 (N.D. Cal. 2025) (certifying contract claim for sharing health information with Meta). So too here: All elements will be proven through common evidence. With respect to the existence of the contract, all class members entered into a common form contract with Meta, which includes the Terms of Service, Data Policy, and Privacy Policy, and performed by providing information when signing up to be Facebook users. Ex 63 (TOS); Ex. 61 (Data Policy), ECF 443 (Answer) ¶¶ 369, 376.

Next, Meta's breach will be determined classwide for each class and proven with common evidence. The contract provisions at issue have been substantially the same since April 19, 2018. First, Meta promises that it "require[s]" its advertising partners "to have lawful rights" or "the right to . . . share your data before providing any data to us." Ex. 61 at '861.[7] Whether Meta breached this promise turns on the interpretation of the word "require" and whether Meta's conduct—uniform to the class members—complied with its Terms. *See* ECF 159 at 16; ECF 316 at 17-18. Common evidence will show that Meta did not *require* healthcare advertisers to have the right or lawful right to share health data with Meta. Instead, "the Pixel captures information that connects a particular user to a particular healthcare provider—i.e., patient status—which falls within the ambit of information protected under HIPAA." ECF 159 at 15. Meta's 30(b)(6) witness on the topic identified the actions that Meta claims to have done to comply with that promise—and all are common. Ex. 16 at 131:19-133:1; *see also* Ex. 45 (Health Data Best Practices guide, explaining advertisers receive a notice if they send health information, but nothing more); Ex. 48 (email with Supernus rep re multiple violations and appeals); Ex. 39 at 249:13-251:18.

Here, common evidence will determine whether Meta's uniform conduct breached the contract. Plaintiffs will submit expert testimony that healthcare provider use of the Pixel violated medical ethics and legal duties. Cohen Rep. ¶¶ 93-150. It also violated common law privacy and

[7] From April 2018 until July 2022, Meta promised that it "required each of its partners to have lawful rights" to share users' data. Ex. 61. On July 26, 2022, it published a new Privacy Policy that removed the word "lawful." Ex. 62. Meta's corporate designee testified that this was a clarification of the existing contract (not a change to the contract) meaning that partners "have to respect industry norms or other kinds of rights." Ex. 16 at 49:22-51:7.

property protections and computer crime laws, like the CDAFA. Worse, the information was, in fact, HIPAA-protected, which would require an authorization to share that information and restrictions on its uses. *Id*. At ¶¶ 94, 118-41. But Meta never required healthcare providers to obtain HIPAA-compliant authorization from users, nor did Meta ever sign a Business Associate Agreement with healthcare providers. Ex. 47 [redacted] Ex. 44 ("I've confirmed that [redacted] Plaintiffs will present common evidence that Meta encouraged healthcare providers to collect health data it knew it did not have the rights to collect. *See supra* at 6-8.

Meta also breached its contractual promise because healthcare providers did not have the right to send Meta the at-issue health data under industry norms. Cohen Rep. ¶¶ 93-150; Ex. 16 at 47:12-24 (Q: "[Is it] Meta's belief that users have written Meta a blank check to collect information from advertisers?" A: "No. Advertisers are required to comply with the laws in their jurisdiction, even the norms . . . of their industry . . .. So in no way, shape, or form does this indicate any sort of a blank check.").

Similarly, common evidence will show Meta breached a second provision of the contract: Meta's promise to use "advanced technical systems to detect misuse" or "potential misuse" of Meta's products, and its promise that it "will" or "may" "take appropriate action" against those who misuse its products, including "blocking" or "removing or restricting access to certain features." Ex. 82 at '877; Ex. 83 at '934. Again, Meta's 30(b)(6) deponent on this issue identified a discrete set of acts that Meta claims to have complied with this promise—and all are common. Ex. 16 at 133:2-135:15. Plaintiffs will use Meta's admissions, expert testimony, and documentary evidence (including classwide sampled data) to demonstrate that Meta breached this promise because its filter was designed so that it had no impact on the vast majority of data in this case. *See* Hashmi ¶¶ 76-77, 81, 85, 87; Shafiq ¶¶ 158-69; Ex. 84 (Wooldridge 30(b)(6) Dep.) at 141:15-142:16; Ex. 202 (document acknowledging [redacted] Similarly, there is common evidence that Meta took no action when it was alerted *by health advertisers* that their use of the Pixel was inappropriate, and instead encouraged advertisers not to stop using the Pixel. *See supra*

Background Sec. C.2. Any attempt Meta makes to cite the filter will be common because it worked the same for all class members—and rejected as a matter of law because the filter did not work.

Plaintiffs will present several common measures of damages, including nominal and benefit-of-the-bargain damages, as well as a request for specific performance going forward unless Meta changes the contract. Finally, even if valid, Meta's limits on liability clause does not preclude the direct (actual) damages sought by Plaintiffs. *Lewis Jorge Constr. Mgmt., Inc. v. Pomona Unified Sch. Dist.*, 34 Cal. 4th 960, 968 (2004).[8]

Good Faith and Fair Dealing. If Meta "frustrates [its users'] rights to the benefits of the contract," *Love v. Fire Ins. Exch.*, 221 Cal. App. 3d 1136, 1153 (Ct. App. 1990), by engaging in "objectively unreasonable conduct," "eva[ding] the spirit of the bargain[,]" or "abus[ing] a power to specify terms," it will also be liable to class members. *Carma Devs. (Cal.), Inc. v. Marathon Dev. Cal., Inc.*, 2 Cal. 4th 342, 373 (1992); *R.J. Kuhl Corp. v. Sullivan*, 13 Cal. App. 4th 1589, 1602 (1993). Here, Plaintiffs will present common evidence that Meta did all three: (1) Meta claims its promise to "require" partners to have the right to share information was satisfied by putting language in its form Commercial Terms, but took no action to ensure that advertisers were actually complying; (2) Meta's sales team actively encouraged healthcare providers to violate their responsibilities under Meta's Terms and federal law; (3) Meta designed its filter in a way that effectively did not block any health information—while claiming the opposite publicly and to this Court; and (4) Meta knowingly used health information it claimed publicly and throughout this case violated its terms of use. For the same reasons as the breach claim, Meta's actions toward its users were uniform and can be evaluated on a classwide basis.

Intrusion Upon Seclusion. Plaintiffs will show that Meta "intrude[d] into a place, conversation, or matter as to which [plaintiffs have] a reasonable expectation of privacy . . . in a manner highly offensive to a reasonable person." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (cleaned up; citation omitted). These elements are subject to common proof. Whether class members had a "reasonable expectation of privacy" in their communications

[8] Any argument by Meta that the contract limits liability is also resolvable classwide.

is common to each class. It is an objective question. *Frasco*, 349 F.R.D. at 582 (certifying nationwide intrusion claim under California law); *Opperman v. Path, Inc.*, 2016 WL 3844326, at *11 (N.D. Cal. July 15, 2016) (plaintiffs not required to prove "subjective expectation"). The expectation need not be one of "*absolute* or *complete* privacy." *Sanders v. ABC*, 20 Cal. 4th 907, 915 (1999); *Hill v. Nat'l Collegiate Athletic Ass'n.*, 7 Cal. 4th 1, 36 (1994).

Common facts, including Meta's own public representations, contractual promises, and legal protections for the intercepted communications, will show class members had a reasonable expectation of privacy in their computing devices, their communications with healthcare providers, and reading about their own prescriptions. While each class involves different contextual circumstances from which an expectation of privacy may be measured, each is uniform within that class. For the Patient Device Intrusion class, the common question is whether a patient class member has a reasonable expectation that, when they are at their own healthcare provider's property, they would not be subjected to placement of the _fbp tracking cookie. Whatever Meta may argue on the merits, it cannot deny that the question yields a common answer. The same is true for the Prescription Drug Information Class: whether Plaintiffs' expectations are reasonable that they would not be tracked on those websites is objective and common to the class.

For the Patient Status Button Click and Health Information Classes, the Court has already opined that it is objectively reasonable for Plaintiffs to expect that "communications with their medical providers were confidential," *see* ECF 159 at 24, and Plaintiffs' expert concluded the same. *See* Vohs Rep. ¶¶ 15-29. Meta may again argue the merits, but this too is answerable classwide. These expectations are grounded in community-wide facts and norms about privacy in medical treatment and protections under HIPAA. ECF 159 at 24. Plaintiffs will also argue that it is objectively reasonable for individuals with a valid prescription, reading up on the drugs they've been prescribed, to expect that information will not be tracked—and whether that is true or not will be the same for all class members. Finally, Meta's own Terms say Meta *requires* advertisers to have the right to share their information with Meta before they send it and promises that Meta will work to remedy any misuse of its products. Ex. 82 at '877; Ex. 83 at '934. Certification is appropriate where an expectation of privacy arises from a defendant's common promises. *E.g.*, *Rodriguez v.*

Google LLC, 2024 WL 38302, at *5 (N.D. Cal. Jan. 3, 2024); *Frasco*, 349 F.R.D. at 580-84.

The "highly offensive" element is also an objective standard that asks whether "the intrusion is unacceptable as a matter of public policy." *Facebook Tracking*, 956 F.3d at 606; *Opperman*, 2016 WL 3844326, at *11 (describing the inquiry as "essentially a policy determination" that "may require an examination of [defendant's] motives, but [ ] will not require individualized determinations of class members' subjective expectation. "[Courts] must examine whether the data itself is sensitive *and* the manner it was collected . . . violates social norms." *Facebook Tracking*, 956 F.3d at 603 (emphasis in original). Whether Meta acted "egregiously" will involve considering its "policies forbid[ding] the transmission of health-related information" and "criminal and civil statutes forbidding the disclosure of protected health information without proper authorization"—factual information common to all class members. ECF 159 at 26-27. This necessarily includes Meta's choice to design its filter as underinclusive, despite proponents of a much more conservative model to respond to privacy concerns. *See supra* Background Sec. C.3. Ultimately, whether it was highly offensive for Meta to take patients' health data to build secret profiles to improve advertising is answerable classwide.

CDAFA. The classes also seek to certify their claims under two sections of the CDAFA. This statute proscribes knowingly (1) "access[ing] and without permission . . . us[ing] any data [or] computer . . . to wrongfully control or obtain money, property, or data" or (2) "introduc[ing] any computer contaminant into any computer[.]" Cal. Pen. Code § 502(c)(1), (8). CDAFA "sets no threshold" for damages: "any amount of damage or loss may be sufficient." *Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750, at *4 (N.D. Cal. July 20, 2010); *see also* ECF 417 at 5. Common questions predominate for both Plaintiffs' (c)(1) and (c)(8) claims.

Start with § 502(c)(1). The Pixel source code shows that Meta accessed and used class members' devices to (1) set _fbp cookies on class member devices that were disguised as belonging to their healthcare providers, even though they belonged to Meta; and (2) directed the devices to send information to Meta while class members were exchanging communications with their healthcare providers. *See* Shafiq Rep. ¶¶ 177-80. Internal documents point out that this was expressly [redacted]. Shafiq Rep. ¶ 114. As explained above,

Plaintiffs' consent (or lack thereof) to this practice will be resolvable on a classwide basis because Meta's setting of the _fbp cookie and commandeering of patient devices occurs in an identical manner for all class members.

Next, § 502(c)(8) is met because common proof will determine if the Pixel is a computer contaminant that Meta "introduced" to Plaintiffs' devices. Shafiq Rep. ¶¶ 181–85. The Pixel's functionality is the same across the class, and so were Meta's actions to introduce the _fbp cookie on class devices. *Id*.

Finally, "damage or loss" is measurable classwide. Plaintiffs' expert explains that the space the _fbp cookie occupies on a device is measurable, as is the load-time delay. *See* Shafiq Rep. ¶¶ 181-85. Meta itself recognizes computational expense. *See* Ex. 84 (Wooldridge Dep. II) at 83:14-84:23 ("computational resources" to crawl web-pages "would be expensive"); 149:4-11 ("stateful filtering" more "computationally expensive" than "stateless filtering").

Monetary relief. Damages can be reasonably determined on a classwide basis for each of Plaintiffs' claims. *Lytle v. Nutramax Labs, Inc*., 114 F.4th 1011, 1027 (9th Cir. 2024) (requiring only that damages "stemmed from the defendant's actions that create[d] the legal liability") (citing *Comcast Corp. v. Behrend*, 569 U.S. 27 (2013)). "[A]ll the plaintiffs must do at the class certification stage is propose a damages methodology that will be able to reliably calculate damages in a manner common to the class at trial." *Weston v. DocuSign, Inc.*, 348 F.R.D. 354, 369 (N.D. Cal. 2024) (Orrick, J.). As discussed below, Plaintiffs have done so.

Statutory Damages. The Patient Status Button Click, Health Information, and Prescription Drug Classes seek statutory damages under ECPA and CIPA for each class member. *See* 18 U.S.C. § 2520(c)(2) (permitting a baseline recovery of $10,000); Cal. Pen. Code § 632.7 (prescribing $5,000 per violation). That damages may be large is no reason to deny certification. *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1276-77 (9th Cir. 2019).

Actual Damages. The Patient Status Button Click, Health Information, and Prescription Drug Classes have two methods to measure actual or compensatory damages for their ECPA, CIPA, contract, breach of the implied covenant of good faith and fair dealing, and intrusion upon seclusion claims: (i) a survey-based valuation approach, and (ii) a market-value approach. Each measures loss

as a result of Meta's wrongful data collection. Put simply, Meta took more data than Plaintiffs agreed to share for access to Facebook. For the survey-based valuation, Plaintiffs' expert Hal Singer measured how Facebook users value the confidentiality of certain health-related communications online. *See generally* Ex. 7 (Singer Rep.) Parts II-IV. Dr. Singer determined Meta would have to pay each class member a certain amount per month to have access to the type of data it took for each of the three information classes: $5.89/month to Patient Status Button Click Class members, $3.83/month to Patient Health Information Class members, and $3.77/month to Prescription Drug Information Class members. *Id.* at ¶ 9.

For market value, Plaintiffs' expert Health Capital Consultants analyzed what tech companies pay *willing* market participants for their data. HCC concluded that the fair market value of browsing information is between $8.25 to $9.87 per person, per month. *See* Ex. 8 (HCC Rep.) at 23.

Disgorgement. The Patient Status Button Click, Health Information, and Prescription Drug Classes also seek, in the alternative, disgorgement of Meta's profits attributable to its unlawful collection practices. Disgorgement is an available remedy for damages from Meta's breach of contract, breach of the implied covenant of good faith and fair dealing, violations of the ECPA, CIPA, intrusion upon seclusion, and CDAFA claims. *See* 18 U.S.C. § 2520(2)(A) (permitting recovery of "the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation"); *In re Google Ass't*, 546 F. Supp. 3d 945, 967 (N.D. Cal. 2021) (disgorgement is a remedy for contract); *Rodriguez*, 2024 WL 38302, at *6 (certifying nationwide CDAFA class with disgorgement damages theory). "In calculating damages . . . California law requires only that some reasonable basis of computation of damages be used, and the damages may be computed even if the result reached is an approximation." *Pulaski & Middleman, LLC v. Google, Inc.*, 802 F.3d 979, 989 (9th Cir. 2015) (citation and internal quotations omitted). Here, Plaintiffs' damages expert has developed a model to calculate evidence of the amount of unearned revenues and profits that Meta obtained as a result of its misconduct. *See* HCC Rep. at 11-22.

Nominal and Punitive Damages. The Patient Status Button Click, Health Information, Prescription Drug Class, and Patient Device Intrusion Classes also seek nominal and punitive

damages, which are amenable to classwide resolution. *Rodriguez*, 2024 WL 38302, at *7.

2. A class action is superior to other means of adjudication.

Class proceedings here are doubtless "superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). The technological complexity of this case, and the "relatively high costs" and resources needed to pursue it, all show that this case will proceed as a class action—or not at all. *See Frasco*, 349 F.R.D. at 587. Certifying this case as a class action therefore allows the Court to "achieve economies of time, effort, and expense, and promote . . . uniformity of decision as to persons similarly situated, without sacrificing procedural fairness or bringing about other undesirable results." *Amchem*, 521 U.S. at 615.

C. Certification is also appropriate under Rule 23(b)(2).

The Court can also certify Plaintiffs' claims under Rule 23(b)(2) because Meta "has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). The "key to the (b)(2) class is 'the indivisible nature of the injunctive or declaratory remedy warranted—the notion that the conduct is such that it can be enjoined or declared unlawful only as to all of the class members or as to none of them." *Dukes*, 564 U.S. at 360. Certification under (b)(2) is appropriate where "class members seek uniform relief from a practice applicable to all of them." *Ward v. United Airlines, Inc.*, 2021 WL 534364, at *7 (N.D. Cal. Feb. 12, 2021).

Plaintiffs' injunctive and declaratory relief claims are perfectly suited for Rule 23(b)(2) certification. The Court would "provide relief to each member of the class[es]," *Dukes*, 564 U.S. at 360, by enjoining Meta from collecting and using Health Information communications on Healthcare Provider web-properties, using patient computing device storage and resources on healthcare provider websites (including through _fbp tracking cookies), and requiring it to make certain disclosures, including about its data collection and advertising practices.

CONCLUSION

For the foregoing reasons, the Court should grant Plaintiffs' Motion.

DATED: September 9, 2025

Respectfully submitted,

By: */s/ Jay Barnes*

SIMMONS HANLY CONROY LLP
Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel: 212-784-6400
Fax: 212-213-5949

By: */s/ Geoffrey Graber*

COHEN MILSTEIN SELLERS & TOLL PLLC
Geoffrey Graber, State Bar No. 211547
ggraber@cohenmilstein.com
Jenna Waldman (State Bar No. 341491)
jwaldman@cohenmilstein.com
1100 New York Avenue NW, Suite 800
Washington, DC 20005
Tel: 202-408-4600
Fax: 202-408-4699

Eric Kafka (*pro hac vice*)
ekafka@cohenmilstein.com
88 Pine Street, 14th Floor,
New York, NY 10005
Telephone: (212) 838-7797

GIBBS MURA LLP
Andre M. Mura, State Bar No. 298541
amm@classlawgroup.com
Hanne Jensen, State Bar No. 336045
hj@classlawgroup.com
1111 Broadway, Suite 2100
Oakland, CA 94607
Tel.: 510-350-9700
Fax: 510-350-9701

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Tel: 310-854-4444

Fax: 310-854-0812

TERRELL MARSHALL LAW GROUP PLLC
Beth E. Terrell, State Bar No. 178181
bterrell@terrellmarshall.com
936 North 34th Street, Suite 300
Seattle, WA 98103
Tel.: 206-816-6603
Fax: 206-319-5450

Attorneys for Plaintiffs and the Proposed Classes

SIGNATURE ATTESTATION

The CM/ECF user filing this paper attests that concurrence in its filing has been obtained from its other signatories.

/s/Geoffrey Graber