Jason "Jay" Barnes, *Admitted Pro Hac Vice*
Email: jaybarnes@simmonsfirm.com
SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, New York 10016
Telephone: (212) 784-6400

Jeffrey A. Koncius, CSB #189803
Email: koncius@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, California 90211-2910
Telephone: (310) 854-4444

Beth E. Terrell, CSB #178181
Email: bterrell@terrellmarshall.com
TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 816-6603

Geoffrey Graber, CSB #211547
Email: ggraber@cohenmilstein.com
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW, Fifth Floor
Washington, DC 20005
Telephone: (202) 408-4600

Andre M. Mura, CSB #298541
Email: amm@classlawgroup.com
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
Telephone: (510) 350-9700

Attorneys for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE META PIXEL HEALTHCARE LITIGATION,	Case No. 3:22-cv-3580-WHO-VKD
	CLASS ACTION
This Document Relates To:	**CONSOLIDATED CLASS ACTION COMPLAINT**
All Actions	**DEMAND FOR JURY TRIAL**
	Honorable William H. Orrick

1

TABLE OF CONTENTS

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CONSOLIDATED CLASS ACTION COMPLAINT

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

CONSOLIDATED CLASS ACTION COMPLAINT

I.   NATURE OF THE ACTION

1.   Plaintiffs bring this action on behalf of themselves and millions of other Americans whose medical privacy has been violated by Meta's tracking tools, including the Meta Pixel. The Meta Pixel allows Meta to intercept individually identifiable health information from Meta health care "Partner" websites and monetize the collected information for its own financial gain.

2.   Meta operates the world's largest social media company. Meta's revenue is derived almost entirely from selling targeted advertising.

3.   Meta's "Health" division is dedicated to marketing to and servicing Meta's health care "Partners." Meta defines its "Partners" to include "businesses" that use Meta's products, including the Meta Pixel or Meta Audience Network tools "to advertise, market, or support their products and services."

4.   Meta has worked with hundreds of Meta health care Partners to deploy the Meta Pixel and other Meta products to learn about visitors to their websites and use that information for targeted advertising based on patients' online behavior. Meta's health care Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

5.   Plaintiffs are Facebook users who allege that Meta acquires their confidential health information from their healthcare providers and covered entities in violation of federal and state laws and despite Meta's promises that it: (1) only collects and uses their data if Meta's Partners have obtained the "right" or "lawful right" to share their data with Meta; and (2) "employ[s] dedicated teams around the world, work[s] with … partners … and develop[s] advanced technical systems to detect potential misuse of [Meta's] products," which would include the Meta Pixel.

6.   When a patient uses their healthcare provider or covered entities' website or application where the Meta Pixel is present, the Pixel transmits the content of their communications to Meta, including, but not limited to (1) signing-up for a patient portal; (2) signing-in or -out of a patient portal; (3) taking actions inside a patient portal; (4) making, scheduling, or participating in appointments; (5) exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; (6) conduct a

CONSOLIDATED CLASS ACTION COMPLAINT

search on the Meta health partner website; and (7) other information that qualifies as "personal health information" under federal and state laws.

7.   In many circumstances, Meta also obtains information from its health care Partners' that identify a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools that Meta encourages its health care Partners to use to upload customer lists to Meta for use in its advertising systems. In the case of Meta's health care Partners, a customer list is a patient list.

8.   The information transmitted from a health care Partner's website or application to Meta always includes information sufficient to uniquely identify a patient under federal law (such as IP address information and device identifiers that Meta associates with a patient's Meta account), and may also include a patient's demographic information, email address, phone number, computer ID address, or contact information entered as emergency contacts or for advanced care planning, along with information like appointment type and date, a selected physician, button and menu selections, the content of buttons clicked and typed into text boxes, and information about the substance, purport, and meaning of patient requests for information from their providers and other "covered entities" under federal and state health privacy laws.

9.   The transmission is instantaneous—Meta often receives the information before the health care provider or covered entity does.

10.   The transmission is invisible.

11.   The transmission is made without any affirmative action taken by the patient.

12.   The transmission occurs without any notice to the patient that it is occurring.

13.   Meta collects the transmitted identifiable health information and uses "cookies" to match it to Facebook users, allowing its health care Partners and others to target advertisements both on and off Facebook. For example, Meta can target ads to a person who has used a patient portal and exchanged communications about a specific condition, such as cancer.

14.   Meta says its health care Partners are required to have the right to share patients' data before transmitting it to Meta. But Meta knows its Pixel tracking tool is being used on health care provider and covered entity websites and is contemporaneously transmitting patients'

CONSOLIDATED CLASS ACTION COMPLAINT

1 individually identifiable health information to Meta without patients' consent. Meta's "Health"

2 division targets its services directly to health care providers and pharmaceutical companies. Meta

3 is aware of every advertiser that it engages with through its Health division. Meta is also able to

4 identify health care providers, pharmaceutical companies, and other covered entities that are using

5 the Pixel without consent through its web-crawler and the deployment of common industry tools

6 (called "verticals") that categorize the content and types of businesses on which tech tools appear.

7   15.   It is against the law for Meta to disclose or obtain individually identifiable health

8 information without giving appropriate notice to the patient and obtaining their consent.

9   16.   The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

10 protects sensitive patient health information, including patient status, from being obtained or

11 disclosed without the patient's knowledge and consent – and directly applies to companies that

12 obtain individually identifiable health information without authorization. *See* 42 U.S.C. § 1320d-

13 6.

14   17.   In addition to the protections afforded patients by federal law, Meta's Terms of

15 Service, as explained below, include a California choice of law provision for all of its users.

16 California has enacted several laws prohibiting the disclosure of patient information without

17 consent, including the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56

18 *et seq.*, and the California Consumer Privacy Protection Act, Cal. Civ. Code § 1798.100 *et seq.*

19   18.   The United States Department of Health and Human Services ("HHS") recently

20 confirmed that HIPAA and its regulations prohibit the transmittal of individually identifiable

21 health information by tracking technology like the Meta Pixel without the patient's authorization

22 and other protections like a business associate agreement with the recipient of patient data.

23   19.   Meta's Terms of Service, Data Policy, and Cookies Policy do not inform Facebook

24 users that Meta may acquire their health information when they interact with health care providers

25 or covered entity websites, or obtain consent to do so.

26   20.   Meta health Partners include hundreds of health care providers and other "covered

27 entities" under federal and state health privacy laws. As used herein, "covered entity" refers to any

28 person or business entity for which Plaintiffs and Class members have a reasonable expectation of

CONSOLIDATED CLASS ACTION COMPLAINT

1 privacy that the "covered entity" will not share patient health information with third parties such

2 as Meta for any non-healthcare related purpose, including marketing. This expectation is based on,

3 among other things: ancient and modern common law and ethical rules relating to the privacy of

4 health-related communications; and federal and state laws that expressly apply standards of

5 privacy to health information related to these covered entities. Under HIPAA, a "covered entity"

6 includes health care providers (which includes doctors, clinics, psychologists, dentists,

7 chiropractors, nursing homes, hospitals, and pharmacies), health plans, and health care

8 clearinghouses. 45 C.F.R. § 160.103. In addition, confidentiality rules also apply to "business

9 associates" that "creates, receives, maintains, or transmits protected health information for a

10 function or activity regulated by" HIPAA "on behalf of" a covered entity. 45 C.F.R. § 160.103.

11 Under the California Confidentiality of Medical Information Act, rules of confidentiality apply to

12 "medical information" created, maintained, preserved, stored, abandoned, destroyed, or disposed

13 of by "[e]very provider of health care, health care service plan, pharmaceutical company, or

14 contractor." Cal. Civ. Code § 56.101.

15   21.   To avoid including a lengthy list of such entities or from having to refer to "covered

16 entities or business associates/contractors" throughout the Complaint, Plaintiffs refer to these

17 entities collectively as "covered entities" throughout. Thus, as used below, "covered entities"

18 includes health care providers, health insurers, health care clearinghouses, patient portal providers,

19 pharmacies, pharmaceutical companies, and any other entity, business associate, or contractor for

20 which patient health or medical information is protected by HIPAA or the CMIA.

21   22.   Meta's interception, dissemination, and use of individually identifiable health

22 information not only violates federal and state law but also harms patients by intruding upon their

23 privacy; erodes the confidential nature of the provider-patient relationship; and takes patients'

24 property and property rights without compensation and ignores their right to control the

25 dissemination of their health information to third parties. In addition, Meta has been unjustly

26 enriched by its misconduct, obtaining unearned revenues derived from its unauthorized taking of

27 patient information.

28 / / /

23.   Plaintiffs exchanged numerous communications with their healthcare providers and covered entities. Plaintiffs' communications included logging in and out of patient portals, exchanging communications about doctor sand conditions, and using click-to-call functionality from their providers' websites. Without Plaintiffs' knowledge and consent, Meta intercepted the content of those communications. Plaintiffs bring this lawsuit on behalf of themselves and other Facebook users in the United States who were also subject to Meta's unlawful practices.

II.   PARTIES

24.   Plaintiff John Doe I is a Maryland resident, Facebook user, and a patient of MedStar Health, Inc. who used MedStar's website, including the myMedStar patient portal, currently located at https://www.medstarhealth.org/mymedstar-patient-portal, to view medical records, medications, and lab results, pay bills, and communicate with his health care provider, including using the "click to call" functionality. He used the myMedStar patient portal while the Meta Pixel was present on the portal login page.

25.   Plaintiff Jane Doe I is a Wisconsin resident, Facebook user, and a patient of Rush University System for Health who used Rush's website, including the MyChart patient portal, currently located at https://mychart.rush.edu, to view medical records and lab results, schedule appointments, search for doctors, and communicate with her health care provider. She used the Rush MyChart patient portal while the Meta Pixel was present on the portal login page.

26.   Plaintiff John Doe II is a North Carolina resident, Facebook user, and a patient of WakeMed Health & Hospitals who used WakeMed's website, including the MyChart patient portal, currently located at https://mychart.wakemed.org, to view medical records, lab results, and communicate with his health care provider, including using the "click to call" functionality. He used the WakeMed MyChart patient portal while the Meta Pixel was present on the portal login page.

27.   Plaintiff Jane Doe II is an Ohio resident, Facebook user, and a patient of the Ohio State University Wexner Medical Center who used OSU's website, including the MyChart patient portal, currently located at https://wexnermedical.osu.edu/features/mychart, to view medical records, lab results, and communicate with her health care provider, including using the "click to

1   call" functionality. She used the OSU MyChart patient portal while the Meta Pixel was present on

2   the portal login page.

3   28.   Plaintiff Jane Doe III is a Missouri resident, Facebook user, and a patient of North

4   Kansas City Hospital who used North Kansas City's wesite, including the myhealth patient portal,

5   currently located at https://myhealthnkch.iqhealth.com to view medical records and lab results,

6   and communicate with her health care provider, including using the "click to call" functionality.

7   She used these patient portals while the Meta Pixel was present on the portal login pages.

8   29.   Defendant Meta Platforms, Inc. is a publicly traded Delaware corporation,

9   headquartered in Menlo Park, California, that does business throughout the United States and the

10   world, deriving substantial revenue from interstate commerce.

11   **III.   JURISDICTION AND VENUE**

12   30.   This Court has personal jurisdiction over Meta because Meta has sufficient

13   minimum contacts with this District in that it operates and markets its services throughout the

14   country and in this District. Meta is also headquartered in this District.

15   31.   This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this

16   action arises under 18 U.S.C. § 2510, *et seq.* (the Electronic Communications Privacy Act). This

17   Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d) (the Class Action Fairness

18   Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a

19   member of the Class is a citizen of a different State than Meta.

20   32.   This Court has supplemental jurisdiction over the state law claims under 28 U.S.C.

21   § 1367 because the state law claims form part of the same case or controversy under Article III of

22   the United States Constitution.

23   33.   Venue is proper in this District because a substantial part of the events or omissions

24   giving rise to the claim occurred in this District and because Meta's Terms of Service governing

25   its relationship with its users and Partners adopts California law and chooses the Northern District

26   of California as the venue for disputes.

27   / / /

28   / / /

CONSOLIDATED CLASS ACTION COMPLAINT

IV.   **FACTUAL ALLEGATIONS**

A.   **Meta's Pixel tracking tool redirects patients' data from health care provider and covered entity websites to use for ad targeting.**

34.   Meta maintains profiles of its Facebook users that include the users' real names, locations, email addresses, friends, "likes," and communications.

35.   Meta associates this information with personal identifiers, including IP addresses, cookies, and device identifiers.

36.   Meta also tracks non-users across the web through its widespread Internet marketing products and source code, including the Meta Pixel.

37.   Meta's revenue is derived almost entirely from selling targeted advertising, which includes but is not limited to targeted advertising to Meta properties and to all Internet users on non-Meta sites and apps. .

38.   Meta's Business division provides advertising services and tools to web developers, including the Meta Pixel. Meta's Business division and its advertising services and tools are focused on trade and commerce.

39.   The Meta Pixel is a free and publicly available "piece of code" that third-party web developers can install on their website to "measure, optimize and build audiences for … ad campaigns."[1]

40.   Meta describes the Pixel as "a snippet of Javascript code" that "relies on Facebook cookies, which enable [Facebook] to match … website visitors to their respective Facebook User accounts."[2]

41.   Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[3]

[1] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.
[2] Meta for Developers, Meta Pixel (2023), https://developers.facebook.com/docs/meta-pixel/.
[3] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.

42.   Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

         a.   "Measure cross-device conversions" and "understand how your cross-device ads help influence conversion.";

         b.   "Optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action."; and

         c.   "Create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[4]

43.   Meta explains that the Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:[5]

Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

44.   The Meta Pixel is customizable. Web developers can choose the actions the Pixel will track and measure.

---

[4] *Id.*

[5] Meta Business Help Center, About Meta Pixel (2023), https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

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

CONSOLIDATED CLASS ACTION COMPLAINT

45.   Meta advises web developers to place the Pixel early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website:[6]

Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing `<head>` tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your `<head>` tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

46.   Meta also provides advertisers with step-by-step instructions for setting up and installing the Meta Pixel on their website, so that companies can add the Meta Pixel to their website without a developer.[7]

47.   If a health care provider or covered entity installs the Meta Pixel code as Meta recommends, patients' actions on the provider or entity's website are contemporaneously redirected to Meta. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with her health care provider. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the health care provider or covered entity receives it.

48.   Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing."[8]

---

[6] Meta For Developers, Get Started (2023), https://developers.facebook.com/docs/meta-pixel/get-started.

[7] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.

[8] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything*, USA Today (March 4, 2020 4:52 am), https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/.

49.   For example, when a patient clicks a button to schedule a doctor's appointment on a health care provider or covered entity's public scheduling page where the Meta Pixel is present, the Pixel sends Meta sensitive information about the patient, including the text of the button the patient clicked, the doctor's name with whom the patient scheduled an appointment with, and search terms the patient used to find the doctor, such as "home abortion."[9]

50.   The Pixel literally consists of a 1x1 pixel that is set on a user's computing device and screen by Meta's source code.

51.   By design, the Pixel is invisible.

52.   Meta acquires the content of the communication while the patient is exchanging the communication with their health care provider or other covered entity.

B.   Meta uses identifiers to match the health information it collects with Facebook users.

53.   Meta uses cookies to identify patients, including cookies named c_user, datr, fr, and _fbp.

54.   The c_user cookie identifies Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Meta uses the c_user cookie to record user activities and communications.

55.   An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse, (3) selecting 'View page source,' (4) executing a control-f function for "UserID," and (5) copying the number value that appears after "UserID" in the page source code of the Facebook user's page.

56.   Following these directions, it is easy to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing www.facebook.com/4 into a browser and hitting enter, the browser will be re-directed to Mr. Zuckerberg's page at www.facebook.com/zuck.

---

[9] Anson Chan, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022 6:00 am), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

1   57.   The Meta datr cookie identifies the web browser the patient is using. It is an

2   identifier that is unique to the patient's specific web browser and is therefore another way that

3   Meta can identify Facebook users.

4   58.   Meta keeps a record of every datr cookie identifier associated with each of its users,

5   and a Facebook user can obtain a redacted list of all datr cookies associated with his or her

6   Facebook account from Meta by using the Facebook Download Your Information tool.

7   59.   The Meta fr cookie is an encrypted combination of the c_user and datr cookies.[10]

8   60.   The c_user, datar, and fr cookies are traditional third-party cookies. That is, they

9   are cookies associated with a party other than the entity with which a person is communicating at

10   the time. In the example of a health care provider, they are third-party cookies because Meta is a

11   third-party to the communication between a patient and their health care provider.

12   61.   The Meta _fbp cookie is a Facebook identifier that is set by Facebook source code

13   and associated with the health care provider using the Meta Pixel.

14   62.   Upon information and belief, the letters fbp are an acronym for Facebook Pixel.

15   63.   The _fbp (or Facebook Pixel) cookie is also a third-party cookie in that it is also

16   cookie associated with Meta that is used by Meta to associate information about a person and their

17   communications with non-Meta entities while the person is on a non-Meta website or app.

18   64.   Meta disguises the _fbp cookie as a first-party cookie even though it is Meta's

19   cookie on non-Meta websites.

20   65.   By disguising the _fbp cookie as a first-party cookie for a health care provider

21   rather than a third-party cookie associated with Facebook, Meta ensures that the _fbp cookie is

22   placed on the computing device of patients who seek to access the patient portal.

23   66.   Most and perhaps all health care providers with a patient portal require patients to

24   have enabled first-party cookies to gain access to their patient records through the portal.

25   67.   The purpose of these portal-associated first-party cookies is security.

26

27   [10] *See* Gunes Acar, et al., Facebook Tracking Through Social Plug-ins: Technical Report
Prepared for the Belgian Privacy Commission (Mar. 27, 2015),
28   https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

68.   The _fbp cookie is then used as a unique identifier for that patient by Meta.

69.   If a patient takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted – even though it is a Meta cookie – again, because Meta has disguised it as a first-party cookie.

70.   Meta also uses IP address and user-agent information to match the health information it collects from Meta health care Partners with Facebook users.

C.   Meta also encourages health care Partners to upload patient lists for ad targeting.

71.   Meta offers an ad targeting option called "Custom Audiences." When a patient takes an action on a Meta health care Partner's website embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta matches to its users. A web developer can then create a "Custom Audience" based on Events to target ads to those patients. The Pixel can then be used to measure the effectiveness of an advertising campaign. Dkt. 76-1 (Wooldridge Declaration) ¶ 4.

> 4.   Specifically, when someone takes an action a developer chooses to track on their website (like subscribing to email updates), the Meta Pixel is triggered and sends Meta certain data, called an "Event." Meta attempts to match the Events it receives to Meta users (Meta cannot match non-Meta users). The developer can then create "Custom Audiences" based on Events and can target ads on Facebook, Instagram, and publishers within Meta's Audience Network to Meta users who have taken certain actions on their own website. Meta can also provide the developer with de-identified, aggregated reporting that helps the developer better understand the impact of its ads by measuring what happens when people see them. The identity of matched Meta users is never revealed to the developer or to any advertiser.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

72.   Meta also allows Meta health care Partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[11]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information – called "identifiers" – you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

73.   Meta provides detailed instructions for health care Partners to send their patients' individually identifiable information to Meta through the customer list upload. For example:[12]

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

74.   The Meta health care Partner can then use the Custom Audiences derived from its patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

///

---

[11] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=246909753376494.
[12] Meta Business Help Center, *Create a Customer List Custom Audience* (2023), https://www.facebook.com/business/help/170456843145568?id=246909753376494.

D.   **Meta acquires a broad spectrum of identifiable health information from health care providers' use of the Meta Pixel.**

75.   The information Meta acquires from its health care Partners' use of the Meta Pixel includes, but is not limited to, the following:

a.   When a patient clicks to register for a provider's patient portal;

b.   Information that a patient types into registration forms;

c.   When a patient clicks to log in to the patient portal;

d.   When a patient clicks to log out of the patient portal;

e.   When a patient sets up or schedules an appointment;

f.   Information that a patient types into an appointment form;

g.   When a patient clicks a button to call the provider from a mobile device directly from the provider's website;

h.   The communications a patient exchanges through her health care provider's website, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including whether they are made while a patient is still logged in to a patient portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged in or out of the patient portal; and

i.   The same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

76.   Meta's conduct constitutes an egregious breach of social norms.

/ / /

/ / /

/ / /

/ / /

/ / /

77.   Public polling shows that, "[n]inety-seven percent of Americans believe that doctors, hospitals, labs and health technology systems should not be allowed to share or sell their sensitive health information without consent." [13]

78.   In response to the Court's question during a hearing in this matter about how a Facebook user can "prevent disclosure of that information to Meta," Meta stated a patient would need "to pick up the phone" to call "their doctor" or "[t]heir hospital" and that "[t]here are many, many people out there who don't have computers and don't use these portals as their sole means of communication with their doctors." Nov. 9, 2022 Hearing Transcript at 5:15-17 (question from Court); 9:10-22 (Meta response). But if a patient clicked on the telephone number on a health care provider's webpage with a Meta Pixel to make that call via a smart phone, that patient's individually identifiable health information, including patient status, would still be redirected to Meta.

79.   <u>Plaintiff John Doe I</u> is a patient of MedStar Health in Baltimore, Maryland. When he used the "myMedStar" patient portal to review his lab results, make medical appointments, and communicate with his health care providers, the Meta Pixel on MedStar's website redirected his identity and the fact that he clicked to log in to the patient portal to Meta. The Meta Pixel redirected the following information about John Doe I to Meta:

        a.   He was communicating with MedStar via its www.MedStarHealth.org website;

        b.   He engaged in an 'ev' or event called a SubscribedButtonClick;

        c.   The content of the button he clicked was "Login to myMedstar;"

        d.   The page on which he clicked the button was Patient Portal, or "Home;"

        e.   He had previously visited a MedStar page about breast health;

        f.   His Internet Protocol address;

---

[13] *Poll: Huge majorities wants control over health info,* Healthcare Finance (Nov. 10, 2020), https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info.

CONSOLIDATED CLASS ACTION COMPLAINT

1 g. Identifiers that Facebook uses to identify him and his device, including the

2 c-user, datr, fr, and fbp cookies; and

3 h. Browser attribute information sufficient to fingerprint his device.

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

80. In other words, the Meta Pixel transmitted to Meta—even before MedStar received it—John Doe I's identity, his log in to the patient portal, the contents of the webpage he was visiting before he logged in, and the contents of the webpage he accessed upon logging in. John Doe I did not know that the Meta Pixel on the MedStar webpage redirected this information to Meta when he used the MedStar website and the myMedStar portal. And, of course, John Doe I certainly never consented to such sharing.

81. Plaintiff Jane Doe I. Plaintiff Jane Doe I is a patient of Rush University System for Health. The Meta Pixel on Rush's webpage also transmitted, without her knowledge or consent, similar identifiable health information about Jane Doe I to Meta when she clicked to log in to the Rush MyChart patient portal:

a. She was communicating with Rush via its mychart.rush.edu webpage:

b. She engaged in an 'ev' or event called a SubscribedButtonClick;

c. The content of the button the she clicked was "MyChart;"

1   d.   The page from which the button she clicked was Patient Portal, the

2   "Patients & Visitors" page;

3   e.   She had previously visited a Rush page about medical records;

4   f.   Her Internet Protocol address;

5   g.   Identifiers that Facebook uses to identify her and her device, including

6   cookies named c-user, datr, fr, and fbp (*i.e.* Facebook Pixel); and

7   h.   Browser attribute information sufficient to fingerprint her device.

Name	Value
id	▮▮▮▮
ev	SubscribedButtonClick
dl	https://www.rush.edu/patients-visitors
rl	https://www.rush.edu/patients-visitors/medical-records
if	false
ts	▮▮▮▮
cd[buttonFeatures]	{"classList":"icon-mychart external","destination":"https://mychart.rush.edu/?_ga=▮▮▮▮
cd[buttonText]	MyChart
cd[formFeatures]	[]
cd[pageFeatures]	{"title":"Patients & Visitors | Rush System"}
cd[parameters]	[]
sw	1920
sh	1080
v	2.9.64
r	stable
ec	2
o	30
fbp	fb.▮▮▮▮
it	▮▮▮▮
coo	false
es	automatic
tm	3
exp	p1
rqm	GET

23   82.   Substantially similar transmissions were sent to Meta when Plaintiffs John Doe II

24   (WakeMed), Jane Doe II (OSU), and Jane Doe III (North Kansas City) used their health care

25   providers' websites, including when they logged into their providers' patient portals. No Plaintiff

26   had any knowledge of those transmissions or consented to them.

27   83.   Plaintiffs all expected that their communications with their health care providers

28   were confidential and private. Plaintiffs' expectations of privacy were reasonable.

84.   Plaintiffs' expert, Richard Smith, provides additional details about how Meta uses the Pixel and its other tracking tools to collect Plaintiffs' and other patients' individually identifiable health information in his declaration attached to this Complaint as Appendix A.

85.   Plaintiffs' detailed investigation is supported by an article published by The Markup in June 2022, which found that 33 of the top 100 hospitals in the country were sending health information to Meta via the Pixel, including appointment scheduling.[14]

E.   Meta falsely promises Facebook users that it requires its health care Partners to have the right to share their data.

86.   Every Facebook user is legally deemed to have agreed to the Terms of Service, Data Policy/Privacy Policy, and Cookie Policy via a checkbox on the sign-up page. The Terms of Service, Data Policy/Privacy Policy, and Cookie Policy are binding on Meta and its users.[15]

87.   The Meta contract documents contain general statements that, in exchange for the use of Meta's services, Meta will generally collect information about Facebook users.

88.   Meta does not charge users any money to use its services, but Meta is not "free."

89.   Rather than charge money, Meta makes users pay for its services with their personal data, i.e. a "data license."

90.   Meta has told this Court that "Facebook is free … *because we gather this data* and we use it for ads." Nov. 9, 2022 Hearing Transcript at 20:20-21.

91.   The Court has already explained, based on evidence submitted by Meta in opposition to Plaintiffs' Motion for Preliminary Injunction, that "[t]o provide [its] services, Meta's terms explain, Meta 'collect[s] and use[s] your personal data." Dkt. 159 at 6 (citing Dkt. 76-3 (Terms of Service) at 4).

/ / /

/ / /

/ / /

---

[14] Anson Chan, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022 6:00 am), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[15] *See* Dkt. 76-3 (Terms of Service), 76-4 (Data Policy), 76-5 (Cookies Policy).

CONSOLIDATED CLASS ACTION COMPLAINT

92.   Meta's contract states, "We collect and use your personal data in order to provide the services described above to you." It then informs users, "You can learn how we collect and use your data in our Data Policy."[16]

93.   Although the Meta Data Policy makes general broad disclosures about the data it collects, the "data license" Meta charges users in place of money is not unlimited.

94.   For example, by signing up for Meta, a Facebook user has not agreed to exchange with Meta the right for Meta to obtain their bank account information or Social Security number.

95.   Like any other contract, by signing up for Meta, the "data license" that Meta charges is limited by the terms of the written contract between Meta and users.

96.   The Meta Privacy Policy establishes a minimum amount of information that a person must provide directly to Meta to use Meta's products.

What if you don't let us collect certain information?

Some information is required for our Products to work. Other information is optional, but without it, the quality of your experience might be affected.

Learn more >

97.   When a Facebook user clicks the "Learn more" hyperlink, Meta explains that when it says "[s]ome information is *required* for our Products to work" (emphasis added), it means that service will not be permitted unless the requirement is met:

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

---

[16] The hyperlink to Data Policy sends users to the Meta Privacy Policy at https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0.

CONSOLIDATED CLASS ACTION COMPLAINT

1

2

3

4

5

6

7

8

9

What happens if you don't let us collect certain information

For example, if you don't provide an email address or phone number, we won't be able to create an account for you to use our Products.

Or you can choose not to add Facebook friends, but then your Facebook Feed won't show friends' photos and status updates.

10

11   98.   Meta's Terms of Service also expressly incorporates the Meta Privacy Policy by

12 hyperlink, stating that "Our Privacy Policy explains how we collect and use your personal data to

13 determine some of the ads you see and provide all of the other services described" in Meta's Terms

14 of Service.

15   99.   The Meta Privacy Policy begins with the statement, "We at Meta want you to

16 understand what information we collect, and how we use and share it. That's why we encourage

17 you to read our Privacy Policy. This helps you use Meta Products in the way that's right for you."

18   100.   Next, the Meta Privacy Policy has a section titled "What information do we

19 collect?," in which Meta tells users:

20   At Meta, we use information to provide you with a more personal,
               secure, and meaningful experience. But where does that information
21   come from? The information we collect comes from a variety of
               sources.... *And, sometimes businesses also share information with*
22   *us like your activity on their websites. They may also share*
               experiences you have offline, like signing up for a Rewards card
23   *with your email address.* This makes it easier for them to share
               promotions, product information, and other ads with you through
24   our ads consistent with the choices that you make.

25   (Emphasis added.)

26

27   101.   Meta places the information it collects into four categories:

28

CONSOLIDATED CLASS ACTION COMPLAINT

102.   The word "Partners" is a defined term in Meta's contract, which Meta explains are "[b]usinesses and people" who use Meta's "Products," including the Meta Pixel or Meta Audience Network tools "to advertise, market, or support their products and services." Meta's "examples" of "Partners" include: advertisers, "companies that measure how well ads are doing and provide reports," and "publishers (like a website or app) and their business partners."

103.   The Meta Privacy Policy does not include any category for information collected from Facebook users' health care providers, health insurers, pharmacies, prescription drug companies, or other covered entities under 45 C.F.R. § 160.103 and Cal. Civil Code § 561.101, which includes patient portal providers.

104.   The Meta Privacy Policy does not specify anywhere that Meta's Partners include health care providers, health insurers, pharmacies, prescription drug companies, and other covered entities under 45 C.F.R. § 160.103 and Cal. Civ. Code § 56.101.

105.   The Meta Privacy Policy does not state anywhere that Meta actively solicits Facebook users' health care providers, health insurers, pharmacies, prescription drug companies, and other covered entities under 45 C.F.R. § 160.103 and Cal. Civ. Code § 56.101 to become Meta Partners using Meta's business services.

106.   The Meta Privacy Policy does not state anywhere that, in exchange for use of its Products, Meta will collect health information from a Facebook user's health care providers, health insurers, pharmacies, prescription drug companies, or other covered entities under 45 C.F.R.

CONSOLIDATED CLASS ACTION COMPLAINT

1   § 160.103 and Cal. Civ. Code § 56.101 about the Facebook user, including their communications,

2   actions, and status as patients with those health entities.

3   107.   As the Court has previously stated, "Meta's policies do not … specifically indicate

4   that Meta may acquire *health data* from Facebook users' interactions with their *medical providers'*

5   *websites*." Dkt. 159 at 15.

6   108.   Meta has admitted that there is no "specific consent" for Meta's collection of health

7   information as described in this action.

8   109.   Meta told the Court that "*there is not a specific consent* because Meta doesn't want

9   this data." Nov. 9, 2022 Hearing Transcript at 20:20-21 (emphasis added).

10   110.   In addition to not obtaining specific consent, Meta has affirmatively promised users

11 that it requires "Partners" to have the right to share the users' data before providing it to Meta.

12   111.   In April 2018, Meta added a new clause to its contract with users that states: "We

13 require each of these partners to have lawful rights to collect, use and share your data before

14 providing any data to us."

15 ///

16 ///

17 ///

18 ///

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

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

112. Before April 2018, Meta's contract did not require Partners to have the lawful right to share user data before doing so.

Before April 19, 2018	After April 19, 2018
Information from websites and apps that use our Services. We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us. **Information from third-party partners.** We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.	**Information from partners.** Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information. Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from. To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

CONSOLIDATED CLASS ACTION COMPLAINT

1   113.   Meta changed this provision again in July 2022—after Plaintiffs filed this lawsuit—

2   to remove the word "lawful" while still promising that it requires partners to have the right to share

3   patient information with Meta:[17]

4   **How do we collect or receive this information from partners?**

5   Partners use our Business Tools, integrations and Meta Audience Network
    technologies to share information with us.

6

7   These Partners collect your information when you visit their site or app or use
    their services, or through other businesses or organizations they work with. We

8   require Partners to have the right to collect, use and share your information be-

9   fore giving it to us.

10

11   114.   Despite the changes it made to this provision over time, Meta has never "required"

12   health care providers or other covered entities, to have the right to "collect, use and share" patient

13   information before redirecting it to Meta. Instead, Meta merely includes a provision in its form

14   contract that creates an unenforced "honor system," stating that by using Meta's Business Tools

15   the health care provider or covered entity "represent[s] and warrant[s] that [it has] provided robust

16   and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing

17   and usage":[18]

18   / / /

19   / / /

20   / / /

21   / / /

22   / / /

23   / / /

24   / / /

25

26   [17] Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023),

27   https://www.facebook.com/privacy/policy?subpage=1.subpage.4-
    InformationFromPartnersVendors.

28   [18] Dkt. 76-6 at 4.

3. Special Provisions Concerning the Use of Certain Business Tools

a. This section applies to your use of Business Tools to enable Facebook to store and access cookies or other information on an end user's device.

b. You (or partners acting on your behalf) may not place pixels associated with your Business Manager or ad account on websites that you do not own without our written permission.

c. You represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage that includes, at a minimum:

i. For websites, a clear and prominent notice on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites and elsewhere on the Internet and use that information to provide measurement services and target ads, (b) how users can opt-out of the collection and use of information for ad targeting, and (c) where a user can access a mechanism for exercising such choice (e.g., providing links to: http://www.aboutads.info/choices and http://www.youronlinechoices.eu/).

ii. For apps, a clear and prominent link that is easily accessible inside your app settings or any privacy policy and from within any store or website where your app is distributed that links to a clear explanation (a) that third parties, including Facebook, may collect or receive information from your app and other apps and use that information to provide measurement services and targeted ads, and (b) how and where users can opt-out of the collection and use of information for ad targeting.

d. In jurisdictions that require informed consent for storing and accessing cookies or other information on an end user's device (such as but not limited to the European Union), you must ensure, in a verifiable manner, that an end user provides all necessary consents before you use Facebook Business Tools to enable the storage of and access to Facebook cookies or other information on the end user's device. (For suggestions on implementing consent mechanisms, visit Facebook's Cookie Consent Guide for Sites and Apps.)

115. Meta does not verify that health care providers or covered entities have provided adequate notice and obtained valid consent or authorization to share their patients' data with Meta.[19]

116. Instead, Meta makes the Pixel available to any advertisers who uses Meta's automated tools to create and deploy the Pixel. This process does not include any effort by Meta to require its Partners to have lawful rights to use the Pixel. Meta does nothing to determine whether an advertiser is placing the Pixel on a website that contains health information and through which Meta will acquire health information.

117. Elsewhere in Meta's Privacy Policy, the term "require" signifies that something is not possible unless it is complied with by a user. For example:

a. Meta states that "Some information is required for our Products to work," explaining that "if you don't provide an email address or phone number, we won't be able to create an account for you to use our Products. Or you can

---

[19] The European Union recently ruled that Meta's attempt to obtain consent from users by including a clause in its terms and conditions allowing Meta to collect their data for personal advertising violated Europe's General Data Protection Regulation. Adam Satariano, *Meta's Ad Practices Ruled Illegal Under E.U. Law*, N.Y. Times (Jan. 4, 2023), https://www.nytimes.com/2023/01/04/technology/meta-facebook-eu-gdpr.html.

choose not to add Facebook friends, but then your Facebook Feed won't show friends' photos and status updates."[20] Dkt. 76-12 at 7, 17.

      b.   Meta states that it engages in "manual review" to access and review information in some cases but promises, "We require every reviewer who's allowed access to your information to meet privacy and security standards."[21] Dkt. 76-12 at 24.

118.   Meta stated to this Court that it has created a "filter to detect data sent through the Pixel" that Meta "categorizes as potentially sensitive data, including health data." Wooldridge Decl. (Dkt. 76-1) ¶ 8. Meta has also stated to members of Congress that it has the ability to "suspend[ ] or terminat[e] [a] developer from using our Business Tools" such as the Pixel.[22]

119.   Meta does not use the filter or any other technological means to require web developers to have the right to share health information with Meta.

120.   Meta's contract with health care providers for use of the Meta Pixel does not mention HIPAA.

121.   In its Terms of Service, Meta promises that it goes to great lengths to ensure "the safety, security, and integrity" of its products and services:

> We employ dedicated teams around the world, work with external service providers, partners and other relevant entities and develop advanced technical systems to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community, including to respond to user reports of potentially violating content.[23]

122.   Meta does not "employ a dedicated team" or contract with an external service provider to determine whether the Pixel is installed on websites that will transmit individually identifiable health information to Meta.

---

[20] Meta, Privacy Policy: What happens if you don't let us collect certain information (Jan. 1, 2023), https://www.facebook.com/privacy/policy?annotations[0]=1.ex.43-WhatHappensIfYou.

[21] Meta, Privacy Policy: Manual review (Jan. 1, 2023), https://www.facebook.com/privacy/policy?annotations[0]=2.ex.2-ManualReviewExamplesOf.

[22] Meta letter to Senator Mark Warner at 4 (Nov. 3, 2022).

[23] Dkt. 76-3 at 4.

123. Meta does not use an advanced technical system to monitor whether the Pixel is installed on websites that will transmit individually identifiable health information to Meta.

124. To the contrary, Meta Health urges health care providers and other covered entities to use the Pixel and other Meta tools to target ads to patients.

F.   Meta's health marketing division targets its "Partner" health care providers and covered entities and their patients to "disrupt health" and "market to patients."

125. On November 9, 2022, Meta told the Court in oral argument in opposition to Plaintiffs' Motion for Preliminary Injunction that:

a.   "Meta doesn't want sensitive information. It doesn't want health information. … It doesn't want any information that web developers have no right to send, and so Meta is very over-inclusive about what it tries to block out, both contractually and through its own systems, which it is constantly working hard at improving." Nov. 9, 2022 Mot. for PI Hearing Tr. at 21:11-18.

b.   Meta represented to the Court that it tells developers "don't send us anything that you don't have the legal right to send us and don't send us health information …, even if you think you have the right. Even if you think your disclosures are terrific and you have total consent, don't send us that stuff. We don't want it." *Id*. at 22:1-6.

c.   Meta represented to the Court that it has "an over-inclusive filter system … that classifies our partners, these web developers, not as HIPAA-covered, okay, because we go beyond that. We say if it has anything to do with health, then we operate our systems, which are described in the Wooldridge declaration in the portion that are sealed, and we have multiple different backstopping ways of preventing this information from coming into Meta. So we're doing the best we can to prevent that information from coming in and being used." *Id*. at 22:7-18.

126.   Meta actively encourages health entities to use its marketing tools.

127.   Meta maintains a "Health" marketing division called Meta Health, with a page at https://www.facebook.com/business/industries/consumer-goods/healthcare where Meta offers advertisers the chance to "get help growing your healthcare business" and explains how "Healthcare marketers are partnering with Meta."

128.   The underlying metadata written for this page by Meta describe the page keywords to include: " <meta name="keywords" content="healthcare, marketers, facebook, meta for business, healthcare business, virtual healthcare, preventative healthcare" />."

129.   Meta Health is dedicated to helping web developers and advertisers in health care-related industries to increase their marketing spend with Meta and improve their marketing campaigns using the Pixel and other Meta marketing products.

130.   Meta Health's role is to "inspir[e]" health care marketers "to think about how we can really disrupt health and how we market to patients."[24]

131.   Meta Health employees are assigned to specific health care providers and other covered entities to encourage and aid their use of the Pixel and other Meta marketing products for targeting patients.

132.   Meta provides guidance and resources for web developers and advertisers on a dedicated webpage at https://www.facebook.com/business/industries/health. Among other things, this webpage includes examples of advertising campaigns so that web developers and advertisers can "See how health brands are reaching new audiences with Facebook advertising."

133.   The underlying metadata written for this page by Meta describes the page keywords to include: ""<meta name="keywords" content="facebook for health, facebook marketing for health communities, facebook ad solutions for health brands, social media marketing, facebook video ads facebook for mobile advertising, health campaign marketing, reach new patients online facebook ads, advertising on facebook" />."

---

[24] Facebook, Disrupting Health: A Conversation with Jasson Gilmore, https://www.facebook.com/business/industries/health?deeplink=829704181304626.

134.   For example, Meta highlights an advertising campaign "for adults with COPD":
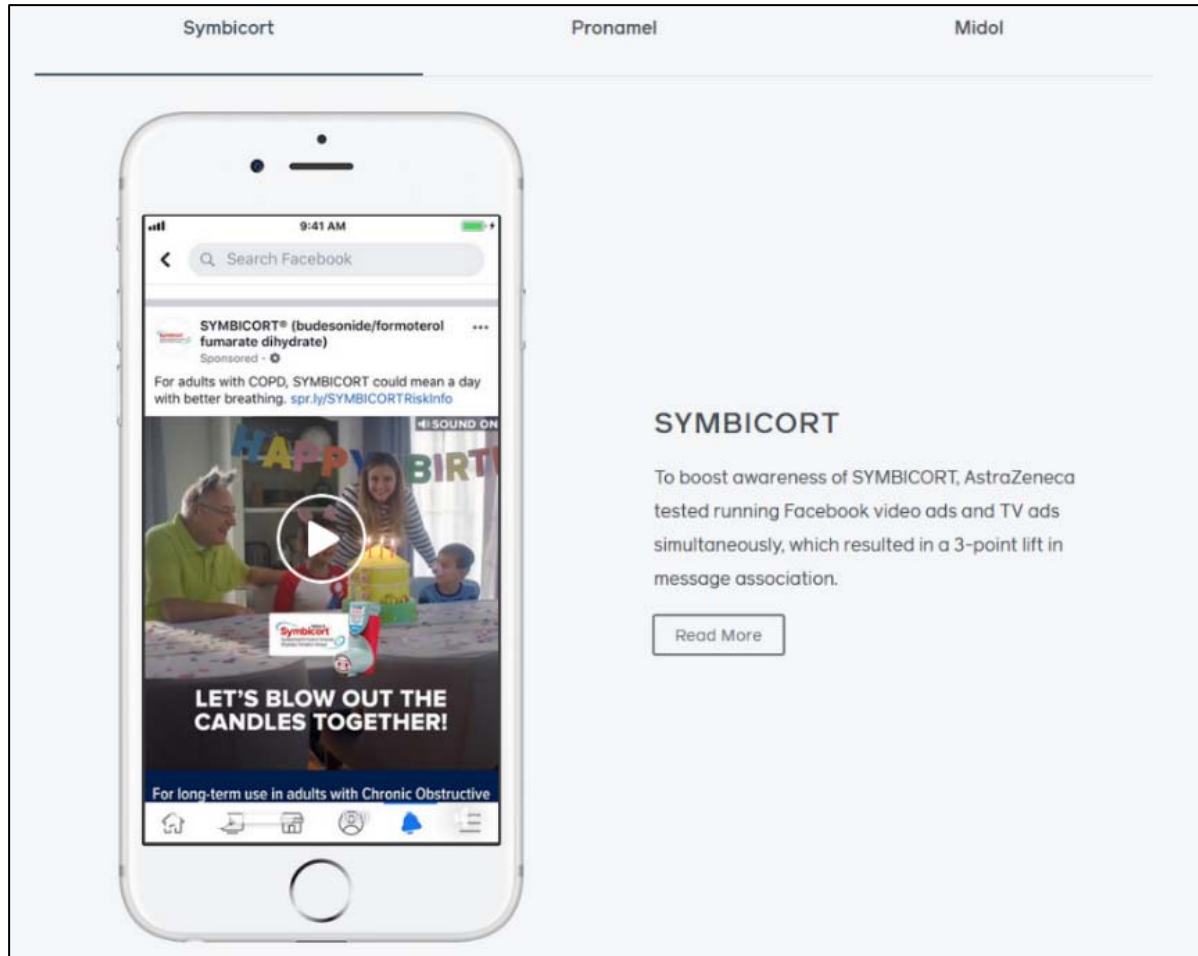
135.   Meta also highlights a campaign aimed at "young women" through video ads promising to "Relieve your period symptoms today":[25]

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

---

[25] Meta, *Midol* (2023), https://www.facebook.com/business/success/2-midol.
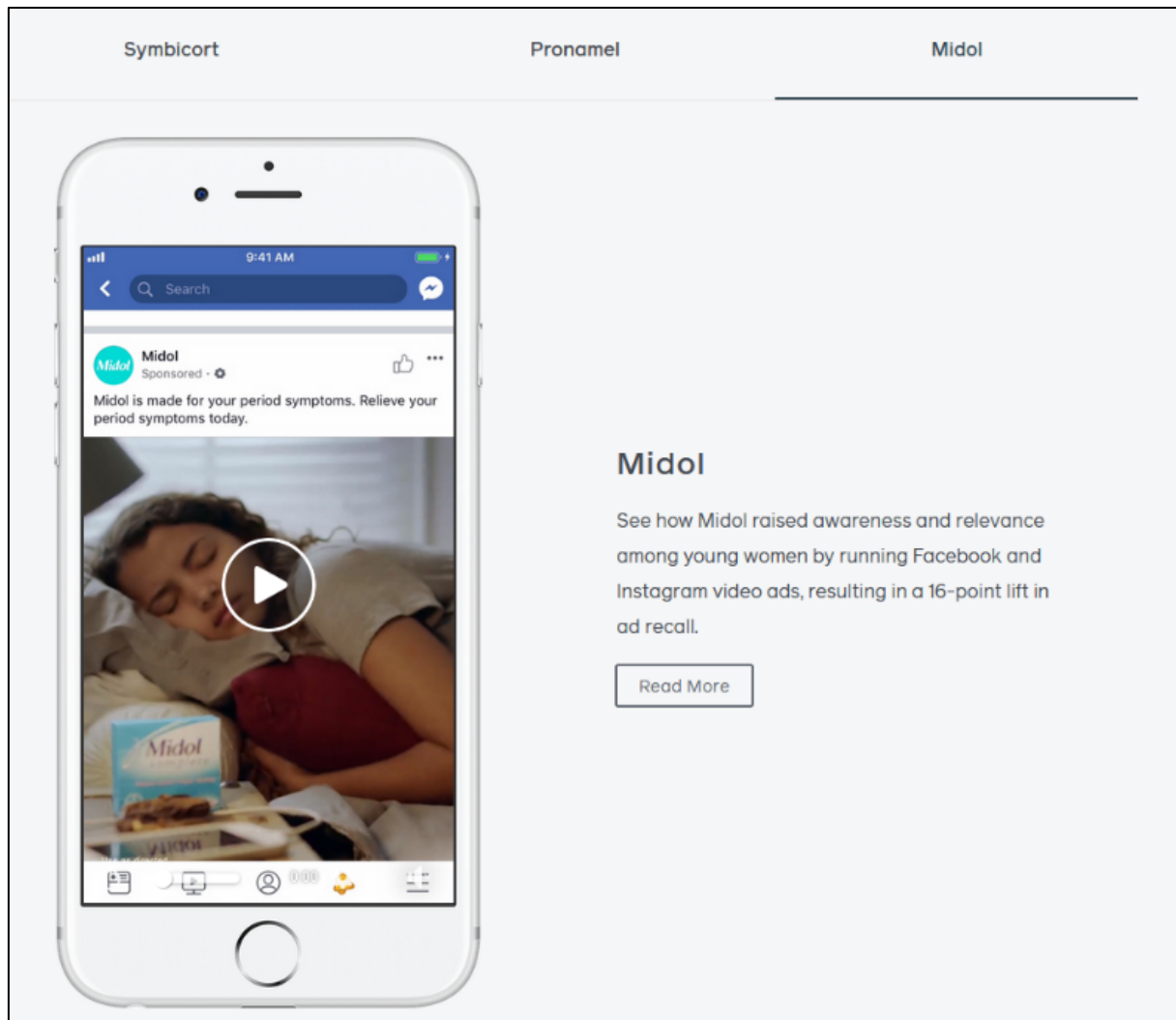
136.   Meta also highlights a campaign as "a unique way to reach [cancer] patients":[26]

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

---

[26] Meta, *AstraZeneca: Reaching more patients with video ads in Facebook In-Stream Reserve* (2023), https://www.facebook.com/business/success/2-astrazeneca.

137.   Meta has also discussed successful advertising campaigns relating to lung cancer, high cholesterol, arthritis, acne, allergies, hair loss, birth control, erectile dysfunction, migraines, and many additional prescription drugs and treatments.[27]

138.   To promote its marketing tools to health care providers and covered entities, the Meta health webpage includes Meta Health's Erin Ott's interview with Jasson Gilmore, Senior Vice President for Global Consumer & Digital Marketing at AbbVie. In the interview, Gilmore

---

[27] *See generally* Meta, *Get winning advertising solutions from businesses like yours* (2023), https://www.facebook.com/business/success/categories/health-pharmaceuticals. The "marketing case studies" on this page change on occasion.

CONSOLIDATED CLASS ACTION COMPLAINT

1 states, "Social media is a primary place your target audience spends their time" and "if you're

2 going to be trying to market to potential patient populations that have unmet needs or under-

3 serviced, these are platforms that give you immense control and measurability around the way you

4 spend and allocate capital." The pitch also stresses that it can be a "research platform" that provides

5 "millions and millions of data points of the consumers who are interested in our brands," which is

6 "an invaluable asset." Through Meta, an advertiser can get "millions and millions of consumers

7 who actually use [its] brands."[28]

8   139.   Ott then asks Gilmore specifically about "the patient journey" and how Metacan

9 "play a role in that patient journey."
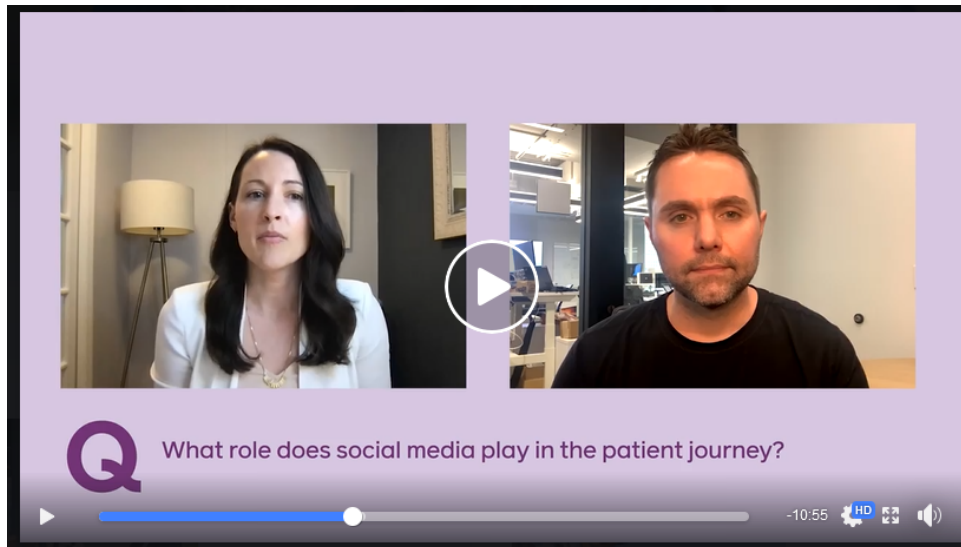
19   140.   The response is that Meta's marketing tools (including the Pixel) can target

20 potential and existing patients:

> We look at these channels in the conventional sort of framework of
> the patient journey. You have what we call the upper funnel, things
> like television. I think social media conventionally would be
> plugged into that sort of upside-down pyramid slide we've all seen
> a million times, right? It doesn't matter where you work, you've
> seen a slide like that. And then you have your lower intent, you have
> things like search, and then obviously we're trying to drive at an
> event where a consumer is talking to a provider, right? That's sort
> of your, kind of, conventional consumer journey slot.

[28] Facebook, Disrupting Health: A Conversation with Jasson Gilmore,
https://www.facebook.com/business/industries/health?deeplink=829704181304626.

I don't think about social that way actually. I think that, you know, really all the way through to a patient who's already on our products. I look at their journey as a continuum. Now there's a dynamic in our particular brands where consumers stay on our products for a period of time, and they have a lifetime value. And I want to increase that lifetime value. I want to increase the frequency with which consumers use our products and I want to drag outward the timeline for how long they use our products.

So, in my view, from someone who is a potential consumer, who looks like, you'll hear this phrase 'Lookalike Audience,' the next person who is likely to receive one of our products looks like the last person who uses our product. And so we can use social media to help target potential new consumers, but all the way through, down to people who've been in care on our products for many years.

I use [social media] as a way to reach them. I know who those people are. I can target my media and my messaging around it. And I can actually tailor the message, right? And this gets into the buzzword 'personalization' that we hear so much about. I know who those people who are already on our products, I know who they are. And

I can tailor a message that is custom to the product that they're using, how long they've used it, even how frequently they use it, and even the region and the provider they use it with.

> ❝
>
> We can use social media to help target potential new consumers, but all the way through, down to people who've been in care on our products.
>
> **Jasson Gilmore**
> SVP Global Consumer & Digital Marketing, AbbVie

And so, from my perspective, it's an essential tool not just for driving that kind of traditional upper-funnel sort of dynamic, but really increasing the lifetime of our consumers and then that increases what your cost per acquisition threshold can be.

141.   The conversation then makes a direct reference to the detailed level through which Meta's systems work, stating that Meta offers ads "personalization" where "you can know who your audience is," "you can tailor a message that's custom to the product they're using," and "you

CONSOLIDATED CLASS ACTION COMPLAINT

1 | can know their region and provider."

PERSONALIZATION

1. You can know who your audience is.

2. You can tailor a message that's custom to the product they're using.

3. You can know their region and provider.

Jasson Gilmore
SVP Global Consumer & Digital Marketing, AbbVie

142.   In a pitch directly to health care providers, Meta's Ott asks Gilmore, "How are you guys thinking about … arming [health care providers] with the tools to advertise for themselves?" The answer: "You have to be using these tools to stay relevant with your customer in this day and age – whatever industry you happen to be in – and this is just as true for our physician partners as it is for our own business."

Q   Why has building marketing tools for healthcare providers become such a business priority for you?

CONSOLIDATED CLASS ACTION COMPLAINT

143.   Gilmore explains how his company is helping health care providers use Meta's tools and adds, "I think you all do a fabulous job, frankly, of enabling that for your customers."

144.   At the end of the video, Gilmore emphasizes the benefit to health care providers of knowing who their patients and potentials patients are:

145.   Meta's Ott concludes the video with a final thought: "Hopefully everyone is really inspired now to think about how we can really disrupt health and how we market to patients."

> **"**
>
> It's such an optimistic thing to know who your patients are or who your potential patients are and how to reach them in a way that is very financially **manageable** and **feasible** and **profitable.**
>
> **Jasson Gilmore**
> SVP Global Consumer & Digital Marketing, AbbVie

146.   Presumably, if Meta thought that any part of the interview with Gilmore incorrectly explained how Meta's marketing worked, it would not be promoted as a case study of its services.

G.   Meta's health marketing division already has systems it could adapt to comply with an injunction.

147.   Plaintiffs request permanent injunctive relief in this action.

148.   Meta's public descriptions of systems it already has in place for advertising are relevant to demonstrate that Meta is fully capable of complying with an injunction order.

149.   In response to Plaintiffs' Motion for Preliminary Injunction, Meta argued that it did not want to receive health information.

150.   Plaintiffs filed an expert declaration in support of their reply explaining how Meta could and should create a system to detect Pixel data that it was wrongfully acquiring from health

1 care providers that would involve: (1) the use of automated systems to detect health content;

2 (2) automatic blocking of Pixel data from properties sending health content; and (3) an appeal

3 process to address Meta's concerns that its filter may unintentionally block some otherwise lawful

4 data.

5   151.   In response, Meta suggested such a system would be unworkable.

6   152.   The video on "compliance" that Meta already has in place for ads describes a

7 similar system to the one described by Plaintiffs' expert.[29]

8   153.   Meta provides health care advertisers with a diagram of its ad review system:
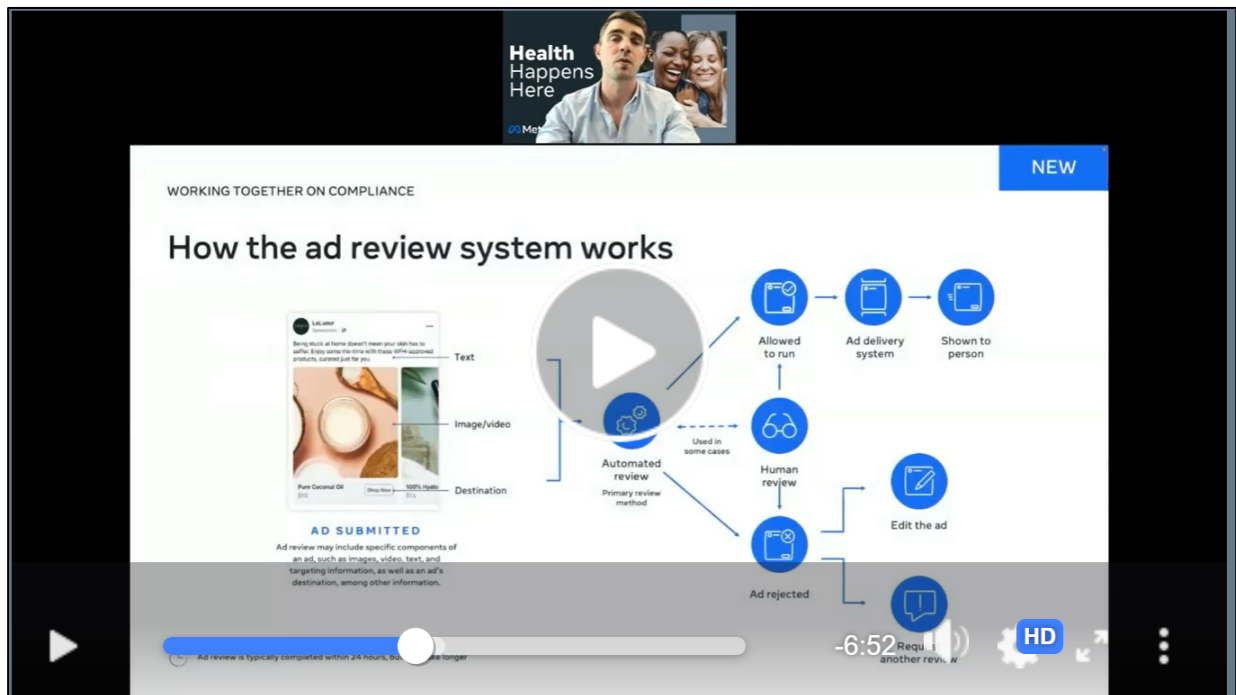
20   154.   Meta claims that its "ad review system is actually designed to review all ads

21 proactively, which means before they go live" and "relies primarily on automated technology to

22 apply our advertising policies to the millions of ads that we have going live every single day."

23   155.   Meta also states that it uses human reviewers in some cases, and that, the "review

24 process may include specific components of an ad, such as images, video, text, targeting

25 information, or an ad's destination, amongst other information."

26

27

[29] *See* Meta, *Chapter 3: Working together on compliance* (June 13, 2022),
28 https://www.facebook.com/business/inspiration/video/healthcare-chapter-3.

156.   The ad review process is "typically … completed within 24 hours, but it may take longer and ads may be reviewed again, including after they are live."

157.   An ad is either rejected or allowed to run based on the results of Meta's review.

158.   When an ad is rejected, Meta offers advertisers options to appeal or work around the rejection. The advertiser can create an entirely new ad or revise the rejected ad to address any policy violations. And "if an advertiser believes that their ad is wrongfully rejected, another review can be requested and the status of this can be tracked in account quality."

159.   Meta advises advertisers that "[u]nlike the initial review, we rely more heavily on teams of human reviewers to process re-review requests from advertisers."

160.   Later in the same video, Meta tells advertisers that it may place "restrictions on their ability to advertise on Meta platforms" if they repeatedly engage in certain conduct.

161.   Meta could and should adapt these systems to, as alleged in further detail below to stop: (1) acquiring health information in violation of federal and state law; (2) acquiring health information in violation of its express privacy promises; and (3) permitting advertisers to use health information to target advertising to patients.

H.   Meta's conduct violates federal and state privacy laws.

1.   The HIPAA Privacy Rule protects patient health care information.

162.   Patient health care information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

163.   The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[30]

164.   The Privacy Rule broadly defines "protected health information" ("PHI") as "individually identifiable health information" ("IIHI") that is "transmitted by electronic media;

---

[30] HHS.gov, *Health Information Privacy* (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

1 maintained in electronic media; or transmitted or maintained in any other form or medium." 45

2 C.F.R. § 160.103.

3   165. IIHI is defined as "a subset of health information, including demographic

4 information collected from an individual" that is: (1) "created or received by a health care provider,

5 health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future

6 physical or mental health or condition of an individual; the provision of health care to an

7 individual; or the past, present, or future payment for the provision of health care to an individual";

8 and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable

9 basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

10   166. Under the HIPAA de-identification rule, "health information is not individually

11 identifiable only if": (1) an expert "determines that the risk is very small that the information could

12 be used, alone or in combination with other reasonably available information, by an anticipated

13 recipient to identify an individual who is a subject of the information" and "documents the methods

14 and results of the analysis that justify such determination'"; or (2) "the following identifiers of the

15 individual or of relatives, employers, or household members of the individual are removed:

16   A. Names;

17   H. Medical record numbers;

18   J. Account numbers;

19   M. Device identifiers and serial numbers;

20   N. Web Universal Resource Locators (URLs);

21   O. Internet Protocol (IP) address numbers; … and

22   R. Any other unique identifying number, characteristic, or code…; and"

23   the covered entity must not "have actual knowledge that the information

24   could be used alone or in combination with other information to identify

25   an individual who is a subject of the information." 45 C.F.R. § 164.514.

26   167. The HIPAA Privacy Rule requires any "covered entity"—which includes health

27 care providers—to maintain appropriate safeguards to protect the privacy of protected health

28

1   information and sets limits and conditions on the uses and disclosures that may be made of

2   protected health information without authorization. 45 C.F.R. §§ § 160.103, 164.502.

3   168.   An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1)

4   uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health

5   information relating to an individual." The statute states that a "person … shall be considered to

6   have obtained or disclosed individually identifiable health information … if the information is

7   maintained by a covered entity … and the individual obtained or disclosed such information

8   without authorization." 42 U.S.C. § 1320d-6.

9   169.   The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to

10   Meta when it is knowingly obtaining individually identifiable health information relating to an

11   individual, as those terms are defined under HIPAA.

12   170.   Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. §

13   1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell,

14   transfer, or use individually identifiable health information for commercial advantage, personal

15   gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable

16   health information relating to an individual shall "be fined not more than $250,000, imprisoned

17   not more than 10 years, or both."

18   **2.**   **Patient status is among the health information protected by HIPAA.**

19   171.   An individual's status as a patient of a health care provider is protected by HIPAA.

20   Dkt. 159 at 12 ("I agree that the information at issue here appears to show patient status and thus

21   constitutes protected health information under HIPAA."), 15 ("[T]he Pixel captures information

22   that connects a particular user to a particular health care provider—i.e., patient status—which falls

23   within the ambit of information protected under HIPAA").

24   172.   Guidance from HHS confirms that patient status is protected by HIPAA:

25   Identifying information alone, such as personal names, residential
26   addresses, or phone numbers, would not necessarily be designated
        as PHI. For instance, if such information was reported as part of a
27   publicly accessible data source, such as a phone book, then this
        information would not be PHI because it is not related to health data.
28   … **If such information was listed with health condition, health**

care provision or payment data, **such as an indication that the individual was treated at a certain clinic**, then this information would be PHI.[31]

173.   HHS's guidance for marketing communications states that health care providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, **covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list**.[32]

174.   HHS has previously instructed that patient status is protected by the HIPAA Privacy Rule:

a.   "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b.   "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

c.   It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

---

[31] Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[32] Office for Civil Rights, *Marketing* at 1-2 (emphasis added) (Apr. 3, 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

d.   The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

3.   There is no HIPAA exception for marketing on the Internet.

175.   HHS issued a bulletin in December 2022 "to highlight the obligations" of health care providers and their business associates under the HIPAA Privacy Rule "when using online tracking technologies" such as the "Meta Pixel," which "collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application."[33]

176.   In the bulletin, HHS confirmed that HIPAA applies to health care providers' use of tracking technologies like the Meta Pixel.[34] Among other things, HHS explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an

---

[33] HHS.gov, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information* (Dec. 1, 2022), https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html.

[34] HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. **This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e*. it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care**.

177.   HHS explained that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnosis and treatment information, in addition to other sensitive data:

Tracking on user-authenticated webpages

Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. **Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal**. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.

178.   Tracking technology vendors like Meta are considered business associates under HIPAA if they provide services to health care providers and receive or maintain PHI, like Meta does:

Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a

CONSOLIDATED CLASS ACTION COMPLAINT

regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.

179.   HIPAA applies to health care providers' webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … **[and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

180.   And no PHI may be disclosed to tracking technology vendors like Meta unless the health care provider has properly notified its website users and entered into a business associate agreement with the vendor:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on

> a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.
>
> If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.
>
> [I]t is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

181.   HHS's bulletin did not create any new obligations. Instead, it highlighted long-standing obligations with citations to previous guidance and rules that have been in place for decades.

4.   State law also protects health information.

182.   The Meta Terms of Service expressly provide that "the 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."

183.   California has enacted several laws to protect patients' information. The California Confidentiality of Medical Information Act requires health care providers to preserve the confidentiality of patients' medical information and to obtain valid authorization before disclosing a patient's medical information to a third party. Cal. Civ. Code § 56, *et seq*. The California Consumer Privacy Protection Act requires businesses to disclose that they are obtaining medical information for marketing purposes and obtain written consent. Cal. Civ. Code § 1798.91(a)(2), (c). The California Consumer Privacy Act of 2018 requires business to notify consumers when they collect sensitive personal information, including medical information, and the purposes of the collection and use of that information. Cal. Civ. Code § 1798.100 *et seq.*

/ / /

184. Meta's conduct in this action violates each of these California laws or involves Meta's knowing participation with health care entities in violating these California laws.

185. For example, the California Confidentiality of Medical Information Act provides that "[e]very provider of health care, health care service plan, *pharmaceutical company*, or contractor who creates, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101 (emphasis added). The CMIA then incorporates "remedies and penalties" for violations of the statute, including the creation of a civil action, under Cal. Civ. Code § 56.36 (b) and (c).

186. Thus, the California Confidentiality of Medical Information Act applies to pharmaceutical companies and information within their control, rendering Meta's actions with respect to pharmaceutical companies and the interception of health communications with pharmaceutical companies unlawful under California law, which Meta expressly adopts in its relationship with Facebook users.

187. The California Consumer Privacy Protection Act applies to "medical information" maintained by any entity, which would include pharmaceutical companies. It provides that "[a] business may not request in writing medical information directly from an individual regardless of whether the information pertains to the individual or not, and use, share, or otherwise disclose that information for direct marketing purposes," without first (1) "disclosing in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual;" and (2) "obtaining the written consent of either the individual to whom the information pertains or a legally authorized representative to consent for the individual, to permit his or her medical information to be used or shared to advertise products, goods, or services to the individual." Cal. Civ. Code § 1798.91I.

188. The California Consumer Privacy Act of 2018 requires that "[i]f the business collects sensitive personal information," it shall inform consumers of "the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared" and "shall not

1   collect additional categories of sensitive information or use sensitive personal information

2   collected for additional purposes that are incompatible with the disclosed purpose for which the

3   sensitive personal information was collected without providing the consumer with notice

4   consistent with this section." Cal. Civ. Code § 1798.100. As defined under the Act, "sensitive

5   personal information" means "personal information that reveals … personal information collected

6   and analyzed concerning a consumer's health." Cal. Civ. Code § 1798.140(ae)(2)(B).

7   189.   The California Consumer Privacy Act of 2018 also provides that "[a]ny consumer

8   whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of

9   paragraph (1) of subdivision (d) of Section 1798.81.5 …. is subject to an unauthorized access and

10   exfiltration, theft, or disclosure as a result of a business's violation of the duty to implement and

11   maintain reasonable security procedures and practices appropriate to the nature of the information

12   to protect the personal information may institute a civil action for" statutory damages, actual

13   damages, injunctive or declaratory relief, or any other relief the court deems proper. Cal. Civ. Code

14   § 1798.150(a). In turn, "personal information" is defined in Cal. Civ. Code § 1798.81.5 to mean

15   "[a]n individual's first name or first initial and the individual's last name in combination with any

16   one or more of the following data elements, when either the name or the data elements are not

17   encrypted or redacted …. Medical information [or] health insurance information." Cal. Civ. Code

18   § 1798.81.5(d)(1)(A)(iv)-(v). "Medical information" means "any individually identifiable

19   information, in electronic or physical form, regarding the individual's medical history or medical

20   treatment or diagnosis by a health care professional." Cal. Civ. Code § 1798.81.5(d)(2). "Health

21   insurance information" means "any unique identifier used by a health insurer to identify the

22   individual or any information in an individual's application and claims history." Cal Civ. Code

23   § 1798.81.5(d)(3).

24   **5.   Patients have protectable property interests in their individually**

25   **identifiable health information.**

26   190.   Property is the right of any person to possess, use, enjoy, or dispose of a thing,

27   including intangible things like data and communications. Plaintiffs and Class members have a

28   vested property right in their individually identifiable health information.

191.   California courts have described property broadly:

    a.   "The word property may be properly used to signify any valuable right or interest protected by law." *Fields v. Michael*, 91 Cal. App. 2d 443, 449 (1949); *Downing v. Municipal Court*, 88 Cal. App. 2d 345, 359 (1948).

    b.   "The term property is sufficiently comprehensive to include every species of estate, real and person, and everything which one person can own and transfer to another. It extends to every species of right and interest capable of being enjoyed as such upon which it is practicable to place a money value." *Yuba River Power Co. v. Nevada Irr. Dist.*, 207 Cal. 521, 523 (1920).

    c.   "The term [property] is all-embracing, including every intangible benefit and prerogative susceptible of possession or disposition." *People v. Kozlowski*, 96 Cal. App. 4th 853, 866 (2002).

    d.   Property includes a copy of a key that is made without the key owner's knowledge when the original is returned to the owner, "which is analogous to making … an unauthorized copy of computer data." *People v. Kwok*, 75 Cal. App. 4th 1236, 1251 (1998).

192.   Federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular health care provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

193.   A patient's right to protect the confidentiality of their health data and restrict access to it is a valuable right.

194.   In addition to property rights in their health data, patients enjoy property rights in the privacy of their health communications.

195.   Patient property rights in their health data and communications are established by:

    a.   HIPAA;

    b.   The California Confidentiality of Medical Information Act;

c. The California Consumer Privacy Protection Act;

d. The California Consumer Privacy Act of 2018; and

e. State health privacy laws.

196. American courts have long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

197. Property rights in communications and information privacy are established by:

a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act);

b. State laws, including the California Invasion of Privacy Act, that establish a right to keep communications confidential;

c. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist. *See Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

198. Meta's unauthorized acquisition of Plaintiffs' and Class members' individually identifiable health information violated their property rights to control how their data and communications are used and who may be the beneficiaries of their data and communications.

6.   The information Meta acquires without Plaintiffs' and Class members' consent has actual, measurable monetary value

199. Meta's services are not free.

200. Rather than pay with cash, Facebook users pay for Meta's services by agreeing to provide Meta with the right to collect certain data, the "data license."

201. Meta's "data license" rights to collect data about its users is not unlimited.

202. The "data license" for Meta's services is defined by law and Meta's contract.

203. By law, Meta may not collect individually identifiable health information about users without express informed consent on a form separate from the contract of adhesion that Meta

1   presents to users. Where individually identifiable health information is collected for marketing

2   purposes, the legal requirements for its collection and use are even more stringent.

3   204.   Other limitations on the "data license" paid for Meta's services are outlined by the

4   Meta contract.

5   205.   The "data license" includes data that Facebook users provide when signing up for

6   Meta and when using Meta platforms on Meta properties – subject to limitations in Meta's contract.

7   206.   The "data license" also includes data that Meta specifically discloses as part of the

8   "data license" in the Meta contract documents, and that Meta does not specifically exclude from

9   the "data license" as part of the contract.

10   207.   As described above, the "data license" to become a Facebook user does not include

11   individual health information associated with a Facebook user and their health care provider or

12   other covered entities under federal and state health privacy laws.

13   208.   Although not included in the contract, Meta collects this additional data anyway,

14   thereby overcharging Plaintiffs and Class members for use of Meta's services.

15   209.   The "data license" overcharge that Meta collects without authorization, and the

16   collected data, has monetary value.

17   / / /

18   / / /

19   / / /

20   / / /

21   / / /

22   / / /

23   / / /

24   / / /

25   / / /

26   / / /

27   / / /

28

210.   For example, a 2015 study found respondents placed a value of $59.80 on health information.

Data type	Value
Passwords (login details)	$75.8
Health condition	$59.8
Social Security number *	$55.7
Payment details (credit card)	$36.0
Credit history	$29.2
Names of friends & family members	$23.5
Purchase histories	$20.6
Physical location (GPS)	$16.1
School or employer	$13.3
Home address	$12.9
Photos & videos	$12.2
Hobbies, tastes & preferences	$12.2
Marital status	$8.3
Email address	$8.0
Browser settings & histories	$7.1
Special dates including date of birth	$5.9
Phone numbers	$5.9
Name	$3.9
Gender	$2.9

$0.0 $10.0 $20.0 $30.0 $40.0 $50.0 $60.0 $70.0 $80.0
* This response was only available for US participants

211.   In addition, some companies sell de-identified health information in the open market. For example, a company named Prognos Health provides a data platform where it purports to sell information from "more than 325 million de-identified patients."[35]

212.   Meta obtains substantial revenues from the collection and use of private health data for targeted ads. For example, one way that Meta and other data companies report on the value of

---

[35] Prognos Health, *Prognos Health Announces Patent-Pending Technology* (Apr. 6, 2021), prognoshealth.com/about-us/news/press-release/prognos-health-announces-patent-pending-technology.

1   their business is through average revenue per user or "ARPU." Meta has long used ARPU in its

2   Annual and Quarterly Reports to the United States Securities and Exchange Commission.

3   213.   In its 2022 Form 10-K, Meta reported total advertising revenue of $15 billion in the

4   United States and Average Revenue Per User of $58.77 for the fourth quarter of 2022.
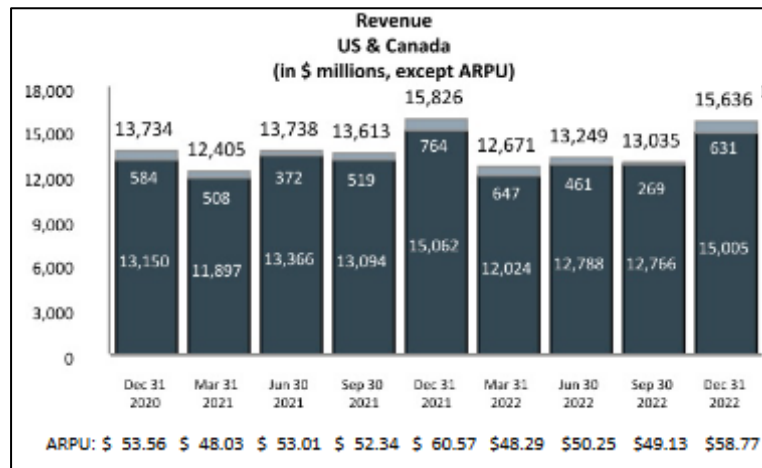
13   214.   Several companies have products through which they pay consumers for a license

14   to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all

15   companies that pay for browsing history information.

16   215.   Meta itself has paid users for their digital information, including browsing history.

17   Until 2019, Meta ran a "Facebook Research" app through which it paid $20 a month for a license

18   to collect browsing history information and other communications from consumers between the

19   ages 13 and 35.

20   216.   Because Americans typically do not want to sell their individually identifiable

21   health information for any purpose and it is illegal to even share it without express, written

22   authorization, there are fewer open markets for a license to collect or sell individually identifiable

23   health information for non-health purposes than other types of data. However, black markets do

24   exist for such data. It has been reported that health data can be "more expensive than stolen credit

25   card numbers" on black markets.[36]

26

27   [36] Aarti Shahani, *The Black Market For Stolen Health Care Data*, NPR: All Tech Considered
     (Feb. 13, 2015 4:55 am ET), https://www.npr.org/sections/alltechconsidered/
28   2015/02/13/385901377/the-black-market-for-stolen-health-care-data.

I.   Meta has acknowledged that targeted health advertising is not appropriate, but provides Pixel-based "work-arounds" for its health care providers and covered entities

217.   Meta has publicly acknowledged that targeted advertising based on health information is not appropriate.

218.   On April 10, 2018, Meta CEO Mark Zuckerberg testified in a joint hearing before the United States Senate Committees on Commerce and Judiciary. During the hearing, Zuckerberg had the following exchange with Senator Edward Markey:[37]

> Sen. Markey: In response to Sen. Blumenthal's pointed questions, you refused to answer whether Facebook should be required by law to obtain clear permission from users before selling or sharing their personal information. So I'm going to ask it one more time. Yes or no. Should Facebook get clear permission from users before selling or sharing sensitive information about your *health*, your finances, your relationships? Should you have to get their permission?
>
> Zuckerberg: Senator, *we do require permission* to use the – the system, and to – to put information in there, and for – *for all the uses of it*. I want to be clear. We don't sell information. So regardless of whether could get permission to do that, that's just not a thing …we're going to do.

219.   In the same hearing, Zuckerberg was asked by Sen. Mazie Hirono what assurances Zuckerberg could give that targeting based on sensitive categories, such as race, was "going to stop?" Zuckerberg responded by stating that Meta had "removed the ability to exclude ethnic groups and other sensitive categories from ad targeting. So that just isn't a feature that's even available anymore."

220.   Yet again in the same hearing, Zuckerberg was unable or unwilling to directly answer a question during the hearing from Sen. Roger Wicker whether Meta could track someone's browsing activity even when there were logged off of Facebook.[38]

---

[37] C-Span, *Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection* (April 10, 2018), https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection&event=443543&playEvent, at 2:23:53-2:30:02.

[38] *Id.* at 1:06:11-106:59.

1

2

3

4

5

6

7

8

9

    <u>Sen. Wicker</u>: One other thing: There have been reports that Facebook can track a user's Internet browsing activity, even after that user has logged off of the Facebook platform. Can you confirm whether or not this is true?

    <u>Zuckerberg</u>: Senator – I – I want to make sure I get this accurate, so it would probably be better to have my team follow up afterwards.

    <u>Sen. Wicker</u>: You don't know?

    <u>Zuckerberg</u>: I know that the – people use cookies on the Internet, and that you can probably correlate activity between – between sessions. We do that for a number of reasons, including security, and including measuring ads to make sure that the ad experiences are the most effective, which, of course, people can opt out of. But I want to make sure that I'm precise in my answer.

10   221.   In March 2020, Meta responded to an article in the Washington Post titled,

11 "Facebook has a prescription: More pharmaceutical ads," by claiming that "Medical history is not

12 used to inform the interest categories that we make available to advertisers, and we prohibit

13 businesses from sending us sensitive health information. Our teams work with health related

14 companies looking to reach their audiences on Facebook and we require them to act in accordance

15 with the law."[39]

16   222.   Upon information and belief, Meta staffers advised CEO Mark Zuckerberg as early

17 as 2020 that Meta should stop using health information for advertising.

18   223.   On November 9, 2021, Meta announced that it was removing the ability to target

19 users on "topics people may perceive as sensitive, such as options referencing causes,

20 organizations, or public figures that relate to health."[40]

21   224.   Meta's announcement was a public relations success.

22   a.   Reuters published a story headlined "Facebook plans to remove thousands

23   of sensitive ad-targeting options" and lead the story with a sentence about

24

25 [39] Nitasha Tiku, *Facebook Has a Prescription: More pharmaceutical ads: Pharmacy companies are ramping up their spending on social media, triggering some patient advocate concerns about privacy*, Washington Post (Mar. 3, 2020 1:15 am), https://www.washingtonpost.com/technology/2020/03/03/facebook-pharma-ads/.

26

27 [40] Meta, *Removing Certain Ad Targeting Options and Expanding Our Ad Controls* (Mar. 30, 2022), https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls.

28

Facebook's "plans to remove detailed ad-targeting options that refer to 'sensitive' topics, such as ads based on interactions with content around … health."[41]

b. The New York Times published a similar story with a similar headline, "Meta plans to remove thousands of sensitive ad-targeting categories: Ad buyers will no longer be able to use topics such as health . . . to target people."[42]

c. The Associated Press, CNN, UPI, Wall Street Journal, Forbes, Politico and hundreds of other medical outlets published identical or similar articles, giving Facebook's users the misimpression that Meta would not allow targeted advertising based on health-related topics.

d. Appendix B that contains headlines, links, and quotations from articles published by just eight of these outlets as a result of Meta's public announcement.

225. The Wall Street Journal reported that Meta's decisions relating to health involved CEO Mark Zuckerberg: "Meta … said it would eliminate micro-targeting options for advertisers on topics related to … sensitive issues, a reversal for the company after CEO Mark Zuckerberg overruled staffers who called for tougher restrictions on such practices. Starting Jan. 19, the company will no longer allow advertisers to highly personalize their messages to users on topics including politics, race, health, and sexual orientation, the company said Tuesday."[43]

---

[41] Elizabeth Culliford, *Facebook plans to remove thousands of sensitive ad-targeting options*, Reuters (Nov. 9, 2021), https://www.reuters.com/technology/facebook-removes-target-options-advertisers-some-topics-2021-11-09/.

[42] Mike Isaac & Tiffany Hsu, *Meta plans to remove thousands of sensitive ad-targeting categories*, N.Y. Times (Nov. 9, 2021), https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html.

[43] Jeff Horowitz, *Facebook-Parent Meta Limits Ad Targeting for Politics and Other Sensitive Issues: CEO Mark Zuckerberg Had Overruled Staffers Last Year When They Pushed for Similar Changes*, The Wall Street Journal (Nov. 9, 2021 4:34 pm), wsj.com/articles/facebook-parent-meta-bans-targeting-for-political-ads-11636488053.

CONSOLIDATED CLASS ACTION COMPLAINT

1   226.   Despite the impression that it was prohibiting targeting based on health, in fact, Meta informed advertisers they could still use "website custom audiences and lookalike" to "help reach people who have already engaged with a business or group's website or products."[44] In the case of health care providers and covered entities, the "people who have already engaged" are patients.

227.   According to Meta, "A lookalike audience uses an existing Custom Audience you select for its source audience. To create a lookalike audience, our system leverages information such as demographics, interests, and behaviors from your source audience to find new people who share similar qualities. When you use a lookalike audience, your ad is delivered to that audience of people who are similar to (or 'look like') your existing customers."[45]

///

///

///

///

///

///

///

///

///

///

///

///

///

///

---

[44] Meta, *Removing Certain Ad Targeting Options and Expanding Our Ad Controls* (Mar. 30, 2022), https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls.

[45] Meta Business Help Center, *About Lookalike Audiences* (2023), https://www.facebook.com/business/help/164749007013531?id=401668390442328.

1   228.   Meta publishes guidance for brands in the health and pharmaceutical industry

2 (which includes health care providers and covered entities).[46] As seen in the image below, Meta's

3 2022 guidance for health-related advertising instructs that targeting "Lookalikes of Meta Pixel"

4 created the best results:

5

6   229.   In August 2022, Meta published a white paper on its Health page addressing how
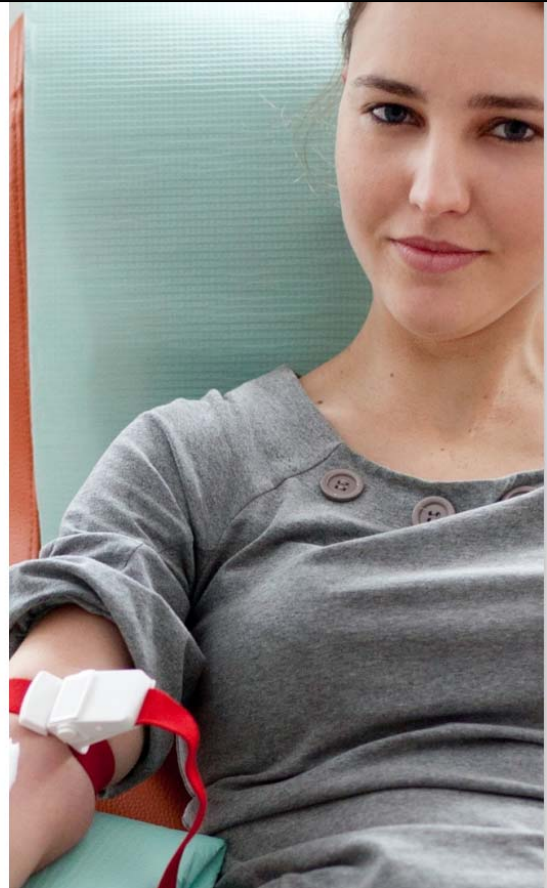
20   229.   In August 2022, Meta published a white paper on its Health page addressing how

21 "to uncover alternative targeting strategies" for health-related targeted advertising. The study

22 advised that "Lookalike Audiences" of "Meta Pixel signals" were a cost-efficient replacement.[47]

23   230.   In other words, while eliminating targeting based on health-interest categories,

24 Meta simultaneously encouraged health care providers and other covered entities to increase their

---

[46] *Id.*

[47] Meta, *Enabling privacy and personalization in health advertising* (2022),
https://www.facebook.com/business/industries/health (choose "Learn more" under "STUDY:
Enabling privacy and personalization in health advertising").

1   use of the Meta Pixel, allowing Meta to continue to collect individually identifiable health

2   information about patients.

3   231.   The Meta Health division publishes videos that it uses to encourage health care

4   providers and other covered entities to use the Pixel for health-based advertising. The page for

5   https://www.facebook.com/business/industries/consumer-goods/healthcare contains hyperlinks to

6   three videos designed to aid health care Partners to send patient information to Meta:

21   / / /

22   / / /

23   / / /

24   / / /

25   / / /

26   / / /

27   / / /

28   / / /

CONSOLIDATED CLASS ACTION COMPLAINT

232.   In its video on the topic of "compliance," Meta advises advertisers how they can (1) block commenters on their Meta pages; (2) add additional product safety information into an ad; and (3) comply with Meta's "restrictions" on health advertising and still target ads to Facebook users based on their health status.[48] This video does not address HIPAA, the CMIA, or other health privacy laws or regulations. However, it does provide Meta's health care Partners with instructions on how to work their way around Meta's health advertising policies.
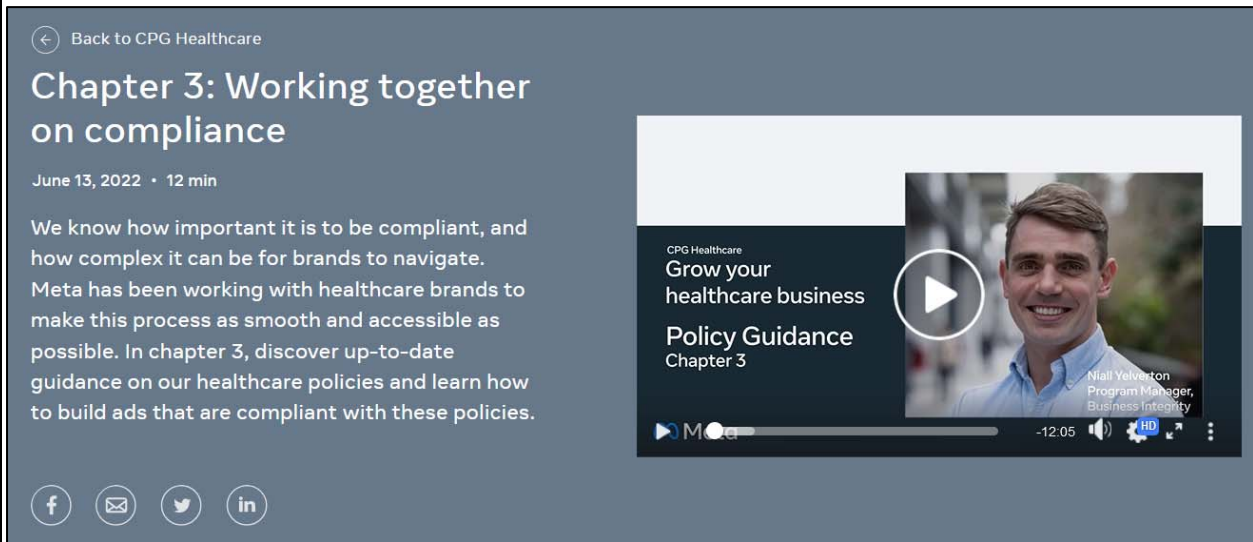
233.   Meta's Niall Yelverton begins the video by explaining that it is the third and "final part of our series on why Meta and its platforms are the right places for your healthcare brands and how we can help you make the most of them."

234.   To help avoid Meta's restrictions, Meta offers to "pre-review your ad to help it get through the approval process. The earlier we can be a part of the creative conversations, the better." By doing so, Meta takes an active role in the content of ads shown on its platform.

235.   Meta tells advertisers:

> It's okay to describe or show a product or service that you want to promote, but you need to make sure your ads don't contain any content that talks about or implies personal attributes. This includes direct or indirect comments about a person such as their name, race, age, or even medical conditions, both mental and physical. You can't use words like 'you' or pose a question and you can't reference

---

[48] Meta, *Chapter 3: Working together on compliance* (June 13, 2022), https://www.facebook.com/business/inspiration/video/healthcare-chapter-3.

1   other in relation to a personal characteristic. For example, 'meet others who suffer from cancer' because you can't imply that you

2   know anything personal about the person that you're targeting.

3   236.   Meta then illustrates the differences between compliant and non-compliant text for

4   targeted ads based on health. Under Meta's rules, it would not be acceptable for an ad targeting

5   people with diabetes or depression to ask, "Do you have diabetes?" or "Depression getting you

6   down? Get help now." But it would be acceptable to target people with bulimia, depression, or

7   diabetes with ads that state, "Bulimia counseling available;" "Depression counseling;" or "New

8   diabetes treatment available."

"Compliant" Personal Health Targeting	"Non-Compliant" Personal Health Targeting
Diabetes treatment available.	Do you have diabetes?
Depression counseling.	Depression getting you down? Get help now.
Bulimia counseling available.	

12   237.   Meta provides advertisers with a PowerPoint slide to emphasize the point:
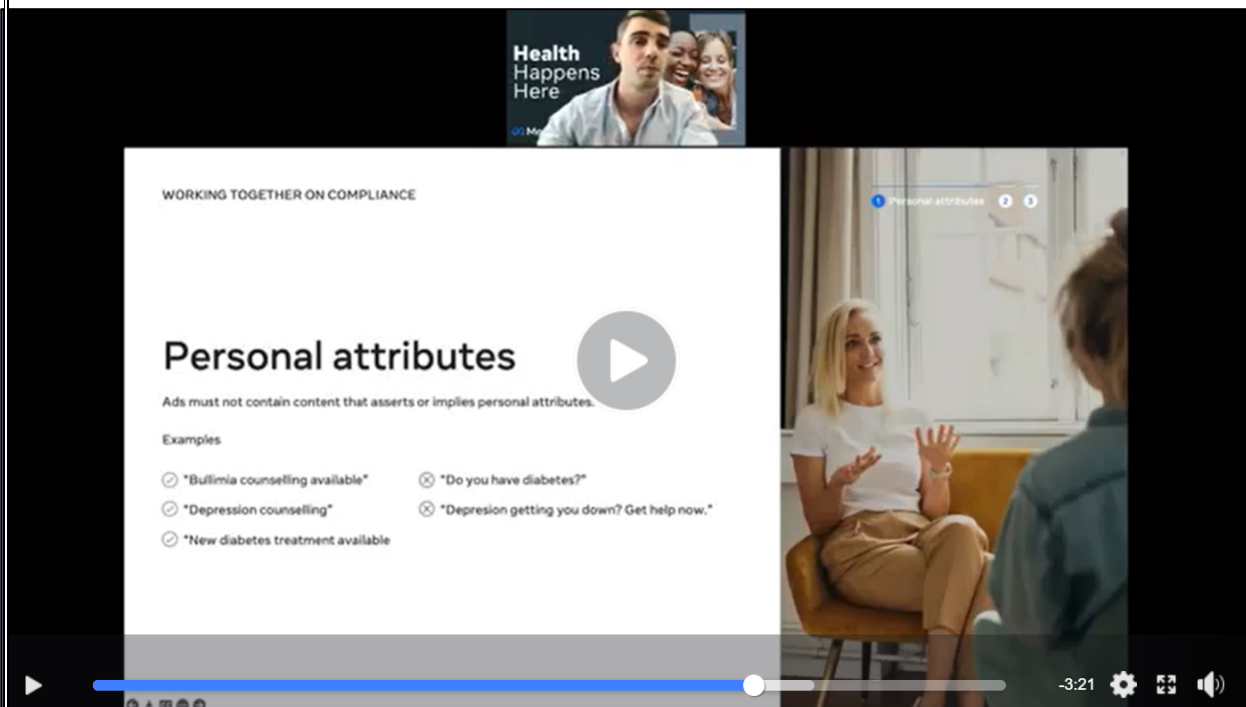
26   238.   Meta's distinctions do nothing to protect the health information of Facebook users.

27   239.   The purpose of Meta's ads policies is not to prevent ad targeting based on health.

28   ///

240.   Meta's ad policies merely mask the fact that Meta is permitting advertisers to target Facebook users based on health information such as bulimia, depression, and diabetes.

241.   The purpose of Meta's ad policies is to make it more difficult for Facebook users to understand that Meta is permitting advertisers to target them based on individually identifiable health information.

242.   As discussed above, Meta actively encourages health care providers and covered entities to install the Meta Pixel on their websites and applications, even though the type of information collected by the Meta Pixel on a health care provider or covered entity's website and application will foreseeably include HIPAA-protected information and information protected by the California Medical Information Act.

243.   Meta actively encourages health care providers and covered entities to create custom audiences and lookalike audiences based on data they have collected from the Meta Pixel, even though that data will foreseeably include HIPAA-protected information and information protected by the California Medical Information Act.

244.   As demonstrated by Meta's course of conduct, knowledge and statements, Meta intends to induce health care providers and covered entities to install the Meta Pixel, collect patient medical data, and share that data with Facebook without authorization.

245.   Meta engages in this scheme in order to make money.

246.   Meta earns additional revenue selling advertisements to health care providers and covered entities who target custom audiences and lookalike audiences based on data containing individually identifiable health information collected through the Meta Pixel.

247.   Meta also earns additional revenue because health care providers and covered entities buy more Meta advertisements due to the health care providers and covered entities being able to share protected health information with Meta without authorization.

248.   Meta saves money, and thus earns unjust profits, by refusing to spend money on systems and procedures that would stop health care providers and covered entities from sharing protected health information with Meta without authorization.

/ / /

CONSOLIDATED CLASS ACTION COMPLAINT

J. **Meta can identify health care provider webpages where the Pixel is redirecting patients' health information to Meta without patients' consent.**

249.   One of Meta's Business Tools, the Facebook Crawler, "crawls the HTML of an app or website …. The crawler gathers, caches, and displays information about the app or website, such as its title, description, and thumbnail image." Meta instructs developers to "[e]nsure that your app or website allows the Facebook Crawler to crawl the privacy policy associated with your app or website."[49]

250.   Meta could use the Facebook Crawler to identify all or practically all significant webpages where the Pixel is deployed by health care providers or covered entities.

251.   Federal law requires every health care provider or covered entity to "prominently post its [HIPAA] notice on the website and make the notice electronically available through the website." 45 C.F.R. § 164.520(c)(3).

252.   Meta could use the Facebook Crawler to identify websites with the required HIPAA notice because the notice must include the phrase, "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THAT INFORMATION." 45 C.F.R. § 164.520(b)(i).

253.   Meta could have used the Facebook Crawler at any point in the past to have identified and prevented health information from being collected via the Pixel.

254.   Meta can identify all web developers and marketers to whom it provides services through the Meta Health division.

255.   Upon information and belief, Meta maintains content classifications or taxonomies (sometimes called "verticals"), including health classifications, for each "Partner" and webpage from which Meta acquires Pixel information.

256.   Meta is capable of using its own internal content classifications to identify health content that it is acquiring through the Pixel without authorization.

---

[49] Meta, *Meta for Developers: The Facebook Crawler* (2023), https://developers.facebook.com/docs/sharing/webmasters/crawler.

257.   The digital advertising industry maintains standards for content classifications or taxonomies (sometimes referred to as "verticals") that are typically used for ad targeting. Industry "Content Taxonomy" standards are published by the Interactive Advertising Bureau, a trade group consisting of more than 700 companies (including Meta) that develops technical standards and solutions for the ad tech industry. The full standards are available at: https://iabtechlab.com/standards/content-taxonomy/ and https://iabtechlab.com/wp-content/uploads/2022/06/Content-Taxonomy-v3.0-Final.xlsx. The IAB "Content Taxonomy" standards include, but are not limited to the following categories: medical health, blood disorders, bone and joint conditions, brain and nervous system disorders, cancer, dental health, diabetes, digestive disorders, ENT conditions, endocrine and metabolic diseases, hormonal disorders, menopause, thyroid disorders, eye and vision conditions, foot health, heart and cardiovascular diseases, infectious diseases, lung and respiratory health, mental health, reproductive health, birth control, infertility, pregnancy, sexual health, skin and dermatology, sleep disorders, substance abuse, medical tests, pharmaceutical drugs, surgery, and vaccines.

258.   Even if Meta did not have its own internal content classification systems, it could easily use the IAB Content Taxonomy classifications utilized by others in the ad tech industry to identify Pixel transmissions that it does not have authorization to acquire.

K.   Meta has been required to thoroughly police itself since at least 2011 by consent decrees governing the company's conduct.

259.   On July 27, 2012, the Federal Trade Commission entered an order pursuant to a Consent Agreement with Meta, wherein it was ordered and agreed that, until July 27, 2032 twenty years from the most recent date that the United States or the FTC files a complaint alleging any violation of the order, whichever comes later, Meta "shall not misrepresent in any manner, expressly, or by implication, the extent to which it maintains the privacy or security of covered information [defined as "information from or about an individual consumer, including name, address, email address, phone number, IP address, User ID or other persistent identifier, physical location, or any information combined with any of the above], including, but not limited to:"

a.   Meta's "collection or disclosure of any covered information";

1   b.   "The extent to which a consumer can control the privacy of any covered

2   information"; and

3   c.   "The steps Respondent takes or has taken to verify the privacy or security

4   protections that any third party provides."

5   260.   Meta also agreed to "establish and implement, and thereafter maintain, a

6 comprehensive privacy program that is reasonably designed to (1) address privacy risks related to

7 the development and management of new and existing products and services for consumers; and

8 (2) protect the privacy and confidentiality of covered information. Such program, the content and

9 implementation of which must be documented in writing, shall contain controls and procedures

10 appropriate to [Meta's] size and complexity, the nature and scope of [Meta's] activities, and the

11 sensitivity of the covered information, including:

12   a.   "Designation of an employee or employees to coordinate and be responsible

13   for the privacy program;"

14   b.   "the identification of reasonably foreseeable, material risks, both internal

15   and external, that could result in [Meta's] unauthorized collection, use, or

16   disclosure of covered information and an assessment of the sufficiency of

17   any safeguards in place to control these risks. At a minimum, this privacy

18   risk assessment should include consideration of risks in each area of

19   relevant operation, including, but not limited to: (1) employee training and

20   management, including training on the requirements of this order; and (2)

21   product design, development, and research."

22   c.   "the design and implementation of reasonable controls and procedures to

23   address the risks identified through the privacy risk assessment, and regular

24   testing or monitoring of the effectiveness of those controls or procedures;"

25   d.   "the development and use of reasonable steps to select and retain service

26   providers capable of appropriately protecting the privacy of covered

27   information they receive from Respondent and requiring service providers,

28

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

1   by contract, to implement and maintain appropriate privacy protections for

2   such covered information;" and

3   e.   "the evaluation and adjustment of [Meta's] privacy program in light of the

4   results of the testing and monitoring required …. any material changes to

5   [Meta's] operations or business arrangements, or any other circumstances

6   that [Meta] knows or has reason to know may have a material impact on the

7   effectiveness of the privacy program."

8   261.   Upon implementation of the privacy program, Meta agreed to "obtain initial and

9   biennial assessments and reports ('Assessments') from a qualified, objective, independent third-

10   party professional, who uses procedures and standards generally accepted in the progression."

11   Each Assessment was required to "set for the specific privacy controls" implemented during the

12   reporting period, "explain how such privacy controls are appropriate to [Meta's] size and

13   complexity, the nature and scope of [Meta's] activities, and the sensitivity of the covered

14   information;" "explain how the privacy controls meet or exceed the protections" required by the

15   Order; and "certify that the privacy controls are operating with sufficient effectiveness to provide

16   reasonable assurance to protect the privacy of covered information and that the controls have so

17   operated throughout the reporting period." Each Assessment is provided to the Associate Director

18   of Enforcement in the Bureau of Consumer Protection at the Federal Trade Commission.

19   262.   Meta is further required to maintain records of:

20   a.   "All widely disseminated statements by [Meta] or its representatives that

21   describe the extent to which [Meta] maintains and protects the privacy,

22   security, and confidentiality of any covered information, including, but not

23   to, any statement related to a change in any website or service controlled by

24   [Meta] that relates to the privacy of such information, along with all

25   materials relied upon in making such statements, and a copy of each

26   materially different privacy setting made available to users;"

27   / / /

28   / / /

1

2

3

      b.   "All consumer complaints directed at [Meta] or forwarded by [Meta] to a third party, that relate to the conduct prohibited by this order and any responses to such complaints;"

4

5

      c.   "Any documents, prepared by or on behalf of [Meta] that contradict, qualify, or call into question [Meta's] compliance with this order;"

6

7

8

9

10

11

      d.   "Each materially different document relating to [Meta's] attempt to obtain the consent of users referred to [in the Order], along with documents and information sufficient to show each user's consent; and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time [Meta] has attempted to obtain and/or been required to obtain such consent;" and

12

13

14

15

      e.   "All materials relied upon to prepare the Assessment, whether prepared by or on behalf of [Meta], including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment."

16

17

18

19

   263.   On or about April 27, 2020, the FTC Modified its Prior Order and issued a new order to which Facebook consented and which was approved by Judge Timothy J. Kelly in the District Court of Columbia. The Decision and Order modifying the prior order added the following provisions:

20

21

22

23

24

      a.   The update defined a "Covered Incident" to mean "any instance in which [Meta] has verified or otherwise confirmed that the Covered Information of 500 or more Users was or was likely to have been accessed, collected, used, or shared by a Covered Third Party in violation of [Meta's] Platform Terms."

25

26

27

28

      b.   "Covered Information" had a substantially similar definition as the previous order except that it added Social Security numbers, driver's licenses, financial account information, credit or debit information, dates of birth, and biometric information.

CONSOLIDATED CLASS ACTION COMPLAINT

c. "Covered Third Party" was defined to include "any individual or entity that uses or receives Covered Information obtained by or an behalf of [Meta] outside of a User-initiated transfer of Covered Information as part of a data portability protocol or standard."

d. Meta is legally required to "[a]ssess and document, at least once every twelve months, internal risks in each area of its operation [including] partnerships with Covered Third Parties … to the privacy, confidentiality, or Integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of such information. [Meta] shall further assess and document internal and external risks as described above as they related to a Covered Incident, promptly following verification or confirmation of such an incident, not to exceed thirty (30) days after the incident is verified or otherwise confirmed."

e. Meta is legally required to "design, implement, maintain, and document safeguards that control for the material internal and external risks identified by [Meta] [with] [e]ach safeguard … based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information."

f. "Specifically with respect to [Meta's] collection, use, or sharing of Covered Information in any new or modified product, service, or practice, such safeguards shall include: … a privacy review that assesses the risks to privacy, confidentiality, and Integrity of the Covered Information, the safeguards in place to control such risks, and the sufficiency of the User notice, and, if necessary, consent; and documenting a description of each reviewed product, service, or practice that was ultimately implemented, any safeguards being implemented to control for the identified risks; and the decision or recommendation made as a result of the review."

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

g. "For each new or modified product, service or practice that presents a material risk to privacy, confidentiality, or Integrity of the Covered Information … producing a written report that describes: the types of Covered Information that will be collected, and how that Covered Information will be used, retained, and shared; the notice provided to users, and the mechanisms, if any, by which Users will consent to, the collection of their Covered Information, and the purposes for which such information will be used, retained, or shared by Respondent; any risks to the privacy, confidentiality, or Integrity of the Covered Information; existing safeguards that would control for the identified risks … and whether any new safeguards would be needed; and any other known safeguards or other procedures that would mitigate the identified risks to the privacy, confidentiality, and Integrity of the Covered Information that were not implemented, such as minimizing the amount or type(s) of Covered Information that is collected, used, and shared, and each reason that those alternatives were not implemented."

h. Meta "must submit a report within thirty (30) days following [Meta's] verification or confirmation of a Covered Incident" to its Assessor and the Federal Trade Commission.

i. Meta must "create" an "Independent Privacy Committee" consisting of Independent Directors that "shall meet with the Assessor at least quarterly."

264. Meta received notice of suits relating to hospitals' unauthorized use of the Meta Pixel *at least as early as* August of 2020.

265. When Meta received notice of the litigation against hospitals based on those hospitals unauthorized use of the Meta Pixel on their websites, it was required by the FTC Consent Decree to produce a "Covered Incident" report.

266. Despite having outside notice of a Covered Incident, Meta took no action to actually require health care providers or covered entities to obtain the right to share patient information

CONSOLIDATED CLASS ACTION COMPLAINT

1   with Meta before doing so. Instead, Meta continued to encourage health care providers and covered

2   entities to use the Meta Pixel and other Meta tools to share individually identifiable health

3   information with Meta for the purpose of "inspiring" health care marketers and providers to "think

4   about how we can really disrupt health and how we market to patients."

5   **L.**   **Meta uses health information it acquires without authorization for**

6   **commercial gain.**

7   267.   Plaintiffs action arises out of Meta's unauthorized acquisition of the health

8   information, regardless of how Meta subsequently used or did not use the information.

9   268.   Plaintiffs incorporate by reference the paragraphs in Appendix A demonstrating

10   how Plaintiffs' expert Richard Smith was served ads based on health information after visiting

11   health entity websites relating to the health information that appeared in the ads. Appendix A ¶¶

12   187-191.

13   269.   For example, within two hours of exchanging communications with the health

14   entity Hartford Healthcare about ulcerative colitis, Smith was shown an ad relating to ulcerative

15   colitis in his Facebook video feed. Appendix A ¶¶ 189-190.

16   270.   Upon information and belief, Meta maintains a history of every ad that it has shown

17   to Plaintiffs and Class members on and off of Meta's social media sites, including on Meta

18   properties and the Facebook Audience Network through which Meta serves ads to Facebook users

19   on non-Meta websites.

20   271.   Meta "generate[s] substantially all of [its] revenue from advertising."[50]

21   272.   Upon information and belief, Meta annually receives billions of dollars of unearned

22   advertising sales revenue from Meta heath care Partners who are targeting Facebook users based

23   on their health information.

24   273.   Meta does not publicly report revenues by advertiser categories or sectors.

25   However, in 2019, the Washington Post reported that "[s]pending on Facebook mobile ads alone

26

27

---

28   [50] Meta 2022 Annual Report at 17.

1   by pharmaceutical and health-care brands reached nearly a billion dollars in 2019, nearly tripling

2   over two years, according to Pathmatics, an advertising analytics company."[51]

3   **V.**   **CLASS ACTION ALLEGATIONS**

4   274.   Plaintiffs bring this case as a class action on behalf of themselves and the following

5   Class:

6
7
> All Facebook users whose health information was obtained by Meta
> from their health care provider or covered entity.

8   275.   Excluded from the Class are the Court and its personnel and Meta and its officers,

9   directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and

10   any entity in which any of them have a controlling interest.

11   276.   <u>Numerosity</u>. The members of the Class are so numerous and geographically diverse

12   that joinder is impracticable.

13   277.   <u>Commonality and Predominance</u>. One or more common questions of law or fact

14   are apt to drive resolution of the case and predominate over any questions affecting solely

15   individual Class members. The common questions include but are not limited to:

16   a.   Whether the Meta Terms of Service, Data Policy, and Cookies Policy
17   constitute a valid contract between Meta and users;

18   b.   Whether Meta failed to "require" health care providers and covered entities
19   to have the right to share patient data with Meta before deploying the Meta
20   Pixel on their websites;

21   c.   Whether Meta "employs dedicated teams around the world" to "detect
22   potential misuse" of the Meta Pixel as alleged in this action;

23   d.   Whether Meta "works with external service providers, partners, and other
24   relevant entities" to "detect potential misuse" of the Meta Pixel as alleged
25   in this action;

26

27

---

28   [51] Nitasha Tiku, *Facebook has a prescription: More pharmaceutical ads*, Washington Post (Mar. 4, 2020 at 1:15 am), washingtonpost.com/technology/2020/03/03/facebook-pharma-ads/.

e.   Whether Meta "develop[s] advanced technical systems" to "detect potential misuse" of the Meta Pixel as alleged in this action;

f.   Whether Meta acquired the content of Class members' health communications;

g.   Whether Meta breached its contract with Class members;

h.   Whether Class members validly authorized Meta to acquire their individually identifiable health information;

i.   Whether Meta's acquisition of Class members' communications with their health care providers and covered entities occurred contemporaneous to their making;

j.   Whether Meta's collection of individually identifiable health information through placement of the Meta Pixel on health care provider and covered entity websites is highly offensive;

k.   Whether Meta's placement of the _fbp cookie as a disguised first-party cookie through health care provider and covered entity websites is highly offensive;

l.   Whether Meta's placement of the _fbp cookie on Plaintiffs and Class members computing devices as a disguised first-party cookie through health care provider and covered entity websites was a trespass to chattels;

m.   Whether Meta failed to implement reasonable security procedures and practices in collecting Class members' individually identifiable health information;

n.   Whether the information at issue has economic value; and

o.   Whether Meta unjustly profited from its collection of patient portal, appointment, and phone call information.

278.   <u>Typicality</u>. Plaintiffs' claims are typical of the claims of other Class members because they arise out of the same common course of conduct by Meta and are based on the same legal theories.

1   279.   Adequacy. Plaintiffs will fairly and adequately protect the interests of Class

2   members. Plaintiffs have retained competent and capable attorneys who are experienced trial

3   lawyers with significant experience in complex and class action litigation, including privacy law.

4   Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the

5   Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests

6   that are contrary to or that conflict with the interests of the Class.

7   280.   Superiority. Plaintiffs and Class members have suffered and will continue to suffer

8   harm and damages due to Meta's unlawful conduct. Absent a class action, however, most Class

9   members are unlikely to be aware of Meta's conduct and would find the cost of litigating their

10   claims prohibitive. Class treatment is superior to multiple individual suits or piecemeal litigation

11   because it conserves judicial resources, promotes consistency and efficiency of adjudication,

12   provides a forum for small claimants, and deters illegal activities. There will be no significant

13   difficulty in the management of this case as a class action.

14   **VI.   TOLLING**

15   281.   Any applicable statute of limitations has been tolled by Meta's knowledge and

16   concealment of the misrepresentations and omissions alleged herein. Through no fault or lack of

17   diligence, Plaintiffs and Class members were deceived and could not reasonably discover Meta's

18   deception and unlawful conduct.

19   282.   Plaintiffs and Class members did not discover and did not know of any facts that

20   would have caused a reasonable person to suspect that Meta was acting unlawfully. Meta's alleged

21   representations were material to Plaintiffs and Class members at all relevant times. Within the time

22   period of any applicable statutes of limitations, Plaintiffs and Class members could not have

23   discovered Meta's alleged wrongful conduct through the exercise of reasonable diligence.

24   283.   At all relevant times, Meta was, and still is, under a continuous duty to disclose to

25   Plaintiffs and Class members the true nature of the disclosures being made and the lack of an actual

26   "requirement" before Plaintiffs' and Class members' data was shared with Meta.

27   284.   Meta knowingly, actively, affirmatively or negligently concealed the facts alleged

28   herein. Plaintiffs and Class members reasonably relied on Meta's concealment.

285. For these reasons, all applicable statutes of limitation have been tolled based on the discovery rule and Meta's concealment, and Meta is estopped from relying on any statutes of limitations in defense of this action.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

(Breach of Contract)

By Plaintiffs on behalf of themselves and the Class

286. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

287. Meta requires Facebook users like Plaintiffs and Class members to click a box indicating that, "By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy."

288. "Click-wrap agreements" like Meta's agreement with users are valid and binding contracts.

289. The Meta Terms of Service are binding on Meta and Plaintiffs and Class members.

290. The Meta Data Policy is binding on Meta and Plaintiffs and Class members.

291. The Meta Cookies Policy is binding on Meta and Plaintiffs and Class members.

292. The Meta Terms of Service state that "the 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."

293. Meta's services to Plaintiffs and Class members are not free.

294. In exchange for access to Meta and its services, Plaintiffs and Class members agree to provide Meta with a limited set of personal information and the ability to show the Plaintiffs advertisements based on the contractually bargained-for limited set of personal information that the parties agree can be acquired and used by Meta.

295. The "personal information" that Plaintiffs' and Class members' must pay for access to Meta's services is not unlimited but instead is bound by the promises made by Meta in the documents that make up the Meta contract with its users.

/ / /

296.   For example, by signing up for Meta, it is undisputed that Plaintiffs have not agreed to pay for the service by permitting Meta to collect their Social Security number. Nor have Plaintiffs or class members agreed to pay for Meta's services with their health information.

297.   The "data license" that Meta promised Plaintiffs' and Class members it would charge for use of Meta products did not include any health information about the Plaintiffs or Class members that Meta would collect from their health entities (i.e. health care providers, health insurers, pharmacies, business associates, and prescription drug companies).

298.   The "data license" that Meta promised it would charge for use of Meta's products expressly excluded any information that Meta's Partners did not have the right to share with Meta.

299.   Meta makes the following contractual promises to Plaintiffs and Class members.

300.   From approximately April 19, 2018 to July 2022, Meta promised: [52]

    a.   "[P]ublishers can send us information through Meta Business Tools they use, including … the Meta pixel. These partners provide information about your activities off of our products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use our services—whether or not you have an account or are logged into our Products. ….We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information. …Partners receive your data when you visit or use their services or through third parties they work with. *We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us*." (emphasis added).

    b.   "Our mission is to give people the power to build community and bring the world closer together. To help advance this mission, we provide the Products and services described to you below … Combat harmful conduct and protect and support our community: … *We employ dedicated teams*

---

[52] The promise that Meta required Partners to have "lawful rights" to "share your data before providing any data to us" did not exist prior to April 19, 2018.

CONSOLIDATED CLASS ACTION COMPLAINT

1   *around the world and develop advanced technical systems to detect misuse*

2   *of our Products*, harmful conduct towards others, and situations where we

3   may be able to help support or protect our community. *If we learn of content*

4   *or conduct like this, we will take appropriate action – for example*, offering

5   help, *removing content, blocking access to certain features, disabling an*

6   *accoun*t, or contacting law enforcement." (emphasis added).

7   301.   Meta changed the language of its policies on July 22, 2022. But these changes (1)

8   reiterated the previous promises; and (2) included additional promises.

9   302.   From July 22, 2022 to present, the Meta contract has promised:

10   a.   "How do we collect or receive this information from partners? Partners use

11   our Business Tools … to share information with us. These partners collect

12   your information when you visit their site or app or use their services, or

13   through other businesses or organizations they work with. *We require*

14   *Partners to have the right to collect, use, and share your information before*

15   *giving it to us*." (emphasis added).

16   b.   "Our mission is to give people the power to build community and bring the

17   world closer together. To help advance this mission, we provide the

18   Products and services described to you below … Combat harmful conduct

19   and protect and support our community: … *We employ dedicated teams*

20   *around the world, work with external service providers, partners and other*

21   *relevant entities and develop advanced technical systems to detect potential*

22   *misuse of our Products, harmful conduct towards others, and situations,*

23   *where we may be able to help support or protect our community, including*

24   *to respond to user reports of potentially violating content. If we learn of*

25   *content or conduct like this, we may take appropriate action based on our*

26   *assessment that may include – notifying you, offering help, removing*

27   *content, removing or restricting access to certain features, disabling an*

28   *account, or contacting law enforcement*." (emphasis added).

1   303.   A Facebook user who read Meta's contracts would be shocked to learn that Meta

2   was collecting their individually identifiable health information from their health entities,

3   including their health care providers, pharmacies, health insurers, business associates, and

4   prescription drug companies.

5   304.   Meta breached its promises by not requiring health provider and covered entity

6   Partners to have the right to share Plaintiffs' and Class members' health information associated

7   with their health entities before sharing their patient status and other identifiable health

8   information, including their creation of patient portal accounts, access to patient portals,

9   appointments, phone calls, and communications with health entities about their doctors, diagnoses,

10   conditions, treatments, prescription drugs, health insurance, symptoms, patient status, and other

11   information alleged herein.

12   305.   Meta materially breached its contract with its users by failing to require that

13   healthcare providers or covered entities gain the necessary patient authorizations before sharing

14   any patient protected health information with Facebook.

15   306.   Meta materially breached its contract with its users by failing to require that health

16   care providers or covered entities submit records of the necessary patient authorization to

17   Facebook before sharing any patient protected health information with Facebook.

18   307.   Meta took no action to require its health Partners to not send Plaintiffs' and Class

19   members' health information without consent.

20   308.   Meta did not implement any technological blocks to prevent Meta's acquisition of

21   health information without authorization.

22   309.   Meta did not implement any monitoring system to prevent Meta's acquisition of

23   health information without authorization.

24   310.   Despite promising in its Terms of Service that it employs or contracts with external

25   providers to "detect potential misuse" and has developed advanced technical systems for that

26   purpose, Meta does not actively review which websites its Pixel is installed on to determine

27   whether its Pixel is transmitting Plaintiffs' and Class members' health information to Meta.

28   / / /

311.   Instead of requiring Partners to have the right to share health information before doing so, Meta actively encouraged and solicited health entity Partners to share health information without regard or concern to whether the Partner had the right to share such information.

312.   The following chart outlines the promises and Meta's breach:

Promise	Breach
"We require Partners to have the right to … share your information before giving it to us."	Meta does not require Partners to have the right to share health information with Meta before giving it to Meta.
"We employ dedicated teams around the world … to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community.	Meta does not employ dedicated teams to prevent its unauthorized acquisition of health information. To the contrary, Meta employs dedicated teams to encourage health entities to share health information with Meta that the health entities lack rights to share.
"We … develop advanced technical systems to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we will take appropriate action – for example … removing content, blocking access to certain features, disabling an account, or contacting law enforcement."	Meta has developed advanced technical systems to detect potential misuse of certain products and is fully capable of using those systems to detect Pixel Partners from which it is acquiring health information without authorization. However, Meta has not used those systems to stop acquiring such information and has not taken appropriate action to prevent health entities from sharing health information with Meta in the absence of the right to do so.
"We work with external service providers, partners, and other relevant entities … to detect potential misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community, including to respond to user reports of potentially violating content."	Meta does not work with external service providers, Partners, or other relevant entities to detect potential misuse of sending health information to Meta through the Pixel without the right to do so. To the contrary, Meta works with Partners to help those Partners avoid the meaningless restrictions Meta places on ads that are targeted to health. As shown above, Meta teaches health entities how to avoid its "restrictions" on personalized health targeted ads by removing certain words that would give users the idea that the ad was specifically targeted to them, all the while continuing to target ads to specific users based on personal attributes, including health

Promise	Breach
	information that Meta obtained from Partners that did not have the right to share that information.

313.   An implied contract also exists between Meta and Plaintiffs and Class members that Meta will not conspire with others to violate Plaintiffs' and Class members' legal rights to privacy in their individually identifiable health information.

314.   The patient health information that Meta obtains in breach of the contract includes:

a.   Plaintiffs' and Class members' identifiers including, but not limited to, email addresses, IP addresses, persistent cookie identifiers, device identifiers, and browser fingerprint information;

b.   the dates and times that Plaintiffs and Class members register for their health care provider or covered entity patient portals;

c.   the dates and times that Plaintiffs and Class members log in and log out of their health care provider or covered entity patient portals;

d.   the content of communications that Plaintiffs and Class members exchange inside their health care providers' patient portals immediately before logging out of the portals;

e.   the content of Plaintiffs' and Class members' communications relating to appointments with their health care providers;

f.   the content of Plaintiffs' and Class members' communications about their appointments, providers, treatments, conditions, symptoms, diagnoses, prognoses, payment information, prescription drugs, and insurance information with their providers and other covered entities; and

g.   Plaintiffs' and Class members' status as patients of their health care providers or covered entities.

315.   In breaching these promises, Meta overcharged Plaintiffs and Class members by collecting data in excess of the "data license" that was agreed upon in the contract between Meta and its users. Specifically, Meta expressly promised that its "data license" would not include

1   information that its Partners do not have the right to share with Meta, but Meta charged the

2   additional data license anyway.

3   316.   As a direct and proximate results of Meta's breach of contract, Plaintiffs and Class

4   members did not receive the full benefit of the bargain, and instead received services from Meta

5   that were less valuable than described in their contract with Meta. Plaintiffs and Class members,

6   therefore, were damaged in an amount at least equal to the difference in value between that which

7   was promised and Facebook's partial, deficient, and/or defective performance.

8   317.   Meta's breach caused Plaintiffs and Class members the following damages:

9   a.   Nominal damages;

10   b.   The interruption or preclusion of Plaintiffs' and Class members' ability to

11   communicate with their health care providers or covered entities on their

12   health care providers' or covered entity websites;

13   c.   The diminution in value of Plaintiffs' and Class members' protected health

14   information;

15   d.   Plaintiffs' and Class members' inability to use their computing devices for

16   the purpose of communicating with their health care providers or other

17   covered entities;

18   e.   The loss of privacy due to Meta making sensitive and confidential

19   information such as patient status and appointments that Plaintiffs and Class

20   members intended to remain private no longer private;

21   f.   Meta took something of value from Plaintiffs and Class members and

22   derived benefits therefrom without Plaintiffs' and Class members'

23   knowledge or informed consent and without sharing the benefit of such

24   value;

25   g.   The deprivation of the benefit of the bargain in that Meta's contract stated

26   that the data license for its services did not include health information from

27   health Partners who did not have the right to share information with Meta,

28

1   but Meta actually took more data than the contractually agreed-upon

2   amount;

3   h.   The amount that Meta should have spent implementing controls to ensure

4   that patient data was not provided to Meta without the patients' consent;

5   and

6   i.   Plaintiffs and Class Members suffered an invasion of privacy. Plaintiffs and

7   Class Members seek compensatory damages for the invasion of their

8   privacy.

9   318.   For Meta's breaches, Plaintiffs and Class members seek nominal damages, general

10   damages, compensatory damages, consequential damages, unjust enrichment, restitution, and any

11   other relief the Court deems just.

12   **SECOND CLAIM FOR RELIEF**

13   **(Breach of the Duty of Good Faith and Fair Dealing)**

14   **By Plaintiffs on behalf of themselves and the Class**

15   319.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and

16   succeeding paragraphs.

17   320.   A valid contract exists between Meta and Plaintiffs and Class members.

18   321.   The contract specifies that California law governs the parties' relationship.

19   322.   Meta prevented Plaintiffs and Class members from receiving the full benefit of the

20   contract by intercepting the content of their individually identifiable health information.

21   323.   In doing so, Meta abused its power to define terms of the contract, including:

22   a.   The meaning of the term "require" in Meta's promise that it would "require"

23   Partners to have the right to share Plaintiffs' and Class members' data with

24   Meta before doing so and then taking no action to prevent health care

25   providers or covered entities from sharing protected health information

26   without Plaintiffs' and Class members' valid consent.

27   b.   The meaning of the term "appropriate action" in the promise "[i]f we learn

28   of content or conduct like [potential misuse of our products, harmful

1
2
3
4
5
6
7
8
9
10
11

conduct towards others, and situations where we may be able to help support or protect our community] we will take appropriate action – for example … removing content, blocking access to certain features, disabling an account, or contacting law enforcement." Based on Meta's other statements, "appropriate action" for health entities' unauthorized sharing of health information with Meta should have include removing the Pixel from the offending health websites; blocking the offending developers from deploying the Pixel on other health websites; disabling offending developers' accounts; and contacting health regulatory authorities if specific health entities persisted in the violations. Yet, Meta took none of these actions.

12   324.   Meta did not act fairly and in good faith.

13   325.   Rather than "requiring" Partners to obtain the right to share health information,
14   Meta actively solicited them, through the Meta Health division, to share health information
15   regardless of whether they had the right to do so.

16   326.   Rather than taking "appropriate action" upon discovering that health information
17   was being shared with Meta by health entities without the right to do so, Meta actively solicited
18   their further disclosures and advertising revenue, through the Meta Health division.

19   327.   In doing so, Meta frustrated and undercut Plaintiffs' and Class Members'
20   contractual rights, and unfairly interfered with Plaintiffs' and Class Members' rights under the
21   parties' contract.

22   328.   As a direct and proximate results of Meta's breach of contract, Plaintiffs and Class
23   Members did not receive the full benefit of the bargain, and instead received services from Meta
24   that were less valuable than described in their contract with Meta. Plaintiffs and Class Members,
25   therefore, were damaged in an amount at least equal to the difference in value between that which
26   was promised and Facebook's partial, deficient, and/or defective performance.

27   329.   Meta's breach caused Plaintiffs and Class members the following damages:

28   a.   Nominal damages;

1

 b. The interruption or preclusion of Plaintiffs' and Class members' ability to

2

   communicate with their health care providers or covered entities on their

3

   health care providers' or covered entity websites;

4

 c. The diminution in value of Plaintiffs' and Class members' protected health

5

   information;

6

 d. The inability to use their computing devices for the purpose of

7

   communicating with their health care providers or covered entities;

8

 e. The loss of privacy due to Meta making sensitive and confidential

9

   information such as patient status and appointments that Plaintiffs and Class

10

   members intended to remain private no longer private;

11

 f. Meta took something of value from Plaintiffs and Class members and

12

   derived benefits therefrom without Plaintiffs' and Class members'

13

   knowledge or informed consent and without Meta sharing the benefit of

14

   such value;

15

 g. The deprivation of the benefit of the bargain in that Meta's contract stated

16

   that the data license for its services did not include health information from

17

   health Partners who did not have the right to share information with Meta,

18

   but Meta actually took more data than the contractually agreed-upon

19

   amount; and

20

 h. Plaintiffs and Class Members suffered an invasion of privacy. Plaintiffs and

21

   Class Members seek compensatory damages for the invasion of their

22

   privacy.

23

  330. For Meta's breaches, Plaintiffs and Class members seek nominal damages, general

24

damages, compensatory damages, consequential damages, unjust enrichment, restitution, and any

25

other relief the Court deems just.

26

/ / /

27

/ / /

28

/ / /

1

THIRD CLAIM FOR RELIEF

2

(Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*)

3

By Plaintiffs on behalf of themselves and the Class

4   331.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and

5   succeeding paragraphs.

6   332.   The Electronic Communications Privacy Act ("ECPA") prohibits the intentional

7   interception of the contents of any electronic communication. 18 U.S.C. § 2511.

8   333.   The ECPA protects both the sending and receipt of communications.

9   334.   The ECPA provides a private right of action to any person whose electronic

10   communications are intercepted. 18 U.S.C. § 2520(a).

11   335.   Meta intentionally intercepted electronic communications that Plaintiffs and Class

12   members exchanged with their health care providers and covered entities through the Meta Pixel

13   installed on the health care providers' and covered entity websites.

14   336.   The transmissions of data between Plaintiffs and Class members and their health

15   care providers or covered entities qualify as communications under the ECPA. 18 U.S.C. §

16   2510(12).

17   337.   Meta contemporaneously acquired Plaintiffs' and Class members' communications

18   with their health care providers or covered entities.

19   338.   The intercepted communications include:

20   a.   the content of Plaintiffs' and Class members' registrations for patient

21   portals, including clicks on buttons to "Register" or "Signup" for portals;

22   b.   the content Plaintiffs' and Class members' log in and log out of patient

23   portals, including clicks to "Sign-in," "Log-in," "Sign-out," or "Log-out";

24   c.   the contents of communications that Plaintiffs and Class members

25   exchange inside patient portals immediately before logging out of the

26   portals;

27   d.   the contents of Plaintiffs' and Class members' communications relating to

28   appointments with medical providers;

CONSOLIDATED CLASS ACTION COMPLAINT

e.   the contents of Plaintiffs' and Class members' communications relating to specific health care providers, conditions, treatments, diagnoses, prognoses, prescription drugs, symptoms, insurance, and payment information;

f.   Full-string URLs that contain any information concerning the substance, purport, or meaning of patient communications with their health entities.

339.   For example, interception of hartfordhospital.org/services/digestive-health/conditions-we-treat/colorectal-small-bowel-disorders/ulcerative-colitis involves "content."

340.   The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a.   The cookies Meta uses to track Plaintiffs' and Class members' communications;

b.   Plaintiffs' and Class members' browsers;

c.   Plaintiffs' and Class members' computing devices;

d.   Meta's web-servers;

e.   The web-servers of health care providers' or covered entity webpages where the Meta Pixel is present; and

f.   The Meta Pixel source code Meta deploys to acquire Plaintiffs' and Class members' communications.

341.   Meta is not a party to Plaintiffs' and Class members' communications with their health care providers or covered entities.

342.   Meta receives the content of Plaintiffs' and Class members' communications through the surreptitious redirection of those communications from the Plaintiffs' and Class members' computing devices.

343.   Plaintiffs and Class members did not consent to Meta's acquisition of their patient portal, appointment, and phone call communications with their health care providers or covered entities.

/ / /

/ / /

CONSOLIDATED CLASS ACTION COMPLAINT

1   344.   Meta did not obtain legal authorization to obtain Plaintiffs' and Class members'

2   communications with their health care providers or covered entities relating to communications

3   with their health entities.

4   345.   Meta did not require any health entity to obtain the lawful rights to share the content

5   of Plaintiffs' and Class members' communications relating to patient portals, appointments, and

6   phone calls.

7   346.   Any purported consent that Meta received from health care providers or covered

8   entities to obtain the content of Plaintiffs' and Class members' communications was not valid.

9   347.   In acquiring the content of Plaintiffs' and Class members' communications relating

10   to patient portals, appointments, and phone calls, Meta had a purpose that was tortious, criminal,

11   and designed to violate state constitutional and statutory provisions including:

12   a.   The unauthorized acquisition of individually identifiable health

13   information is tortious in and of itself regardless of whether the means

14   deployed to acquire the information violates the Wiretap act or any

15   subsequent purpose or use for the acquisition. Meta intentionally

16   committed a tortious act by acquiring individually identifiable health

17   information without authorization to do so.

18   b.   The unauthorized acquisition of individually identifiable health

19   information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of

20   any subsequent purpose or use of the individually identifiable health

21   information. Meta intentionally violated 42 U.S.C. 1320d-6 by

22   intentionally acquiring individually identifiable health information without

23   authorization.

24   c.   A violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a

25   criminal offensive punishable by fine or imprisonment with *increased*

26   *penalties* where "the offense is committed with intent to sell, transfer, or

27   use individually identifiable health information for commercial advantage

28   [or] personal gain." Meta intentionally violated the enhanced penalty

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

CONSOLIDATED CLASS ACTION COMPLAINT

provision of 42 U.S.C. § 1320d-6 by acquiring the individually identifiable health information "with intent to sell transfer or use" it for "commercial advantage [or] personal gain."

d.   A knowing intrusion upon Plaintiffs' and Class members' seclusion;

e.   Trespass upon Plaintiffs' and Class members' personal and private property via the placement of an _fbp cookie associated with the domains and patient portals for their health care providers and covered entities on Plaintiffs' and Class members' personal computing devices;

f.   Violation of the California Unfair Competition Law;

g.   Violation of the California Consumer Legal Remedies Act;

h.   Violation of the California Constitution's right to privacy;

i.   Violation of various state health privacy statutes, including but not limited to the California Confidentiality of Medical Information Act; the California Consumer Privacy Protection Act; and the California Consumer Privacy Act;

j.   Violation of various state computer privacy and property statutes, including but not limited to the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502;

k.   Violation of Cal. Penal Code § 484 for statutory larceny; and

l.   Violation of the federal wire fraud statutes at 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy), which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

348.   The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with the intent to defraud; (3) that is was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used. The attempt version of the wire fraud statute provides that "[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.." 18 U.S.C. § 1349.

349.   Meta's scheme or artifice to defraud in this action consists of:

a.   the false and misleading statements and omissions in its contract documents set forth above, including the statements and omissions recited in the breach of contract and breach of good faith and fair dealing claims above;

b.   the false and misleading statements and omissions that Meta made to the public regarding health advertising on Meta platforms, including Meta's announcement in November 2021 that it was "Removing Certain Ad Target Options and Expanding Our Ad Controls," an announcement which led directly to news articles from prominent news organizations headlined "Facebook plans to remove thousands and sensitive ad-targeting options;" and descriptions such as that Meta "plans to remove detailed ad-targeting options that refer to 'sensitive' topics, such as ads based on interactions with content around … health" and "ad buyers will no longer be able to use topics such as health … to target people;"

c.   The placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie of the patients' health care providers or covered entities rather than a third-party cookie from Meta.

350.   The "property" involved consists of Plaintiffs' and Class members':

a.   Property rights to the confidentiality of their individually identifiable health information and their right to determine whether such information remains

CONSOLIDATED CLASS ACTION COMPLAINT

1 confidential and exclusive right to determine who may collect and/or use

2 such information for marketing purposes; and

3   b.   Property rights to determine who has access to their computing devices.

4 351. Meta acted with the intent to defraud in that it willfully invaded and took the Named

5 Plaintiffs' and Class members' property:

6   a.   With knowledge that (1) the health care providers or covered entities did

7 not have the right to share such data; (2) courts had determined that a health

8 care providers' use of the Meta Pixel gave rise to claims for invasion of

9 privacy and violations of state criminal statutes; (3) a reasonable Facebook

10 user would not understand that Meta was collecting their individually

11 identifiable health information based on their activities on their health care

12 providers' or covered entity websites; (4) "a reasonable Facebook user

13 would be shocked to realize" the extent of Meta's collection of individually

14 identifiable health information described herein and in the Smith

15 Declaration attached as Exhibit A; (5) a Covered Incident had occurred

16 which required a report to be made to the FTC pursuant to Meta's consent

17 decrees with the FTC; and (6) the subsequent use of health information for

18 advertising was a further invasion of such property rights in making their

19 own exclusive use of their individually identifiable health information for

20 any purpose not related to the provision of their health care;

21   b.   Upon information and belief, Meta CEO Mark Zuckerberg was informed

22 by Meta employees in 2020 that Meta should cease health-based advertising

23 activities, but Zuckerberg overruled those employees;

24   c.   Meta was also aware of the misleading nature of the articles generated by

25 its November 2021 press release regarding health information;

26   d.   Meta's CEO was also aware enough of the sensitive nature of publicity of

27 the fact that Meta is tracking users off the Meta platform on any website

28

1   that he either refused or was unable to answer direct, simple questions about

2   Meta's general tracking when asked in a Congressional hearing; and

3   e.   With the intent to (1) acquire Plaintiffs and Class members' individually

4   identifiable health information without their authorization and without their

5   health care providers or covered entities obtaining the right to share such

6   information; (2) use the Named Plaintiffs' and Class members' individually

7   identifiable health information without their authorization; and (3) gain

8   access to the Named Plaintiffs' and Class members' personal computing

9   devices through the 'fbp' cookie disguised as a first-party cookie.

10   352.   It was reasonably foreseeable to Meta that its scheme and artifice to defraud would

11 involve interstate wire communications and, in fact, interstate wire communications were used in

12 the carrying out of Meta's scheme and artifice to defraud.

13   353.   Meta knew its conduct would be highly offensive, as evidenced by its

14 announcement on November 9, 2021, that it would no longer allow targeted advertising based on

15 health, yet Meta continued to use the Meta Pixel to acquire health information from health care

16 providers' or covered entity webpages for advertising purposes.

17   354.   Any purported consent provided by Meta's health care provider or covered entity

18 "Partners" using the Meta Pixel had a purpose that was tortious, criminal, and in violation of state

19 constitutional and statutory provisions because it constitutes:

20   a.   A knowing intrusion into a private matter that would be highly offensive

21   to a reasonable person;

22   b.   A violation of 42 U.S.C. § 1320d-6, which is a criminal offense punishable

23   by fine or imprisonment and that includes increased penalties where "the

24   offense is committed with intent to sell, transfer, or use individually

25   identifiable health information for commercial advantage [or] personal

26   gain."

27   c.   Trespass;

28   d.   Breach of fiduciary duty; and

1   e.   A violation of various state health privacy and computer privacy statutes,

2   including the CCPA.

3   355.   A Maryland state court found that the facts alleged in this complaint stated a claim

against health care provider MedStar for intrusion upon seclusion, publication of private facts, and

violation of the Maryland Wiretap Act. *Doe v. Medstar*, Case No. 24-C-20-000591 (Baltimore

City, Maryland).

7   356.   Courts around the country have uniformly held that a health care provider's use of

the Meta Pixel on its website without patient authorization is actionable in tort or contract or a

statutory violation. *See Doe v. Mercy Health*, Case No. A 2002633 (Hamilton County, Ohio); *Doe*

v. Partners, Case No. 1984-CV-01651 (Suffolk County, Massachusetts); *Doe v. Sutter Health*,

Case No. 34-2019-00258072-CU-BT-GDS (Sacramento County, California); *Doe v. University*

Hospitals, Case No. CV-20-9333357 (Cuyahoga County, Ohio); *Doe v. Sutter Health*, Case No.

34-2019-00258072-CU-BT-GDS (Sacramento County, California).

14   357.   Meta has been aware since at least 2020 of these court decisions finding that a

health care provider's use of the Meta Pixel without valid patient consent is actionable, yet Meta

continued to acquire patient communications and information via the Pixel.

17   358.   Meta's violations of the ECPA were willful and intentional and caused Plaintiffs

and Class members the following damages:

19   a.   The interruption or preclusion of Plaintiffs' and Class members' ability to

           communicate with their health care providers or covered entities on their

           health care providers' and covered entity websites;

22   b.   The diminution in value of Plaintiffs' and Class members' protected health

           information;

24   c.   The inability to use their computing devices for the purpose of

           communicating with their health care providers;

26   d.   The loss of privacy due to Meta making sensitive and confidential

           information such as patient status and appointments that Plaintiffs and Class

           members intended to remain private no longer private; and

CONSOLIDATED CLASS ACTION COMPLAINT

e.   Meta took something of value from Plaintiffs and Class members and derived benefits therefrom without Plaintiffs' and Class members' knowledge or informed consent and without Meta sharing the benefit of such value.

359.   For Meta's violations set forth above, Plaintiffs and Class members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any profits made by [Meta] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

360.   Unless enjoined, Meta will continue to commit the violations of law alleged here. Plaintiffs want to continue to communicate with their healthcare providers and covered entitities through online platforms but have no practical way of knowing if their communications are being intercepted by Meta, and thus continue to be at risk of harm from Meta's conduct.

361.   For example, Meta told the Court that the way to avoid Meta's collection of health information was for a patient to call their health care provider. Yet, the Meta Pixel is designed so that Meta receives their data even when a patient calls their provider.

362.   Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members seek monetary damages for the *greater of* (i) the sum of the actual damages suffered by the plaintiff and any profits made by Meta as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

FOURTH CLAIM FOR RELIEF

(Violation of California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632)

By Plaintiffs on behalf of themselves and the Class

363.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

364.   The California Invasion of Privacy Act (CIPA) is codified at Cal. Penal Code §§ 630-638. The Act begins with its statement of purpose: "The legislature hereby declares that advances in science and technology have led to the development of new devices and techniques

CONSOLIDATED CLASS ACTION COMPLAINT

1 for the purpose of eavesdropping upon private communications and that the invasion of privacy

2 resulting from the continual and increasing use of such devices and techniques has created a

3 serious threat to the free exercise of personal liberties and cannot be tolerated in a free and

4 civilized society." Cal. Penal Code § 630.

5   365.   Cal. Penal Code § 631(a) provides, in pertinent part: "Any person who, by means

6 of any machine, instrument, or contrivance, or in any other manner …. willfully and without the

7 consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to

8 read, or to learn the contents or meaning of any message, report, or communication while the

9 same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any

10 place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to

11 communicate in any way, any information so obtained, or who aids, agrees with, employs, or

12 conspires with any person or persons to lawfully do, or permit, or cause to be done any of the

13 acts or things mentioned above in this section, is punishable by a fine not exceeding two

14 thousand five hundred dollars."

15   366.   Cal. Penal Code § 632 provides, in pertinent part, that it is unlawful for any

16 person to "intentionally and without the consent of all parties to a confidential communication,"

17 to "use[] [a] recording device to … record the confidential communication." As used in the

18 statute, a "confidential communication" is "any communication carried on in circumstances as

19 may reasonably indicate that any part to the communication desired it to be confined to the

20 parties thereto."

21   367.   Meta is a "person" within the meaning of CIPA §§ 631 and 632.

22   368.   Meta did not have the prior consent of all parties to learn the contents of or record

23 the confidential communications at issue, as Plaintiffs and Class members did not provide

24 express prior consent to Meta's wiretapping of their communications with health care providers

25 and covered entities.

26   369.   Meta is headquartered in California, designed and effectuated its scheme to track

27 the patient communications at issue here from California, and has adopted California substantive

28 law to govern its relationship with its users.

1   370.   At all relevant times, Meta's conduct alleged herein was without the authorization

2   and consent of the Plaintiffs and Class members.

3   371.   Meta's actions were designed to learn or attempt to learn the meaning of the

4   contents of Plaintiffs' and Class members' communications exchanged with their health care

5   providers and covered entities.

6   372.   Meta's learning of or attempt to learn the contents of patient communications

7   occurred while they were in transit or in the process of being sent or received.

8   373.   Unless enjoined, Meta will continue to commit the violations of law alleged here.

9   Plaintiffs continue to want to communicate with their health care providers and covered entities

10   through online platforms but have no practical way of knowing if their communications are

11   being intercepted by Meta, and thus continue to be at risk of harm from Meta's conduct.

12   374.   Plaintiffs and class members seek all relief available under Cal. Penal Code

13   § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

FIFTH CLAIM FOR RELIEF

(Intrusion Upon Seclusion—Common Law)

By Plaintiffs on behalf of themselves and the Class

17   375.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and

18   succeeding paragraphs.

19   376.   By collecting and disseminating the contents of Plaintiffs' and Class members'

20   communications with their health care providers and covered entities without their knowledge,

21   Meta intentionally intruded into a realm in which Plaintiffs and Class members have a reasonable

22   expectation of privacy.

23   377.   Plaintiffs and Class members enjoyed objectively reasonable expectations of

24   privacy in their communications with their medical providers and covered entities relating to the

25   respective patient portals,appointments, and health information and communications based on:

26   a.   The health care providers' or covered entities' status as their health care

27   providers or a covered entity and the reasonable expectations of privacy that

28   attach to patient-provider relationships;

1   b.   HIPAA;

2   c.   the ECPA;

3   d.   Meta's promise that it would "require" Partners to have the right to share

4   their data before Meta would collect it; and

5   e.   California medical and computer privacy laws

6   378.   Furthermore, Plaintiffs and Class Members maintained a reasonable expectation of

7 privacy when providing their patient medical data to their health care providers and covered

8 entities and when communicating with their health care providers and covered entities online.

9   379.   Patient medical data is widely recognized by society as sensitive information that

10 cannot be shared with third parties without the patients' consent.

11   380.   For example, public polling shows that, "[n]inety-seven percent of Americans

12 believe that doctors, hospitals, labs and health technology systems should not be allowed to share

13 or sell their sensitive health information without consent." [53]

14   381.   Meta obtained unwanted access to Plaintiffs' and Class members' data, including

15 but not limited to their patient status, the dates and times Plaintiffs and Class members logged in

16 or out of patient portals, and the communications Plaintiffs and Class members exchanged while

17 logged in to patient portals.

18   382.   Meta's intrusion was also accomplished by placing the "fbp" cookie on the

19 Plaintiffs' and Class members' computing devices through the web-servers of the Plaintiffs' and

20 Class members' health care providers.

21   383.   By disguising the third-party "fbp" cookie as a first-party cookie from the

22 Plaintiffs' health care providers or covered entities, Meta ensure that it could hack its way around

23 attempts that Plaintiffs and Class members might make to prevent Meta's tracking through the use

24 of cookie blockers.

25

26

27 [53] *Poll: Huge majorities wants control over health info,* Healthcare Finance (Nov. 10, 2020),
https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-
28 info.

CONSOLIDATED CLASS ACTION COMPLAINT

384.   In designing the 'fbp' cookie as a disguised first-party cookie, Meta was aware that, like other websites that include sections where users' sign in to an account, any health care provider or covered entity website with a patient portal would require first-party cookies to be enabled for a patient to access the patient portal or other username / password protected "secure" part of the health care provider's website.

385.   With first-party cookies being required for use of a patient portal and the Meta "fbp" cookie disguised as a first-party cookie, Meta was able to implant its tracking device on the computing devices of the Named Plaintiffs and Class members even where Plaintiffs or Class members made attempts to stop third-party tracking through the use of cookie blockers.

386.   Meta's deployment of the "fbp" cookie as a third-party cookie disguised as a first-party cookie that is placed on Plaintiffs and Class members' computing devices is a highly offensive intrusion upon seclusion regardless of whether any information was further re-directed from the Plaintiffs or Class members computing devices to Meta.

387.   Meta's intrusion into Plaintiffs' and Class members' privacy would be highly offensive to a reasonable person, namely because it occurred without Plaintiffs' and Class members' consent or knowledge.

388.   Meta's intrusion caused Plaintiffs and Class members the following damages:

      a.   Nominal damages;

      b.   The interruption or preclusion of Plaintiffs' and Class members' ability to communicate with their health care providers or covered entities on their health care providers' or covered entity websites;

      c.   The diminution in value of Plaintiffs' and Class members' protected health information;

      d.   The inability to use their computing devices for the purpose of communicating with their health care providers or covered entities;

      e.   The loss of privacy due to Meta making sensitive and confidential information such as patient status and appointments that Plaintiffs and Class members intended to remain private no longer private; and

f.   Meta took something of value from Plaintiffs and Class members and derived benefits therefrom without Plaintiffs' and Class members' knowledge or informed consent and without Meta sharing the benefit of such value.

389.   Meta's intrusion into Plaintiffs' and Class members' seclusion was with oppression, fraud, or malice.

390.   For Meta's intrusion into their seclusion, Plaintiffs and Class members seek actual damages, compensatory damages, restitution, disgorgement, general damages, nominal damages, unjust enrichment, punitive damages, and any other relief the Court deems just.

SIXTH CLAIM FOR RELIEF

(California Constitutional Invasion of Privacy)

By Plaintiffs on behalf of themselves and the Class

391.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

392.   Article I, section 1 of the California Constitution provides:

> *All people* are by nature free and independent and *have inalienable rights. Among these are* enjoying and defending life and liberty, acquiring, possessing, and protecting property, and *pursuing and obtaining* safety, happiness, and *privacy*.

Cal. Const. art. I, § 1 (emphasis added).

393.   Plaintiffs and Class members have both an interest in precluding the dissemination and misuse of their health information by Meta, and in making intimate personal decisions and communicating with health providers and covered entities without observation, intrusion, or interference by Meta.

394.   Plaintiffs and Class members had no knowledge and did not consent or authorize Meta to obtain the content of their communications with their health care providers and covered entities as described herein.

395.   Plaintiffs and Class members enjoyed objectively reasonable expectations of privacy surrounding communications with their health care based on the health care providers' and

1 covered entity's status as their health care providers or covered entities subject to federal and state

2 health privacy laws, and the reasonable expectations of privacy that attach to such relationships,

3 as evidenced by (among other things) federal laws such as HIPAA and California law protecting

4 health information, and Meta's promise that it would "require" its Partners to have the right to

5 share their data before Meta would collect it.

6   396.   Plaintiffs' and Class members' claims include but are not limited to Meta's

7 unauthorized access to following private facts:

8   a.   that Plaintiffs and Class members are patients of the various health care

9   providers and covered entities;

10   b.   the dates and times Plaintiffs and Class members clicked to sign up, log in,

11   or log out of the various health care providers' and covered entity patient

12   portals;

13   c.   the dates and times that Plaintiffs and Class members scheduled

14   appointments;

15   d.   the fact that Plaintiffs and Class members were scheduling appointments

16   with their provider or covered entity;

17   e.   Plaintiffs' and Class members' communications with their health care

18   providers or covered entity;

19   f.   Other health information associated with Plaintiffs and Class members,

20   including but not limited to doctors, conditions, treatments, prognoses,

21   symptoms, health insurance, and prescription drug information; and

22   g.   Plaintiffs' and Class members' communications exchanged while logged

23   in to a patient portal.

24   397.   In addition to acquiring Plaintiffs' and Class members' health information without

25 authorization, Meta deposited the _fbp cookie on Plaintiffs' and Class members' computing

26 devices by disguising it as a first-party cookie associated with their health care provider or covered

27 entity rather than a Meta cookie.

28 / / /

1   398.   Meta's intrusion upon seclusion with respect to the _fbp cookie occurred the

2 moment that Meta caused the _fbp cookie to be placed on Plaintiffs' and Class members' devices.

3   399.   Meta's conduct was intentional and intruded on Plaintiffs' and Class members'

4 medical communications which constitute private conversations, matters, and data.

5   400.   Meta's conduct in acquiring patient portal, appointment, and other communications

6 would be highly offensive to a reasonable person because:

7   a.   Meta conspired with Plaintiffs' and Class members' health care providers

8   and covered entities to violate a cardinal rule of the provider-patient

9   relationship;

10   b.   Meta's conduct violated federal and state laws designed to protect patient

11   privacy, including HIPAA and the CMIA;

12   c.   Meta's conduct violated the ECPA; and

13   d.   Meta's conduct violated the express promises it made to Plaintiffs and

14   Class members.

15   401.   Plaintiffs and Class members seek all relief available for invasion of privacy claims

16 under the California Constitution, including:

17   a.   Nominal damages;

18   b.   General privacy damages;

19   c.   The interruption or preclusion of Plaintiffs' and Class members' ability to

20   communicate with their health care providers on their health care providers'

21   or covered entity websites;

22   d.   The diminution in value of Plaintiffs' and Class members' protected health

23   information;

24   e.   Plaintiffs and Class members' inability to use their computing devices for

25   the purpose of communicating with their health care providers or covered

26   entities;

27 ///

28 ///

f.   The loss of privacy due to Meta making sensitive and confidential information such as patient status and appointments that Plaintiffs and Class members intended to remain private no longer private; and

g.   Meta took something of value from Plaintiffs and Class members and derived benefits therefrom without Plaintiffs' and Class members' knowledge or informed consent and without Meta sharing the benefit of such value.

<p align="center"><u>SEVENTH CLAIM FOR RELIEF</u></p>

<p align="center">(Negligence per se)</p>

<p align="center">By Plaintiffs on behalf of themselves and the Class</p>

402.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

403.   At all times, Meta had an obligation to comply with all applicable statutes and regulations, including the HIPAA, 42 U.S.C. § 1320d, *et seq.*, and its associated regulations.

404.   Meta is a business associate within the meaning of HIPAA because, via the Meta Pixel, it receives, maintains, and transmits protected health information for regulated purposes, such as data analysis and marketing. 45 CFR §§ 160.103, 164.501, 164.508(a)(3).

405.   HIPAA privacy laws are intended to protect the confidentiality of individuals' health care information, and apply not only to health care providers, but to any entity with access to health care information, the disclosure of which could put an individual's finances or reputation at risk.

406.   Meta's actions as described herein violated HIPAA and its associated regulations.

407.   Meta fails to meet the requirements of 42 U.S.C. § 1320d-6 by knowingly using or causing to be used unique health identifiers and by knowingly obtaining individually identifiable health information relating to Plaintiffs and Class members, including but not limited to:

a.   when Plaintiffs and Class members log in and out of a patient portal;

b.   when Plaintiffs and Class members request or set appointments;

1
     c.   when Plaintiffs and Class members click a number on a website to call their

2
           health care provider;

3
     d.   Plaintiffs' and Class members' Internet Protocol address;

4
     e.   Plaintiffs' and class members' c_user cookie, which can be easily used to

5
           locate that individual's Facebook profile; and

6
     f.   Plaintiffs' and Class members' datr cookie, which identifies the their

7
           specific web browser and is therefore a means of identifying Facebook

8
           users.

9
408.   Meta also fails to meet the requirements of 45 CFR § 164.502(3) by using protected

10
health information obtained via the Meta Pixel for marketing purposes without prior authorization.

11
45 CFR § 164.508(a)(3).

12
409.   Plaintiffs and Class members are within the class of persons that HIPAA is intended

13
to protect.

14
410.   Plaintiffs' and Class members' injuries are the type of harm that HIPAA is intended

15
to prevent.

16
411.   Meta's violations of HIPAA therefore constitute negligence per se.

17
412.   As a direct and proximate result of Meta's violations of HIPAA, Plaintiffs and

18
members of the Class have suffered and continue to suffer serious injuries, including but not

19
limited to:

20
     a.   The loss of privacy of Plaintiffs' protected health information

21
     b.   The interruption or preclusion of their ability to communicate with their

22
           health care providers on their health care providers' websites;

23
     c.   Damaged relationships with their health care providers;

24
     d.   Time and resources expended to investigate and respond to Meta's

25
           violations;

26
     e.   The diminution in value of their protected health information; and

27
     f.   Inability to use their computing devices for the purpose of communicating

28
           with their health care providers.

CONSOLIDATED CLASS ACTION COMPLAINT

1   413.   Meta acted with oppression, fraud, or malice in breaching its obligations to

2   Plaintiffs and Class members.

3   414.   For Meta's negligence, Plaintiffs and Class members seek actual damages, general

4   damages, unjust enrichment, punitive damages, and any other relief the Court deems just.

5   **EIGHTH CLAIM FOR RELIEF**

6   **(Trespass to Chattel)**

7   **By Plaintiffs on behalf of themselves and the Class**

8   415.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and

9   succeeding paragraphs.

10   416.   Plaintiffs and Class members owned, leased, or controlled their computing devices

11   from which they communicated with their medical providers or covered entities.

12   417.   The Meta Pixel tracking source code is designed such that, when Plaintiffs and

13   Class members visit their health care providers' or covered entity websites and patient portals, a

14   cookie named '_fbp' is automatically set upon Plaintiffs' and Class members' computing devices.

15   418.   The '_fbp' cookie is designed to avoid any attempts by Plaintiffs and Class

16   members to block transmissions to Meta via cookies. To accomplish this task, the Meta Pixel

17   tracking source code transmits and commands the '_fbp' cookie to be lodged in Plaintiffs' and

18   Class members' computing devices by asserting that it is a cookie from their health care providers

19   or covered entities.

20   419.   The Meta Pixel lodges the _fbp cookie on Plaintiffs' and Class members'

21   computing devices regardless of whether they have attempted to block third-party cookies.

22   420.   For security purposes, as a rule, Plaintiffs and Class members must enable first-

23   party cookies to use their health care providers' or covered entity patient portals. As a result, every

24   Plaintiff and Class member had the Facebook _fbp cookie lodged on their computing device.

25   421.   Meta placed the _fbp cookie on Plaintiffs' and Class members' computing devices

26   intentionally and without Plaintiffs' and Class members' knowledge or authorization.

27   422.   Meta's placement of the fbp cookie on Plaintiffs' and Class members' computing

28   devices is the modern equivalent of the placement of a bug in someone's telephone or on the desk

1 where their computer sits. Meta's source code, fbp cookie, and the Meta Pixel have taken the place

2 of the "bug," which is why these tools are often called "web bugs."

3   423.   Plaintiffs' and Class members' computing devices derive substantial value from

4 their ability to facilitate communications with their health care providers or covered entities, which

5 is integral to the intended function of their devices.

6   424.   Meta's placement of cookies results in the persistent and unavoidable interception

7 of Plaintiffs' and Class members' communications with their health care providers or covered

8 entities, which deprives Plaintiffs and Class members of the full value of using their computing

9 devices for those communications.

10   425.   Plaintiffs' and Class members' devices are useless for exchanging private

11 communications with health care providers or other covered entities that use the Pixel on their

12 websites, which substantially impairs the condition, quality, and value of Plaintiffs' and Class

13 members' devices.

14   426.   Meta's trespass into Plaintiffs' and Class members' computing devices caused them

15 the following damages:

16   a.   Nominal damages for trespass;

17   b.   The total deprivation of their use of their computing devices to

18   communicate with their health care providers or covered entities.

19   427.   Meta's repeated interception of Plaintiffs' and Class members' health information

20 knowing it was done without consent is evidence of its malicious disregard of Plaintiffs' and Class

21 members' property rights.

22   428.   For Meta's trespass, Plaintiffs and Class members seek nominal damages, actual

23 damages, general damages, unjust enrichment, punitive damages, and any other relief the Court

24 deems just.

25 / / /

26 / / /

27 / / /

28 / / /

NINTH CLAIM FOR RELIEF

(Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*)

By Plaintiffs on behalf of themselves and the Class

429.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

430.   California Business and Professions Code section 17200 ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising …."

431.   Meta has engaged in unlawful, fraudulent, and unfair business acts and practices in violation of the UCL.

432.   Meta has engaged in unlawful acts or practices under section 17200 by its violations of:

      a.   the California Constitution's right to privacy;

      b.   the ECPA and California Penal Code sections 631 and 632;

      c.   HIPAA, including specifically 42 U.S.C. § 1320d-6; and

      d.   California health and computer privacy statutes, including but not limited to the California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502).

433.   Meta has engaged in fraudulent business acts or practices under section 17200 because its misrepresentations and omissions regarding its requirement that businesses have the right to collect, use, and share Plaintiffs' and Class members' data before providing any data to Meta, and Meta's receipt of the confidential information at issue, were intended to, were likely to, and did deceive reasonable consumers such as Plaintiffs and the Class. The information Meta misrepresented and concealed would be, and is, material to reasonable consumers because Meta takes no action to confirm that its Partner businesses have the right to collect, use, and share Plaintiffs' and Class members' data before transmitting patient data to Meta through the Pixel, and Meta receives the confidential information at issue nonetheless.

///

434. Meta has engaged in unfair acts and practices under section 17200 because Meta claims it requires businesses to have the right to collect, use, and share Plaintiffs' and Class members' data before providing any data to Meta, but in reality knows (or should know) that its Pixel tracking tool is being used on health care provider and covered entity websites to contemporaneously redirect Plaintiffs' and Class members' communications without their knowledge or authorization.

435. Meta's actions offend public policy.

436. Meta's conduct, misrepresentations and omissions have also impaired competition within the health care market in that they have prevented Plaintiffs and Class members from making fully informed decisions about whether to communicate online with their health care providers and covered entities and to use their health care providers' and covered entity websites.

437. Plaintiffs and Class members have suffered injuries in fact, including the loss of money and/or property, as a result of Meta's deceptive, unfair, and unlawful practices. Plaintiffs' individually identifiable and health data has value, as demonstrated by Meta's use and sale of it. While only an identifiable "trifle" of injury need be shown, as set forth above Plaintiffs, Class members, and the public at large value their private health information at more than a trifle. The sale of this confidential and valuable information has diminished its value to Plaintiffs and the Class.

438. Meta's actions caused damage to and loss of Plaintiffs' and Class members' property by preventing them from controlling the dissemination and use of their individually identifiable health information and communications.

439. Had Plaintiffs and Class members known that Meta's representation that it requires businesses to have the right to collect, use, and share their data before providing any data to Meta was untrue, Plaintiffs and Class members would not have used their health care providers' or covered entity websites.

440. The wrongful conduct alleged herein occurred, and continues to occur, in the conduct of Meta's business. Meta's wrongful conduct is part of a pattern or generalized course of conduct that is still perpetuated and repeated in the State of California.

441.   Plaintiffs and Class members want to continue using their health care providers' and covered entity websites and patient portals to communicate with their health care providers or covered entities, including but not limited t request and set appointments, and complete other tasks that necessary to access health care services and maintain their health, such as exchange communications about their doctors, treatments, symptoms, and prescription drugs.

442.   If it does not change its practices, Meta will continue to contemporaneously obtain Plaintiffs' and Class members' individually identifiable and health data and communications.

443.   Plaintiffs and Class members will have no way to discern, while using their current or future health care providers' or covered entity websites and patient portals, whether Meta is contemporaneously obtaining their individually identifiable health information and communications.

444.   In addition, because the _fbp cookie masquerades as a first party cookie to evade third party cookie blockers, Plaintiffs and Class members cannot manually block the _fbp cookie so as to protect the confidentiality of their data and communications.

445.   As a result, the threat of future injuries identical to those that Meta has already inflicted on Plaintiffs and the Class is actual and imminent for Plaintiffs and the Class.

446.   Plaintiffs therefore request that the Court enjoin Meta from continuing its deceptive, unfair, and unlawful practices.

447.   Plaintiffs also request that the Court restore to Plaintiffs and the Class, in the form of restitution, any money Meta acquired as a result of its deceptive, unfair and unlawful practices.

448.   The injuries of Plaintiffs cannot be wholly remedied by monetary relief and such remedies at law are inadequate.

TENTH CLAIM FOR RELIEF

(Violation of California Consumer Legal Remedies Act, Cal. Civ. Code § 1780 *et seq.*)

By Plaintiffs on behalf of themselves and the Class

449.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

/ / /

450.   Under the CLRA, "Any consumer who suffers damage as a result of the use or employment by any person of a method, act, or practices declared unlawful by Section 1770 may bring an action against that person to recover or obtain any of the following:" (1) actual damages; (2) an order enjoining the methods, acts, or practices; (3) restitution of property; (4) punitive damages; and (5) any other relief that the court deems proper. Cal. Civil Code § 1780(a).

451.   By stating that it required its Partners to have the right to collect, use and share Plaintiffs' and Class members' information but doing nothing to ensure their rights were protected, Meta violated section 1770(2) of the CLRA by "[m]isrepresenting the source, sponsorship, approval, or certification of goods or services." Cal. Civ. Code § 1770(2).

452.   By making the same representation, Meta violated section 1770(5) of the CLRA by "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

453.   By making the same representation, Meta violated section 1770(14) of the CLRA by "[r]epresenting that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law."

454.   Plaintiffs seek only injunctive relief but reserve the right to amend their complaint to seek monetary relief after providing statutory notice.

ELEVENTH CLAIM FOR RELIEF

(Violation of Cal. Penal Code §§ 484 and 496 – Statutory Larceny)

By Plaintiffs on behalf of themselves and the Class

455.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

456.   California Penal Code section 496(a) prohibits the obtaining of property "in any manner constituting theft."

457.   California Penal Code section 484 defines "theft," and provides that:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false representation or

pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

458. Section 484 thus defines "theft" to include stealing or taking personal property of another or by obtaining property by false pretense.

459. Meta acted in a manner constituting theft and/or false pretense.

460. Meta stole, took, and fraudulently appropriated Plaintiffs' and Class members' individually identifiable health information without their consent.

461. Meta concealed, aided in the concealing, sold and/or utilized Plaintiffs' and Class members' individually identifiable health information for Meta's commercial purposes and financial benefit.

462. Meta knew that Plaintiffs' and Class members' individually identifiable health information was stolen and/or obtained because Meta designed the code that redirected Plaintiffs' and Class members' individually identifiable health information from their health care providers' or covered entity websites to Meta and operated it in a manner that was concealed or withheld from Plaintiffs and Class members.

463. The reasonable and fair market value of the unlawfully obtained individually identifiable health information can be determined in the marketplace and by examining the unjust enrichment Meta received by using the unlawfully collected information for marketing purposes.

464. As a direct and proximate result of Meta's violation of its duty, Plaintiffs and Class members suffered injuries including but not limited to:

      a.   Treble the value of the individually identifiable health information that was stolen, as permitted by Cal. Penal Code § 496(c);

      b.   Treble the amount of general privacy damages from the highly offensive nature of the theft, as permitted by Cal. Penal Code § 496(c);

/ / /

/ / /

1   c.   Treble the loss of value to their computing devices from the inability to use

2   those devices for communicating with their health care providers or covered

3   entities;

4   d.   The costs of bringing suit; and

5   e.   Reasonable attorney's fees.

6   465.   Plaintiffs seek declaratory and injunctive relief, and reserve the right to amend to

7 seek actual or statutory damages if Meta does not cure these violations within 30 days of receiving

8 notice.

9 <div align="center">**TWELFTH CLAIM FOR RELIEF**</div>

10 <div align="center">**(Violation of the California Comprehensive Computer Data Access and Fraud Act, Cal.**</div>

11 <div align="center">**Penal Code § 502)**</div>

12 <div align="center">**By Plaintiffs on behalf of themselves and the Class**</div>

13   466.   Plaintiffs reallege and incorporate by reference each allegation in the preceding and

14 succeeding paragraphs.

15   467.   The California Comprehensive Computer Data Access and Fraud Act ("CDAFA")

16 was enacted to provide protection from "tampering, interference, damage, and unauthorized access

17 to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

18   468.   The CDAFA affords a private right of action to owners of computers, systems,

19 networks, programs, and data who suffer as a result of a violation of the Act. Cal. Penal Code

20 § 502(e)(1).

21   469.   The CDAFA imposes civil liability on anyone who:

22   a.   Knowingly accesses and without permission alters, damages, deletes,

23   destroys, or otherwise uses any data, computer, computer system, or

24   computer network in order to either (A) devise or execute any scheme or

25   artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain

26   money, property, or data. Cal. Penal Code § 502(c)(1);

27   b.   Knowingly accesses and without permission takes, copies, or makes use of

28   any data from a computer, computer system, or computer network, or takes

<div align="center">107   Case No. 3:22-cv-3580-WHO-VKD</div>

1   or copies any supporting documentation, whether existing or residing

2   internal or external to a computer, computer system, or computer network.

3   Cal. Penal Code § 502(c)(2);

4   c.   Knowingly and without permission uses or causes to be used computer

5   services. Cal. Penal Code § 502(c)(3);

6   d.   Knowingly and without permission provides or assists in providing a means

7   of accessing a computer, computer system, or computer network in

8   violation of this section. Cal. Penal Code § 502(c)(6);

9   e.   Knowingly and without permission accesses or causes to be accessed any

10   computer, computer system, or computer network. Cal. Penal Code

11   § 502(c)(7); and

12   f.   Knowingly introduces any computer contaminant into any computer,

13   computer system, or computer network. Cal. Penal Code § 502(c)(8).

14   470.   "Computer services" under the CDAFA "includes, but is not limited to, computer

15 time, data processing, or storage functions, internet services, electronic mail services, electronic

16 message services, or other uses of a computer, computer system, or computer network." Cal. Penal

17 Code § 502(b)(4).

18   471.   "Computer network" is "any system that provides communications between one or

19 more computer systems and input/output devices, including, but not limited to, display terminals,

20 remote systems, mobile devices, and printers connected by telecommunication facilities." Cal.

21 Penal Code § 502(b)(2).

22   472.   "Computer system" is "a device or collection of devices, including support

23 devices…one or more of which contain computer programs, electronic instructions, input data,

24 and output data, that performs functions, including, but not limited to, logic, arithmetic, data

25 storage and retrieval, communication, and control." Cal. Penal Code § 502(b)(5).

26   473.   "Data" is defined as "a representation of information, knowledge, facts, concepts,

27 computer software, or computer programs or instructions" that "may be in any form, in storage

28

CONSOLIDATED CLASS ACTION COMPLAINT

1 media, or as stored in the memory of the computer or in transit or presented on a display device."

2 Cal. Penal Code § 502(b)(8).

3   474.   "Computer contaminant" is defined as "any set of computer instructions that are

4 designed to modify, damage, destroy, record, or transmit information within a computer, computer

5 system, or computer network without the intent of the owner of the information. They include, but

6 are not limited to, a group of computer instructions commonly called viruses or worms, that are

7 self-replicating or self-propagating and are designed to contaminate other computer programs or

8 computer data, consumer computer resources, modify, destroy, record, or transmit data, or in some

9 other fashion usurp the normal operation of the computer, computer system, or computer network."

10 Cal. Penal Code § 502(b)(12).

11   475.   Meta's conduct, described herein, violates Cal. Penal Code §§ 502(c)(1), (2), (3),

12 (6), (7), and (8).

13   476.   Plaintiffs and Class members were the owners or lessees of the computers,

14 computer systems, computer networks, and data described herein.

15   477.   The Pixel constitutes a "contaminant" under the CDAFA because it is designed to,

16 and does, self-propagate to contaminate users' computers, computer systems, and computer

17 networks to record and transmit data that would not otherwise be transmitted in the normal

18 operation of the computers, computer systems, and computer networks.

19   478.   Meta knowingly accessed, used, and caused to be used Plaintiffs' and class

20 Members' data, computers, computer services, and computer networks in that Meta specifically

21 designed the Pixel to surreptitiously place the _fbp cookie on users' computer browsers, which

22 causes the devices' data processing functions and networks to redirect Plaintiffs' and Class

23 members' data to Meta.

24   479.   Meta knowingly introduced the Pixel into Plaintiffs' and Class members'

25 computers, computer systems, and computer networks and provided itself the means of accessing

26 Plaintiffs' and Class members' computers, computer systems, and computer networks in violation

27 of the CDAFA by developing the Pixel and encouraging and providing instructions to health care

28 providers and covered entities on its use and deployment.

480.   Plaintiffs' and Class members' data that Meta redirects through the Pixel includes nonpublic information related to their communications with their health care providers and covered entities, including that Plaintiffs and Class Members registered for and logged into patient portals, scheduled health care appointments, and searched for physicians and information about medical conditions.

481.   Meta makes use of Plaintiffs' and Class members' data to obtain money through advertising.

482.   Meta's use of Plaintiffs' and Class members' data is wrongful in that the use is prohibited by state and federal laws and Meta's own policies, including but not limited to:

  a. the ECPA and Cal. Penal Code §§ 631 & 632;

  b. HIPAA, including specifically 42 U.S.C. § 1320d-6;

  c. various state health and computer privacy statutes, including but not limited to the California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502); and

  d. Meta's Terms of Service, Data Policy, and Cookie Policy.

483.   Meta's use and access of Plaintiffs' and Class members' data, computers, computer services, and computer networks, and Meta's introduction of the Pixel into Plaintiffs' and Class members' computers, computer services, and computer networks is without permission because:

  a. Plaintiffs and Class members never authorized Meta to place the _fbp cookie on their browser or otherwise access or use their data, computers, computer services, and computer networks;

  b. The Pixel was invisible to Plaintiffs and Class members;

  c. Plaintiffs and Class members were unaware that Meta was using the Pixel to surreptitiously access and use their data, computers, computer services, and computer networks;

  d. It was impossible for Plaintiffs and Class members to opt out of or prevent the functionality of the Pixel;

/ / /

1   e.   Meta's own policies prohibit Meta from accessing and using Plaintiffs' and

2   Class members' health information;

3   f.   Meta circumvented technical and code-based barriers to access and use

4   Plaintiffs' and Class members' data, computers, computer services, and

5   computer networks because the Pixel places the _fbp cookie on Plaintiffs'

6   and Class Members' computing devices, which is designed to disguise itself

7   as a cookie from Plaintiffs and their health care providers and covered

8   entities so that Meta can circumvent password-protected patient portals,

9   cookie blockers, and other technical barriers; and

10   g.   Plaintiffs' and Class members' data that Meta accesses and uses is not

11   publicly viewable and only became accessible to Meta through Meta's

12   surreptitious and unauthorized placement of the _fbp cookie on Plaintiffs'

13   and Class members' computing devices.

14   484.   As a result of Meta's violations of CDAFA, Plaintiffs and Class members suffered

15 damages including but not limited to:

16   a.   The interruption or preclusion of their ability to communicate with their

17   health care providers and covered entities on their health care providers'

18   and covered entity websites;

19   b.   The diminution in value of their protected health information;

20   c.   The inability to use their computing devices for the purpose of

21   communicating with their health care providers and covered entities.

22   485.   Meta's violations of CDAFA were willful, fraudulent, or oppressive.

23   486.   For Meta's violations of CDAFA, Plaintiffs and Class members seek actual

24 damages, general damages, unjust enrichment, punitive damages, appropriate injunctive or other

25 equitable relief pursuant to Cal. Penal Code § 502€(1) and any other relief the Court deems just.

26   487.   Pursuant to Cal. Penal Code § 502(e)(2), Plaintiffs and Class Members also ask

27 the Court to award them their reasonable attorney's fees.

28 / / /

488.	Pursuant to Cal. Penal Code § 502(e)(4), Plaintiffs and Class Members are also entitled to punitive or exemplary damages because Facebook's violations are willful, and upon information and belief, Facebook is guilty of oppression, fraud, or malice as defined in Cal. Civil Code. § 3294.

THIRTEENTH CLAIM FOR RELIEF

(Unjust Enrichment – California Law)

By Plaintiffs on behalf of themselves and the Class

489.	Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

490.	Meta has wrongfully and unlawfully transmitted, received, used, and sold Plaintiffs' and Class members' individually identifiable health information without their consent for substantial profits.

491.	Plaintiffs' and Class members' individually identifiable health information conferred an economic benefit on Meta.

492.	Meta has been unjustly enriched at the expense of the Plaintiffs and Class members.

493.	Meta has unjustly retained the benefits of its unlawful and wrongful conduct.

494.	It would be inequitable and unjust for Meta to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

495.	Plaintiffs and Class members accordingly are entitled to equitable relief, including restitution and disgorgement of all revenues, earnings, and profits that Meta obtained as a result of its unlawful and wrongful conduct.

**VIII.	PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs respectfully request that the Court:

A.	Certify the proposed Class, designating Plaintiffs as class representatives and their counsel as class counsel;

B.	Award compensatory damages, including statutory damages where available, to Plaintiffs and Class members for all damages sustained as a result of Meta's wrongdoing, in an amount to be proven at trial, including interest thereon, except under the CLRA;

C.   Award punitive damages on the causes of action that allow for them and in an amount that will deter Meta and others from like conduct;

D.   Award injunctive relief;

E.   Award restitution and disgorgement of Meta's profits from its unlawful and unfair business practices and conduct;

F.   Issue an order for public injunctive relief under the UCL;

G.   Award attorneys' fees and costs, as allowed by law including, but not limited to, California Code of Civil Procedure section 1021.5;

H.   Award pre-judgment and post-judgment interest, as provided by law; and

I.   For any other, further, and different relief as the Court deems just.

IX.   DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and Class members, demand a trial by jury of any and all issues in this action so triable of right.

<div align="center">

SIGNATURE ATTESTATION

</div>

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

RESPECTFULLY SUBMITTED AND DATED this 21st day of February, 2023.

SIMMONS HANLY CONROY LLC

By: */s/ Jason "Jay" Barnes*
    Jason "Jay" Barnes, *Admitted Pro Hac Vice*
    Email: jaybarnes@simmonsfirm.com
    Eric S. Johnson, *Admitted Pro Hac Vice*
    Email: ejohnson@simmonsfirm.com
    An V. Truong, *Admitted Pro Hac Vice*
    Email: atruong@simmonsfirm.com
    Jennifer Paulson, *Admitted Pro Hac Vice*
    Email:jpaulson@simmonsfirm.com
    112 Madison Avenue, 7th Floor
    New York, New York 10016
    Telephone: (212) 784-6400

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Geoffrey Graber, CSB #211547
Email: ggraber@cohenmilstein.com
Eric Kafka, *Admitted Pro Hac Vice*
Email: ekafka@cohenmilstein.com
Claire Torchiana, CSB #330232
Email: ctorchiana@cohenmilstein.com
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW, Fifth Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

Paul R. Kiesel, CSB #119854
Email: kiesel@kiesel.law
Jeffrey A. Koncius, CSB #189803
Email: koncius@kiesel.law
Nicole Ramirez, CSB #279017
Email: ramirez@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, California 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

Beth E. Terrell, CSB #178181
Email: bterrell@terrellmarshall.com
Amanda M. Steiner, CSB #190047
Email: asteiner@terrellmarshall.com
Benjamin M. Drachler, *Pro Hac Vice Pending*
Email: bdrachler@terrellmarshall.com
TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 816-6603
Facsimile: (206) 319-5450

Andre M. Mura, CSB #298541
Email: amm@classlawgroup.com
Hanne Jensen, State Bar No. 336045
Email: hj@classlawgroup.com
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
Telephone: (510) 350-9700
Facsimile: (510) 350-9701

Attorneys for Plaintiffs and Proposed Class

Case No. 3:22-cv-3580-WHO-VKD
CONSOLIDATED CLASS ACTION COMPLAINT