

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

## TABLE OF CONTENTS

I.	NATURE OF THE ACTION .....	1
II.	PARTIES .....	5
III.	JURISDICTION AND VENUE .....	6
IV.	FACTUAL ALLEGATIONS .....	7
A.	Meta’s Pixel tracking tool redirects patients’ data from health care provider and covered entity websites to use for ad targeting.....	7
B.	Meta uses identifiers to match the health information it collects with Facebook users.....	10
C.	Meta also encourages health care Partners to upload patient lists for ad targeting. ....	12
D.	Meta acquires a broad spectrum of identifiable health information from health care providers’ use of the Meta Pixel.....	14
E.	Meta falsely promises Facebook users that it requires its health care Partners to have the right to share their data.....	18
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.” .....	27
G.	Meta’s health marketing division already has systems it could adapt to comply with an injunction. ....	35
H.	Meta’s conduct violates federal and state privacy laws.....	37
1.	The HIPAA Privacy Rule protects patient health care information.....	37
2.	Patient status is among the health information protected by HIPAA. ....	39
3.	There is no HIPAA exception for marketing on the Internet.....	41
4.	State law also protects health information. ....	44
5.	Patients have protectable property interests in their individually identifiable health information.....	46
6.	The information Meta acquires without Plaintiffs’ and Class members’ consent has actual, measurable monetary value .....	48
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.....	52
J.	Meta can identify health care provider webpages where the Pixel is redirecting patients’ health information to Meta without patients’ consent. ....	61
K.	Meta has been required to thoroughly police itself since at least 2011 by consent decrees governing the company’s conduct. ....	62

1	L.	Meta uses health information it acquires without authorization for commercial gain.....	68
2	V.	CLASS ACTION ALLEGATIONS .....	69
3	VI.	TOLLING .....	71
4	VII.	CLAIMS FOR RELIEF .....	72
5		FIRST CLAIM FOR RELIEF (Breach of Contract) .....	72
6		SECOND CLAIM FOR RELIEF (Breach of the Duty of Good Faith and Fair Dealing).....	79
7		THIRD CLAIM FOR RELIEF (Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510 <i>et seq</i> ) .....	82
8		FOURTH CLAIM FOR RELIEF (Violation of California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632).....	90
9		FIFTH CLAIM FOR RELIEF (Intrusion Upon Seclusion—Common Law).....	92
10		SIXTH CLAIM FOR RELIEF (California Constitutional Invasion of Privacy).....	95
11		SEVENTH CLAIM FOR RELIEF (Negligence per se).....	98
12		EIGHTH CLAIM FOR RELIEF (Trespass to Chattel) .....	100
13		NINTH CLAIM FOR RELIEF (Violation of California’s Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 <i>et seq.</i> ).....	102
14		TENTH CLAIM FOR RELIEF (Violation of California Consumer Legal Remedies Act, Cal. Civ. Code § 1780 <i>et seq.</i> ).....	104
15		ELEVENTH CLAIM FOR RELIEF (Violation of Cal. Penal Code §§ 484 and 496 – Statutory Larceny) .....	105
16		TWELFTH CLAIM FOR RELIEF (Violation of the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502).....	107
17		THIRTEENTH CLAIM FOR RELIEF (Unjust Enrichment – California Law) .....	112
18	VIII.	PRAYER FOR RELIEF .....	112
19	IX.	DEMAND FOR JURY TRIAL .....	113
20			
21			
22			
23			
24			
25			
26			
27			
28			

**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



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

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

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

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

19 10. The transmission is invisible.

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

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

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

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

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

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 website, 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 ///

1 **IV. FACTUAL ALLEGATIONS**

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

4 34. Meta maintains profiles of its Facebook users that include the users’ real names,  
 5 locations, email addresses, friends, “likes,” and communications.

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

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

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

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

16 39. The Meta Pixel is a free and publicly available “piece of code” that third-party web  
 17 developers can install on their website to “measure, optimize and build audiences for ... ad  
 18 campaigns.”<sup>1</sup>

19 40. Meta describes the Pixel as “a snippet of Javascript code” that “relies on Facebook  
 20 cookies, which enable [Facebook] to match ... website visitors to their respective Facebook User  
 21 accounts.”<sup>2</sup>

22 41. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel  
 23 “can help you better understand the effectiveness of your advertising and the actions people take  
 24 on your site, like visiting a page or adding an item to their cart.”<sup>3</sup>

25  
 26  
 27 <sup>1</sup> Meta, Meta Pixel (2023), <https://www.facebook.com/business/tools/meta-pixel>.

28 <sup>2</sup> Meta for Developers, Meta Pixel (2023), <https://developers.facebook.com/docs/meta-pixel/>.

<sup>3</sup> 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.”<sup>4</sup>

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.<sup>5</sup>



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.

<sup>4</sup> *Id.*

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



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.<sup>6</sup>

#### 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.<sup>7</sup>

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."<sup>8</sup>

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

<sup>7</sup> Meta, Meta Pixel (2023), <https://www.facebook.com/business/tools/meta-pixel>.

<sup>8</sup> 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."<sup>9</sup>

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.

---

<sup>9</sup> 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>.

57. The Meta datr cookie identifies the web browser the patient is using. It is an identifier that is unique to the patient's specific web browser and is therefore another way that Meta can identify Facebook users.

58. Meta keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Meta by using the Facebook Download Your Information tool.

59. The Meta fr cookie is an encrypted combination of the c\_user and datr cookies.<sup>10</sup>

60. The c\_user, datar, and fr cookies are traditional third-party cookies. That is, they are cookies associated with a party other than the entity with which a person is communicating at the time. In the example of a health care provider, they are third-party cookies because Meta is a third-party to the communication between a patient and their health care provider.

61. The Meta \_fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the health care provider using the Meta Pixel.

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

63. The \_fbp (or Facebook Pixel) cookie is also a third-party cookie in that it is also cookie associated with Meta that is used by Meta to associate information about a person and their communications with non-Meta entities while the person is on a non-Meta website or app.

64. Meta disguises the \_fbp cookie as a first-party cookie even though it is Meta's cookie on non-Meta websites.

65. By disguising the \_fbp cookie as a first-party cookie for a health care provider rather than a third-party cookie associated with Facebook, Meta ensures that the \_fbp cookie is placed on the computing device of patients who seek to access the patient portal.

66. Most and perhaps all health care providers with a patient portal require patients to have enabled first-party cookies to gain access to their patient records through the portal.

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

<sup>10</sup>See Gunes Acar, et al., Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission (Mar. 27, 2015), [https://securehomes.esat.kuleuven.be/~gacar/fb\\_tracking/fb\\_pluginsv1.0.pdf](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:<sup>11</sup>

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:<sup>12</sup>

**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.

///

<sup>11</sup> Meta Business Help Center, *About Customer List Custom Audiences* (2023), <https://www.facebook.com/business/help/341425252616329?id=2469097953376494>.

<sup>12</sup> Meta Business Help Center, *Create a Customer List Custom Audience* (2023), <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>.

**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.

///

///

///

///

///

1           77. Public polling shows that, “[n]inety-seven percent of Americans believe that  
2 doctors, hospitals, labs and health technology systems should not be allowed to share or sell their  
3 sensitive health information without consent.”<sup>13</sup>

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

13           79. Plaintiff John Doe I is a patient of MedStar Health in Baltimore, Maryland. When  
14 he used the “myMedStar” patient portal to review his lab results, make medical appointments, and  
15 communicate with his health care providers, the Meta Pixel on MedStar’s website redirected his  
16 identity and the fact that he clicked to log in to the patient portal to Meta. The Meta Pixel redirected  
17 the following information about John Doe I to Meta:

- 18           a. He was communicating with MedStar via its www.MedStarHealth.org
- 19           website;
- 20           b. He engaged in an ‘ev’ or event called a SubscribedButtonClick;
- 21           c. The content of the button he clicked was “Login to myMedstar;”
- 22           d. The page on which he clicked the button was Patient Portal, or “Home;”
- 23           e. He had previously visited a MedStar page about breast health;
- 24           f. His Internet Protocol address;

25  
26  
27 <sup>13</sup> *Poll: Huge majorities wants control over health info*, Healthcare Finance (Nov. 10, 2020),  
28 <https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info>.

g. Identifiers that Facebook uses to identify him and his device, including the c-user, datr, fr, and fbp cookies; and

h. Browser attribute information sufficient to fingerprint his device.

QueryString	
Name	Value
cd[buttonFeature]	{"classList":"button medstar-button-primary button-round-medium margin-10","destination":"https://mymedstar.iqhealth.com/home?opt_id=[REDACTED]&ga=[REDACTED] 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=[REDACTED]&ga=[REDACTED]
ec	2
es	automatic
ev	SubscribedButtonClick
fbp	fb.1.1 [REDACTED] 23
id	[REDACTED]
if	false
it	[REDACTED]
o	30
r	stable
rl	https://www.medstarhealth.org/mhs/our-services/womens-health/conditions/breast-health/breast-conditions/
rqm	GET
sh	1080
sw	1920

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;”



- d. The page from which the button she clicked was Patient Portal, the “Patients & Visitors” page;
- e. She had previously visited a Rush page about medical records;
- f. Her Internet Protocol address;
- g. Identifiers that Facebook uses to identify her and her device, including cookies named c-user, datr, fr, and fbp (*i.e.* Facebook Pixel); and
- h. Browser attribute information sufficient to fingerprint her device.

Name	Value
id	[REDACTED]
ev	SubscribedButtonClick
dl	https://www.rush.edu/patients-visitors
rl	https://www.rush.edu/patients-visitors/medical-records
if	false
ts	[REDACTED]
cd[buttonFeatures]	{"classList":"icon-mychart external","destination":"https://mychart.rush.edu/?_ga=[REDACTED]"}
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.[REDACTED]
it	[REDACTED]
coo	false
es	automatic
tm	3
exp	p1
rqm	GET

82. Substantially similar transmissions were sent to Meta when Plaintiffs John Doe II (WakeMed), Jane Doe II (OSU), and Jane Doe III (North Kansas City) used their health care providers’ websites, including when they logged into their providers’ patient portals. No Plaintiff had any knowledge of those transmissions or consented to them.

83. Plaintiffs all expected that their communications with their health care providers 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.<sup>14</sup>

**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.<sup>15</sup>

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).

///

///

///

<sup>14</sup> 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>.

<sup>15</sup> See Dkt. 76-3 (Terms of Service), 76-4 (Data Policy), 76-5 (Cookies Policy).

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.”<sup>16</sup>

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:

///

///

///

///

///

///

///

///

<sup>16</sup> 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](https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0).

## 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.

98. Meta's Terms of Service also expressly incorporates the Meta Privacy Policy by hyperlink, stating that "Our Privacy Policy explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described" in Meta's Terms of Service.

99. The Meta Privacy Policy begins with the statement, "We at Meta want you to understand what information we collect, and how we use and share it. That's why we encourage you to read our Privacy Policy. This helps you use Meta Products in the way that's right for you."

100. Next, the Meta Privacy Policy has a section titled "What information do we collect?," in which Meta tells users:

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

(Emphasis added.)

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

Here's the information we collect:

**Your activity and information you provide** >

**Friends, followers and other connections** >

**App, browser and device information** >

**Information from Partners, vendors and third parties** >

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.

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
<p><b>Information from websites and apps that use our Services.</b> 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.</p> <p><b>Information from third-party partners.</b> 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.</p>	<p><b>Information from partners.</b> Advertisers, app developers, and publishers can send us information through <a href="#">Meta Business Tools</a> they use, including our social plug-ins (such as the Like button), Facebook Login, our <a href="#">APIs and SDKs</a>, or the <a href="#">Meta pixel</a>. 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.</p> <p>Partners receive your data when you visit or use their services or through third parties they work with. <a href="#">We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us.</a> <a href="#">Learn more</a> about the types of partners we receive data from.</p> <p>To learn more about how we use cookies in connection with Meta Business Tools, review the <a href="#">Facebook Cookies Policy</a> and <a href="#">Instagram Cookies Policy</a>.</p>

113. Meta changed this provision again in July 2022—after Plaintiffs filed this lawsuit—to remove the word “lawful” while still promising that it requires partners to have the right to share patient information with Meta:<sup>17</sup>

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

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

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 require Partners to have the right to collect, use and share your information before giving it to us.

114. Despite the changes it made to this provision over time, Meta has never “required” health care providers or other covered entities, to have the right to “collect, use and share” patient information before redirecting it to Meta. Instead, Meta merely includes a provision in its form contract that creates an unenforced “honor system,” stating that by using Meta’s Business Tools the health care provider or covered entity “represent[s] and warrant[s] that [it has] provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage”.<sup>18</sup>

///

///

///

///

///

///

///

<sup>17</sup> Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), <https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors>.

<sup>18</sup> 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.<sup>19</sup>

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

<sup>19</sup> 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.”<sup>20</sup> 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.”<sup>21</sup> 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.<sup>22</sup>

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.<sup>23</sup>

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.

<sup>20</sup> 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](https://www.facebook.com/privacy/policy?annotations[0]=1.ex.43-WhatHappensIfYou).

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

<sup>22</sup> Meta letter to Senator Mark Warner at 4 (Nov. 3, 2022).

<sup>23</sup> 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.

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

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

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

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

12 130. Meta Health’s role is to “inspir[e]” health care marketers “to think about how we  
13 can really disrupt health and how we market to patients.”<sup>24</sup>

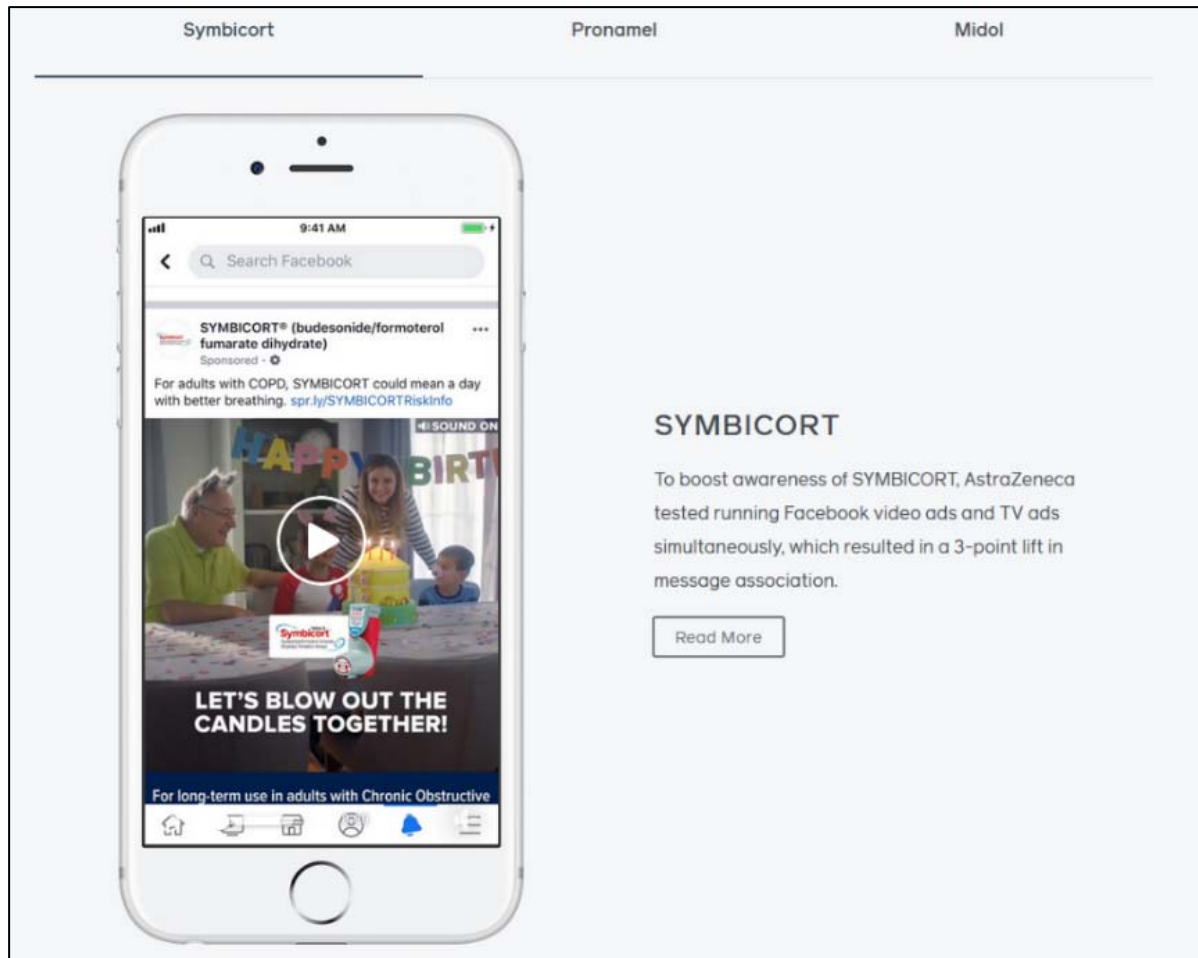
14 131. Meta Health employees are assigned to specific health care providers and other  
15 covered entities to encourage and aid their use of the Pixel and other Meta marketing products for  
16 targeting patients.

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

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

26  
27  
28 <sup>24</sup> 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”:<sup>25</sup>

///

///

///

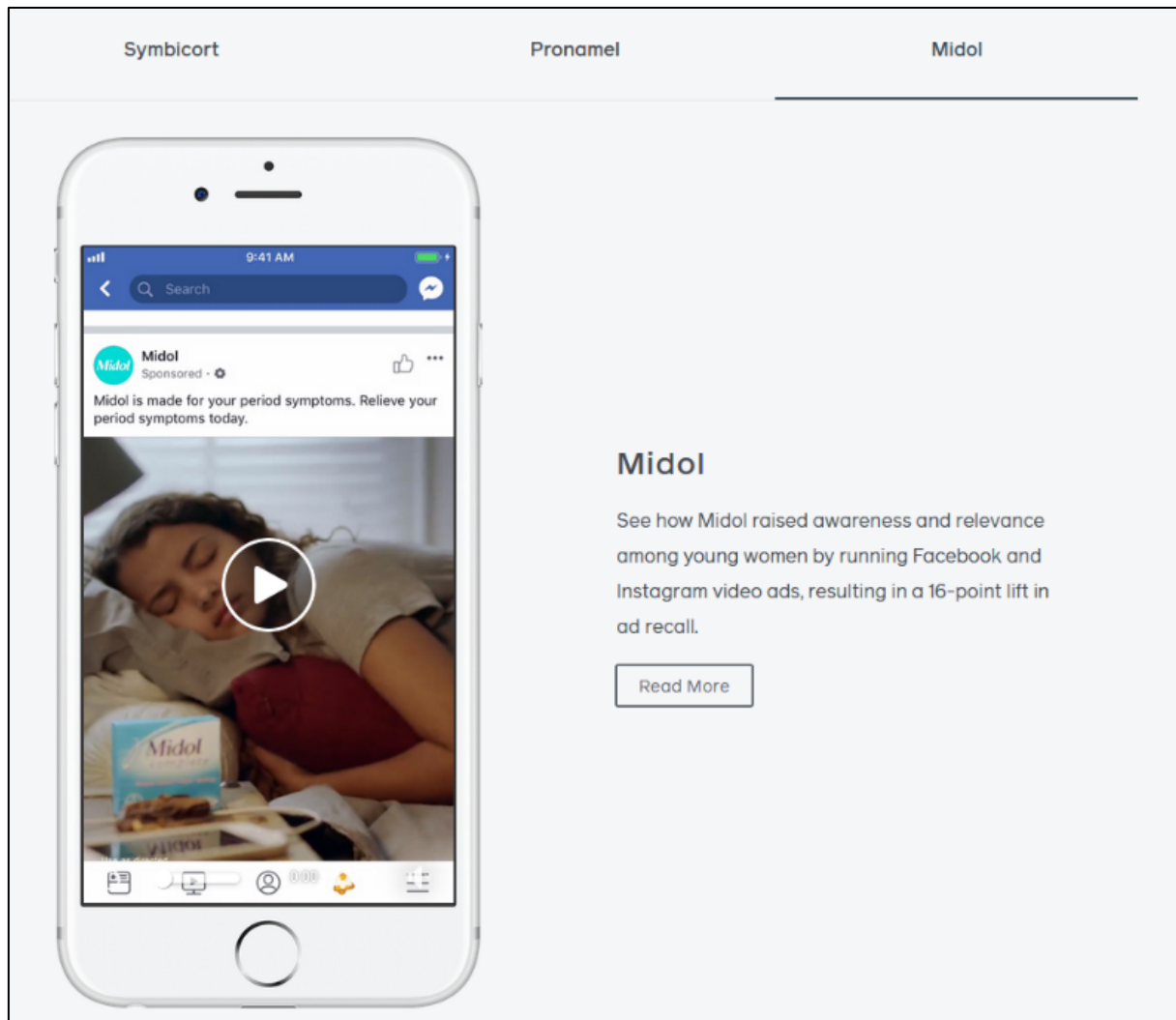
///

///

///

///

<sup>25</sup> 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”.<sup>26</sup>

///

///

///

///

///

///

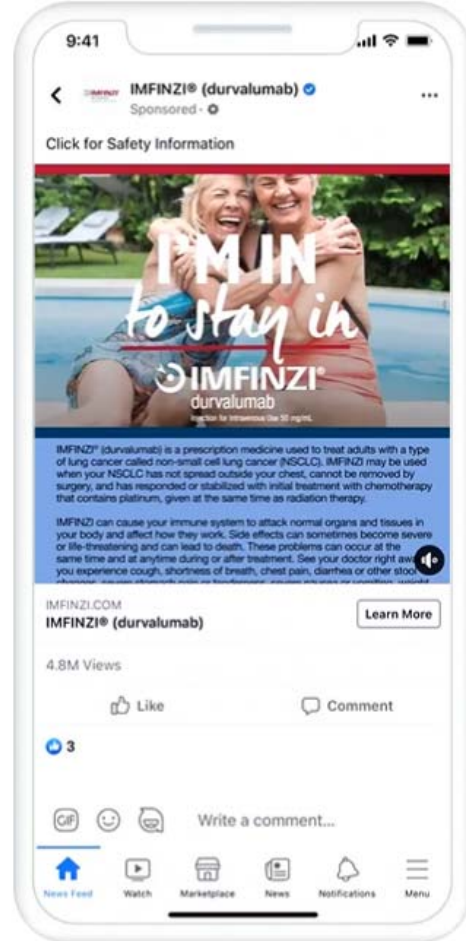
///

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

AstraZeneca is always looking to innovate, so for this Facebook ad campaign, the brand wanted to test a new ad placement. The team decided to run an In-Stream Reserve campaign and measure the results with a Facebook brand lift study—making AstraZeneca the first oncology brand on Facebook to use this strategy.

With the In-Stream Reserve placement, video ads appear as breaks within the highest-quality branded content and premium inventory on the Facebook platform, as well as within other longer-form publisher video content and shows.

The team chose In-Stream Reserve because it is **a unique way to reach patients** where they are already engaged and spending their time. In addition, AstraZeneca could place the message about the availability of IMFINZI as a lung cancer treatment in front of premier publishers on the platform to gain mass awareness, while using the brand lift study to gain learning for future campaigns. AstraZeneca collaborated with its creative agency HealthWork to build the assets, and its media agency CMI Media Group to organize the campaign from launch to completion.



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.<sup>27</sup>

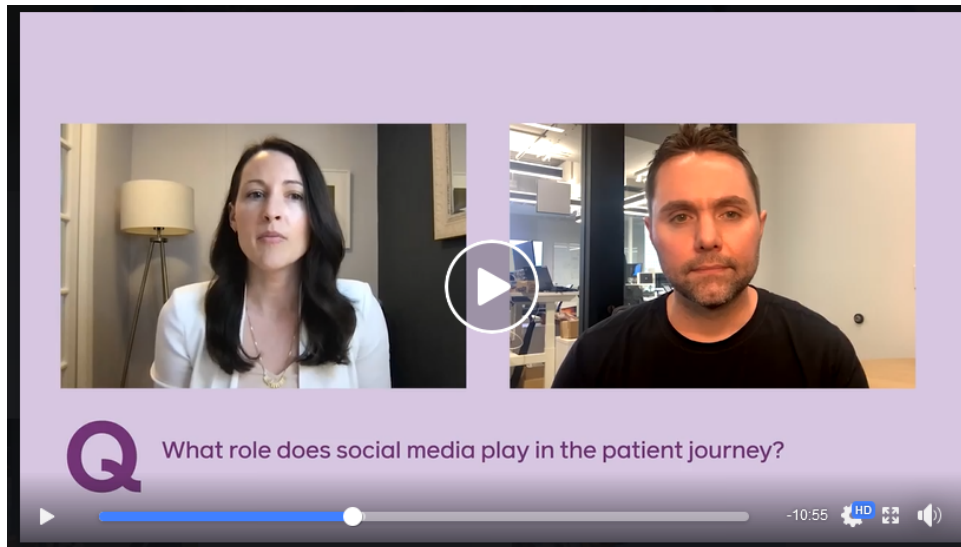
138. To promote its marketing tools to health care providers and covered entities, the Meta health webpage includes Meta Health's Erin Ott's interview with Jasson Gilmore, Senior Vice President for Global Consumer & Digital Marketing at AbbVie. In the interview, Gilmore

<sup>27</sup> 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.



states, “Social media is a primary place your target audience spends their time” and “if you’re going to be trying to market to potential patient populations that have unmet needs or underserved, these are platforms that give you immense control and measurability around the way you spend and allocate capital.” The pitch also stresses that it can be a “research platform” that provides “millions and millions of data points of the consumers who are interested in our brands,” which is “an invaluable asset.” Through Meta, an advertiser can get “millions and millions of consumers who actually use [its] brands.”<sup>28</sup>

139. Ott then asks Gilmore specifically about “the patient journey” and how Metacan “play a role in that patient journey.”



140. The response is that Meta’s marketing tools (including the Pixel) can target 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.

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

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

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

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

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



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



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.”



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

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

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

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

7  
8 “  
9  
10 It's such an optimistic thing to know who  
11 your patients are or who your potential patients  
12 are and how to reach them in a way that is  
13 very financially manageable and feasible  
14 and profitable.

15  
16 Jasson Gilmore  
17 SVP Global Consumer & Digital Marketing, AbbVie

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

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

22 147. Plaintiffs request permanent injunctive relief in this action.

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

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

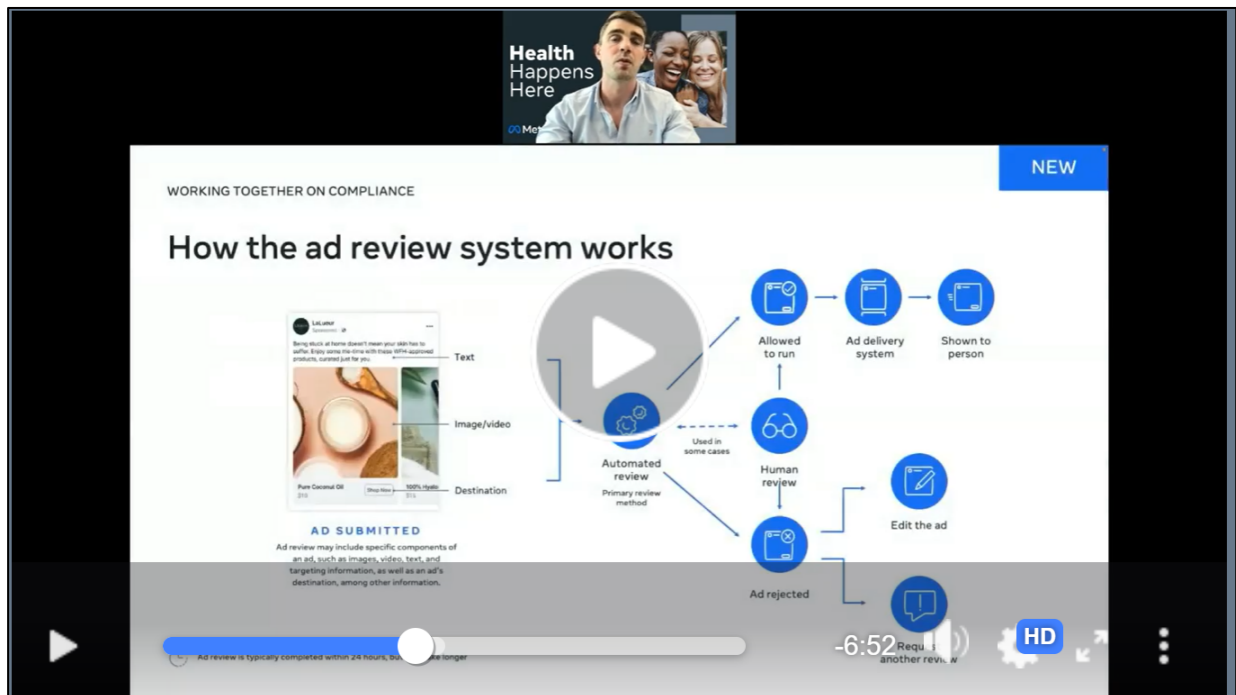
27 150. Plaintiffs filed an expert declaration in support of their reply explaining how Meta  
28 could and should create a system to detect Pixel data that it was wrongfully acquiring from health

care providers that would involve: (1) the use of automated systems to detect health content; (2) automatic blocking of Pixel data from properties sending health content; and (3) an appeal process to address Meta's concerns that its filter may unintentionally block some otherwise lawful data.

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

152. The video on "compliance" that Meta already has in place for ads describes a similar system to the one described by Plaintiffs' expert.<sup>29</sup>

153. Meta provides health care advertisers with a diagram of its ad review system:



154. Meta claims that its "ad review system is actually designed to review all ads proactively, which means before they go live" and "relies primarily on automated technology to apply our advertising policies to the millions of ads that we have going live every single day."

155. Meta also states that it uses human reviewers in some cases, and that, the "review process may include specific components of an ad, such as images, video, text, targeting information, or an ad's destination, amongst other information."

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

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

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

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

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

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

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

16           **H. Meta’s conduct violates federal and state privacy laws.**

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

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

20          163. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part  
21 164, “establishes national standards to protect individuals’ medical records and other individually  
22 identifiable health information (collectively defined as ‘protected health information’) and applies  
23 to health plans, health care clearinghouses, and those health care providers that conduct certain  
24 health care transactions electronically.”<sup>30</sup>

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

27  
28 <sup>30</sup> HHS.gov, *Health Information Privacy* (Mar. 31, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>.

maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

165. IIHI is defined as “a subset of health information, including demographic information collected from an individual” that is: (1) “created or received by a health care provider, health plan, employer, or health care clearinghouse”; (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual”; and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

166. Under the HIPAA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

- A. Names;
- H. Medical record numbers;
- J. Account numbers;
- M. Device identifiers and serial numbers;
- N. Web Universal Resource Locators (URLs);
- O. Internet Protocol (IP) address numbers; ... and
- R. Any other unique identifying number, characteristic, or code...; and”

the covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514.

167. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health

information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

168. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information ... if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

169. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Meta when it is knowingly obtaining individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

170. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

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

171. An individual’s status as a patient of a health care provider is protected by HIPAA. Dkt. 159 at 12 (“I agree that the information at issue here appears to show patient status and thus constitutes protected health information under HIPAA.”), 15 (“[T]he Pixel captures information that connects a particular user to a particular health care provider—i.e., patient status—which falls within the ambit of information protected under HIPAA”).

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

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.  
... **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.<sup>31</sup>

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.**<sup>32</sup>

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

<sup>31</sup> 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/coveridentities/De-identification/hhs\\_deid\\_guidance.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/De-identification/hhs_deid_guidance.pdf).

<sup>32</sup> Office for Civil Rights, *Marketing* at 1-2 (emphasis added) (Apr. 3, 2003), <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/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.”<sup>33</sup>

176. In the bulletin, HHS confirmed that HIPAA applies to health care providers’ use of tracking technologies like the Meta Pixel.<sup>34</sup> 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

<sup>33</sup> 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>.

<sup>34</sup> 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 IHI 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 IHI, 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 IHI 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

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.*

///

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

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

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

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

25           188. The California Consumer Privacy Act of 2018 requires that “[i]f the business  
26 collects sensitive personal information,” it shall inform consumers of “the categories of sensitive  
27 personal information to be collected and the purposes for which the categories of sensitive personal  
28 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 ///

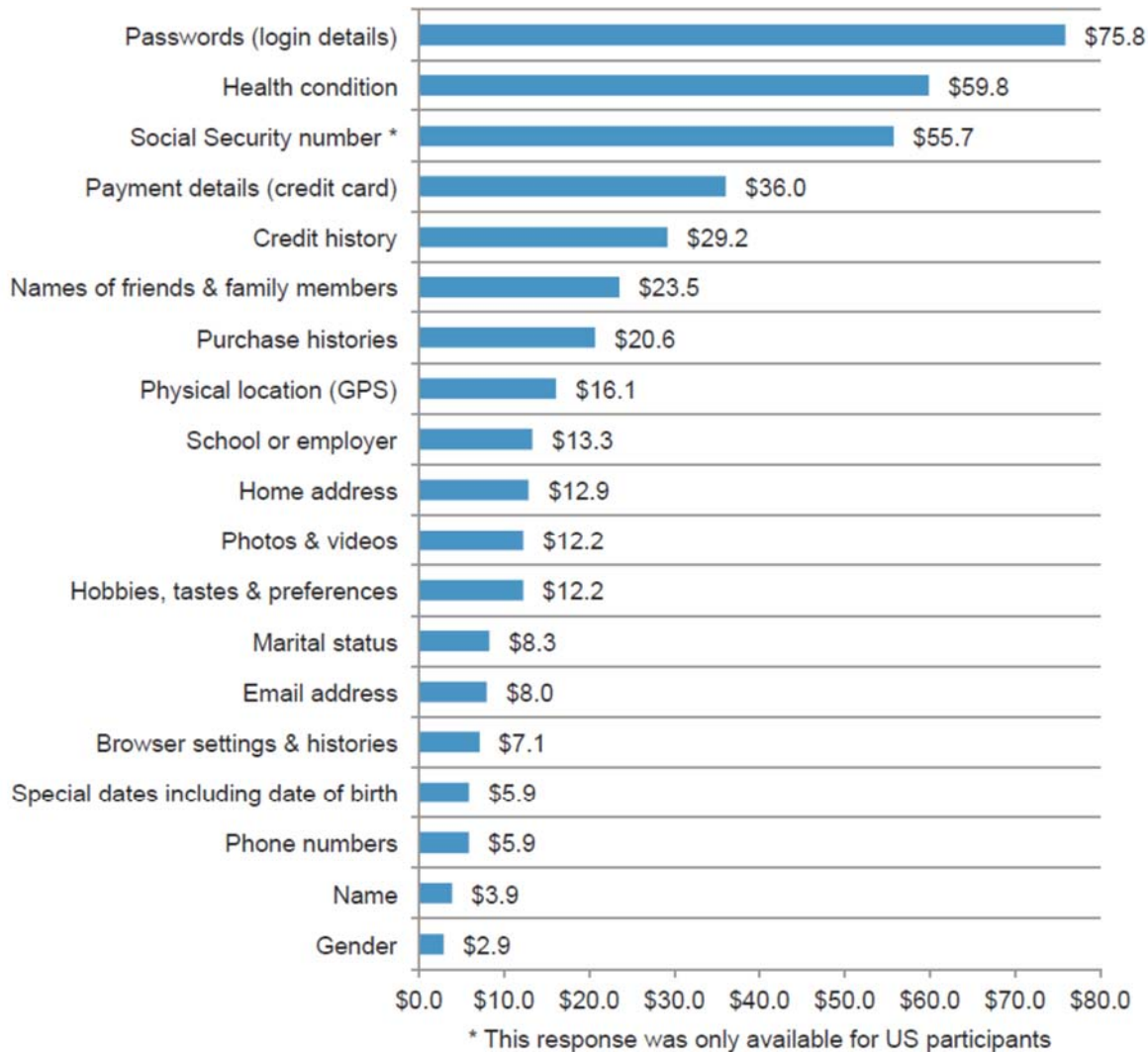
25 ///

26 ///

27 ///

28

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



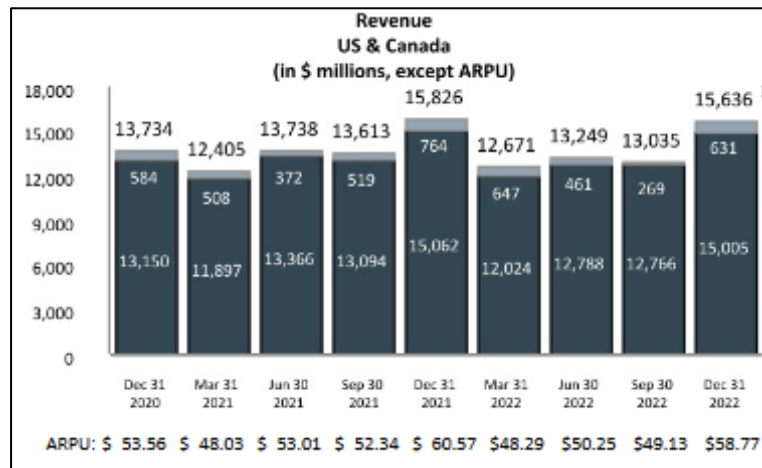
211. In addition, some companies sell de-identified health information in the open market. For example, a company named Prognos Health provides a data platform where it purports to sell information from “more than 325 million de-identified patients.”<sup>35</sup>

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

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

their business is through average revenue per user or “ARPU.” Meta has long used ARPU in its Annual and Quarterly Reports to the United States Securities and Exchange Commission.

213. In its 2022 Form 10-K, Meta reported total advertising revenue of \$15 billion in the United States and Average Revenue Per User of \$58.77 for the fourth quarter of 2022.



214. Several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

215. Meta itself has paid users for their digital information, including browsing history. Until 2019, Meta ran a “Facebook Research” app through which it paid \$20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

216. Because Americans typically do not want to sell their individually identifiable health information for any purpose and it is illegal to even share it without express, written authorization, there are fewer open markets for a license to collect or sell individually identifiable health information for non-health purposes than other types of data. However, black markets do exist for such data. It has been reported that health data can be “more expensive than stolen credit card numbers” on black markets.<sup>36</sup>

<sup>36</sup> 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/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:<sup>37</sup>

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.<sup>38</sup>

<sup>37</sup> 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.

<sup>38</sup> *Id.* at 1:06:11-1:06:59.

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

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

7           Sen. Wicker: You don't know?

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

14          221. In March 2020, Meta responded to an article in the Washington Post titled,  
 15          "Facebook has a prescription: More pharmaceutical ads," by claiming that "Medical history is not  
 16          used to inform the interest categories that we make available to advertisers, and we prohibit  
 17          businesses from sending us sensitive health information. Our teams work with health related  
 18          companies looking to reach their audiences on Facebook and we require them to act in accordance  
 19          with the law."<sup>39</sup>

20          222. Upon information and belief, Meta staffers advised CEO Mark Zuckerberg as early  
 21          as 2020 that Meta should stop using health information for advertising.

22          223. On November 9, 2021, Meta announced that it was removing the ability to target  
 23          users on "topics people may perceive as sensitive, such as options referencing causes,  
 24          organizations, or public figures that relate to health."<sup>40</sup>

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

26               a. Reuters published a story headlined "Facebook plans to remove thousands  
 27               of sensitive ad-targeting options" and lead the story with a sentence about  
 28               

<sup>39</sup> 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/>.

<sup>40</sup> 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>.

Facebook’s “plans to remove detailed ad-targeting options that refer to ‘sensitive’ topics, such as ads based on interactions with content around . . . health.”<sup>41</sup>

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.”<sup>42</sup>

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.”<sup>43</sup>

<sup>41</sup> 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/>.

<sup>42</sup> 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>.

<sup>43</sup> 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](https://www.wsj.com/articles/facebook-parent-meta-bans-targeting-for-political-ads-11636488053).



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.”<sup>44</sup> 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.”<sup>45</sup>

///

///

///

///

///

///

///

///

///

///

///

///

///

///

<sup>44</sup> 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>.

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

228. Meta publishes guidance for brands in the health and pharmaceutical industry (which includes health care providers and covered entities).<sup>46</sup> As seen in the image below, Meta's 2022 guidance for health-related advertising instructs that targeting "Lookalikes of Meta Pixel" created the best results:

Lookalike Audiences were the most cost-efficient in 86% of all studies. But "seed audience" matters.<sup>1</sup>

Lookalikes of website visitors were the most cost-efficient, followed by Lookalikes of video viewers and Lookalikes of Facebook page engagers.

Across four of the fourteen split tests, Lookalikes, of Meta Pixel signals vs. Lookalikes of prior ad engagers were tested.

PHM found that

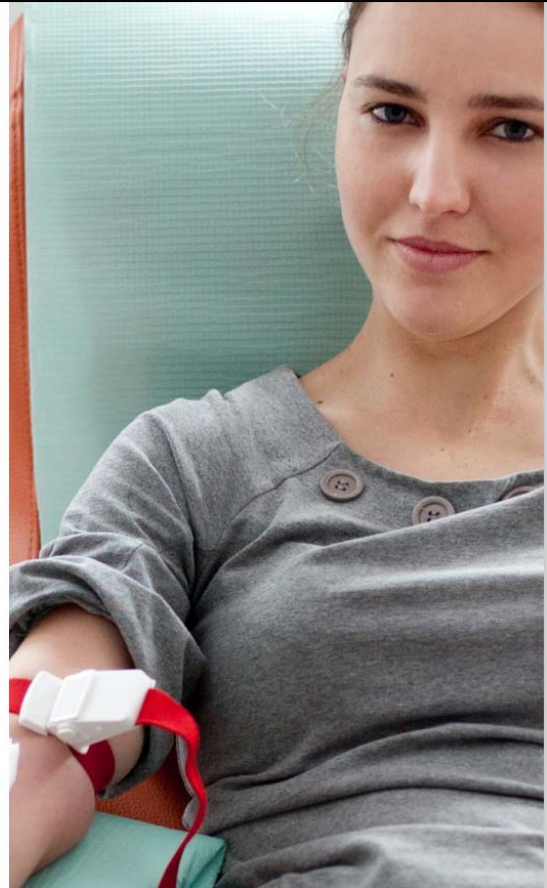
**5%**

Lookalikes of Meta Pixel signals drove the lowest-cost impressions, highest volume of actions, lowest cost per result and highest result rate.<sup>1</sup>

Lookalikes of video viewers and page engagers also out-performed legacy health interest segments

**66%**

of the time they were tested, but were consistently more expensive than Meta Pixel-based Lookalike Audiences.<sup>1</sup>



229. In August 2022, Meta published a white paper on its Health page addressing how "to uncover alternative targeting strategies" for health-related targeted advertising. The study advised that "Lookalike Audiences" of "Meta Pixel signals" were a cost-efficient replacement.<sup>47</sup>

230. In other words, while eliminating targeting based on health-interest categories, Meta simultaneously encouraged health care providers and other covered entities to increase their

<sup>46</sup> *Id.*

<sup>47</sup> 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").


use of the Meta Pixel, allowing Meta to continue to collect individually identifiable health information about patients.

231. The Meta Health division publishes videos that it uses to encourage health care providers and other covered entities to use the Pixel for health-based advertising. The page for <https://www.facebook.com/business/industries/consumer-goods/healthcare> contains hyperlinks to three videos designed to aid health care Partners to send patient information to Meta:

Watch

Track emerging consumer trends and deliver an effective healthcare marketing strategy with Meta

19 min




Adapt to changing consumer trends

Learn how you can use Meta technologies to help your customers achieve their health goals as they move into a preventative healthcare mindset. Create a whole new world of communication touchpoints that will engage your customers.

Watch now

21 min

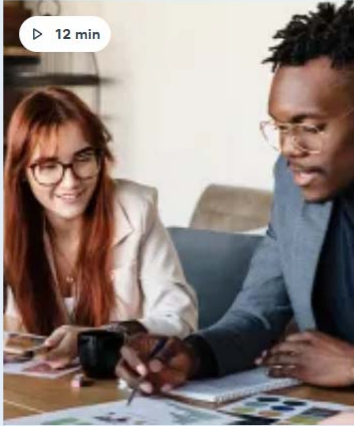


Creating mobile, people-first healthcare ads

Learn how building a multi-channelled creative communication approach through Meta enriches the relationship between your brand and consumers.

Watch now

12 min



Working together on compliance

Meta technologies can be used in many ways to adhere to the various policies and regulations at your company and those of the healthcare industry.

Watch now

///

///

///

///

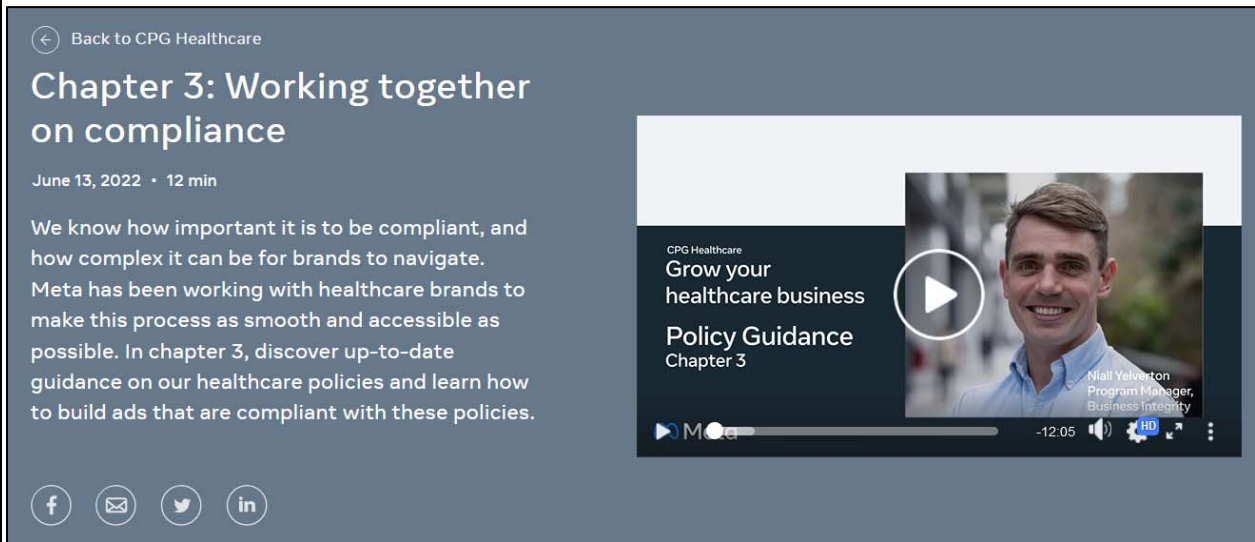
///

///

///

///

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.<sup>48</sup> 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

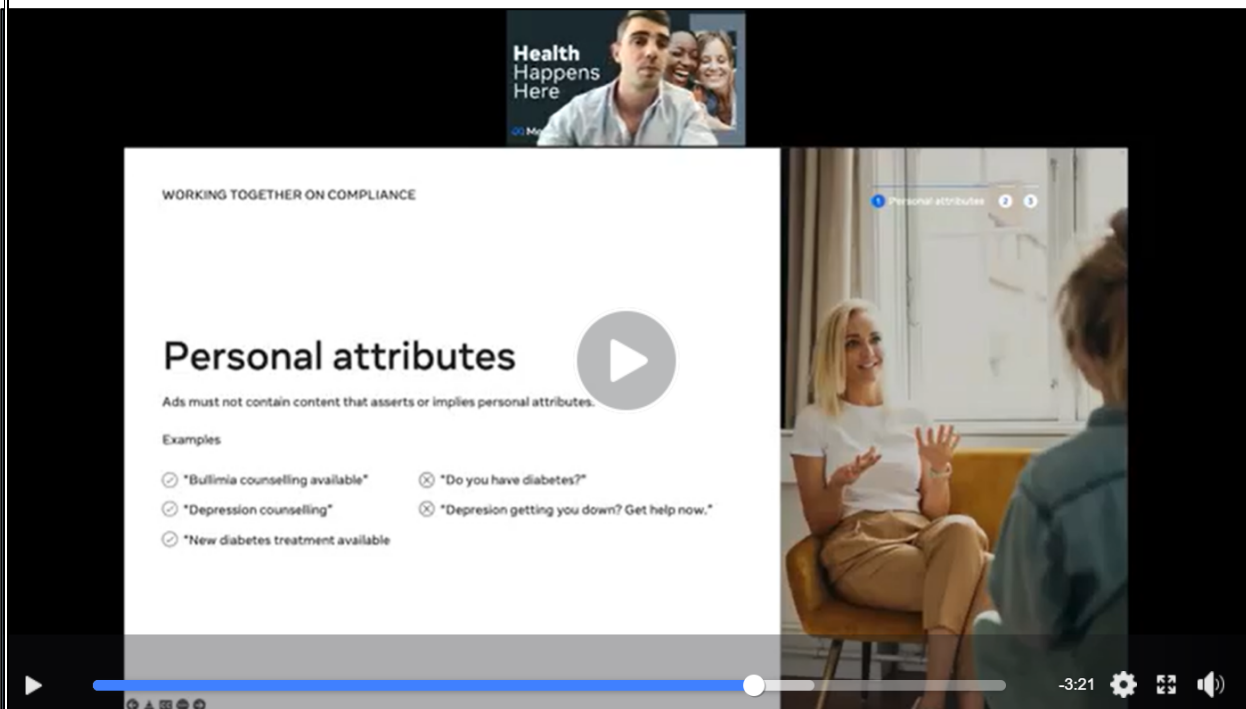
<sup>48</sup> Meta, *Chapter 3: Working together on compliance* (June 13, 2022), <https://www.facebook.com/business/inspiration/video/healthcare-chapter-3>.

other in relation to a personal characteristic. For example, ‘meet others who suffer from cancer’ because you can’t imply that you know anything personal about the person that you’re targeting.

236. Meta then illustrates the differences between compliant and non-compliant text for targeted ads based on health. Under Meta’s rules, it would not be acceptable for an ad targeting people with diabetes or depression to ask, “Do you have diabetes?” or “Depression getting you down? Get help now.” But it would be acceptable to target people with bulimia, depression, or diabetes with ads that state, “Bulimia counseling available;” “Depression counseling;” or “New 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.	

237. Meta provides advertisers with a PowerPoint slide to emphasize the point:



238. Meta’s distinctions do nothing to protect the health information of Facebook users.

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

///



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

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

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

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

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

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

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

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

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

28 ///

**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."<sup>49</sup>

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.

---

<sup>49</sup> 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”;

b. “The extent to which a consumer can control the privacy of any covered information”; and

c. “The steps Respondent takes or has taken to verify the privacy or security protections that any third party provides.”

260. Meta also agreed to “establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers; and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to [Meta’s] size and complexity, the nature and scope of [Meta’s] activities, and the sensitivity of the covered information, including:

a. “Designation of an employee or employees to coordinate and be responsible for the privacy program;”

b. “the identification of reasonably foreseeable, material risks, both internal and external, that could result in [Meta’s] unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order; and (2) product design, development, and research.”

c. “the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls or procedures;”

d. “the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers,

by contract, to implement and maintain appropriate privacy protections for such covered information;” and

- e. “the evaluation and adjustment of [Meta’s] privacy program in light of the results of the testing and monitoring required .... any material changes to [Meta’s] operations or business arrangements, or any other circumstances that [Meta] knows or has reason to know may have a material impact on the effectiveness of the privacy program.”

261. Upon implementation of the privacy program, Meta agreed to “obtain initial and biennial assessments and reports (‘Assessments’) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the progression.” Each Assessment was required to “set for the specific privacy controls” implemented during the reporting period, “explain how such privacy controls are appropriate to [Meta’s] size and complexity, the nature and scope of [Meta’s] activities, and the sensitivity of the covered information;” “explain how the privacy controls meet or exceed the protections” required by the Order; and “certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.” Each Assessment is provided to the Associate Director of Enforcement in the Bureau of Consumer Protection at the Federal Trade Commission.

262. Meta is further required to maintain records of:

- a. “All widely disseminated statements by [Meta] or its representatives that describe the extent to which [Meta] maintains and protects the privacy, security, and confidentiality of any covered information, including, but not to, any statement related to a change in any website or service controlled by [Meta] that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;”

///

///

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

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:

- 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.”
- 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.

- 1 c. “Covered Third Party” was defined to include “any individual or entity that  
2 uses or receives Covered Information obtained by or on behalf of [Meta]  
3 outside of a User-initiated transfer of Covered Information as part of a data  
4 portability protocol or standard.”
- 5 d. Meta is legally required to “[a]ssess and document, at least once every  
6 twelve months, internal risks in each area of its operation [including]  
7 partnerships with Covered Third Parties ... to the privacy, confidentiality,  
8 or Integrity of Covered Information that could result in the unauthorized  
9 access, collection, use, destruction, or disclosure of such information.  
10 [Meta] shall further assess and document internal and external risks as  
11 described above as they related to a Covered Incident, promptly following  
12 verification or confirmation of such an incident, not to exceed thirty (30)  
13 days after the incident is verified or otherwise confirmed.”
- 14 e. Meta is legally required to “design, implement, maintain, and document  
15 safeguards that control for the material internal and external risks identified  
16 by [Meta] [with] [e]ach safeguard ... based on the volume and sensitivity  
17 of the Covered Information that is at risk, and the likelihood that the risk  
18 could be realized and result in the unauthorized access, collection, use,  
19 destruction, or disclosure of the Covered Information.”
- 20 f. “Specifically with respect to [Meta’s] collection, use, or sharing of Covered  
21 Information in any new or modified product, service, or practice, such  
22 safeguards shall include: ... a privacy review that assesses the risks to  
23 privacy, confidentiality, and Integrity of the Covered Information, the  
24 safeguards in place to control such risks, and the sufficiency of the User  
25 notice, and, if necessary, consent; and documenting a description of each  
26 reviewed product, service, or practice that was ultimately implemented, any  
27 safeguards being implemented to control for the identified risks; and the  
28 decision or recommendation made as a result of the review.”

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

with Meta before doing so. Instead, Meta continued to encourage health care providers and covered entities to use the Meta Pixel and other Meta tools to share individually identifiable health information with Meta for the purpose of “inspiring” health care marketers and providers to “think about how we can really disrupt health and how we market to patients.”

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

267. Plaintiffs action arises out of Meta’s unauthorized acquisition of the health information, regardless of how Meta subsequently used or did not use the information.

268. Plaintiffs incorporate by reference the paragraphs in Appendix A demonstrating how Plaintiffs’ expert Richard Smith was served ads based on health information after visiting health entity websites relating to the health information that appeared in the ads. Appendix A ¶¶ 187-191.

269. For example, within two hours of exchanging communications with the health entity Hartford Healthcare about ulcerative colitis, Smith was shown an ad relating to ulcerative colitis in his Facebook video feed. Appendix A ¶¶ 189-190.

270. Upon information and belief, Meta maintains a history of every ad that it has shown to Plaintiffs and Class members on and off of Meta’s social media sites, including on Meta properties and the Facebook Audience Network through which Meta serves ads to Facebook users on non-Meta websites.

271. Meta “generate[s] substantially all of [its] revenue from advertising.”<sup>50</sup>

272. Upon information and belief, Meta annually receives billions of dollars of unearned advertising sales revenue from Meta health care Partners who are targeting Facebook users based on their health information.

273. Meta does not publicly report revenues by advertiser categories or sectors. However, in 2019, the Washington Post reported that “[s]pending on Facebook mobile ads alone

---

<sup>50</sup> Meta 2022 Annual Report at 17.



by pharmaceutical and health-care brands reached nearly a billion dollars in 2019, nearly tripling over two years, according to Pathmatics, an advertising analytics company.”<sup>51</sup>

## V. CLASS ACTION ALLEGATIONS

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

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

275. Excluded from the Class are the Court and its personnel and Meta and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest.

276. Numerosity. The members of the Class are so numerous and geographically diverse that joinder is impracticable.

277. Commonality and Predominance. One or more common questions of law or fact are apt to drive resolution of the case and predominate over any questions affecting solely individual Class members. The common questions include but are not limited to:

- a. Whether the Meta Terms of Service, Data Policy, and Cookies Policy constitute a valid contract between Meta and users;
- b. Whether Meta failed to “require” health care providers and covered entities to have the right to share patient data with Meta before deploying the Meta Pixel on their websites;
- c. Whether Meta “employs dedicated teams around the world” to “detect potential misuse” of the Meta Pixel as alleged in this action;
- d. Whether Meta “works with external service providers, partners, and other relevant entities” to “detect potential misuse” of the Meta Pixel as alleged in this action;

<sup>51</sup> 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/](https://www.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. Typicality. 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.

///

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

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

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

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

11          300. From approximately April 19, 2018 to July 2022, Meta promised:<sup>52</sup>

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

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

27  
28 <sup>52</sup> 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.

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                   *account, 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

but Meta actually took more data than the contractually agreed-upon amount;

h. The amount that Meta should have spent implementing controls to ensure that patient data was not provided to Meta without the patients' consent; and

i. Plaintiffs and Class Members suffered an invasion of privacy. Plaintiffs and Class Members seek compensatory damages for the invasion of their privacy.

318. For Meta's breaches, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, restitution, and any other relief the Court deems just.

## **SECOND CLAIM FOR RELIEF**

### **(Breach of the Duty of Good Faith and Fair Dealing)**

#### **By Plaintiffs on behalf of themselves and the Class**

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

320. A valid contract exists between Meta and Plaintiffs and Class members.

321. The contract specifies that California law governs the parties' relationship.

322. Meta prevented Plaintiffs and Class members from receiving the full benefit of the contract by intercepting the content of their individually identifiable health information.

323. In doing so, Meta abused its power to define terms of the contract, including:

a. The meaning of the term "require" in Meta's promise that it would "require" Partners to have the right to share Plaintiffs' and Class members' data with Meta before doing so and then taking no action to prevent health care providers or covered entities from sharing protected health information without Plaintiffs' and Class members' valid consent.

b. The meaning of the term "appropriate action" in the promise "[i]f we learn of content or conduct like [potential misuse of our products, harmful

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.

324. Meta did not act fairly and in good faith.

325. Rather than “requiring” Partners to obtain the right to share health information, Meta actively solicited them, through the Meta Health division, to share health information regardless of whether they had the right to do so.

326. Rather than taking “appropriate action” upon discovering that health information was being shared with Meta by health entities without the right to do so, Meta actively solicited their further disclosures and advertising revenue, through the Meta Health division.

327. In doing so, Meta frustrated and undercut Plaintiffs’ and Class Members’ contractual rights, and unfairly interfered with Plaintiffs’ and Class Members’ rights under the parties’ contract.

328. As a direct and proximate results of Meta’s breach of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received services from Meta that were less valuable than described in their contract with Meta. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Facebook’s partial, deficient, and/or defective performance.

329. Meta’s breach 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;
- 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;
- g. The deprivation of the benefit of the bargain in that Meta's contract stated that the data license for its services did not include health information from health Partners who did not have the right to share information with Meta, but Meta actually took more data than the contractually agreed-upon amount; and
- h. Plaintiffs and Class Members suffered an invasion of privacy. Plaintiffs and Class Members seek compensatory damages for the invasion of their privacy.

330. For Meta's breaches, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, restitution, and any other relief the Court deems just.

///

///

///

**THIRD CLAIM FOR RELIEF**

**(Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*)**

**By Plaintiffs on behalf of themselves and the Class**

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

332. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional interception of the contents of any electronic communication. 18 U.S.C. § 2511.

333. The ECPA protects both the sending and receipt of communications.

334. The ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

335. Meta intentionally intercepted electronic communications that Plaintiffs and Class members exchanged with their health care providers and covered entities through the Meta Pixel installed on the health care providers’ and covered entity websites.

336. The transmissions of data between Plaintiffs and Class members and their health care providers or covered entities qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

337. Meta contemporaneously acquired Plaintiffs’ and Class members’ communications with their health care providers or covered entities.

338. The intercepted communications include:

- a. the content of Plaintiffs’ and Class members’ registrations for patient portals, including clicks on buttons to “Register” or “Signup” for portals;
- b. the content Plaintiffs’ and Class members’ log in and log out of patient portals, including clicks to “Sign-in,” “Log-in,” “Sign-out,” or “Log-out”;
- c. the contents of communications that Plaintiffs and Class members exchange inside patient portals immediately before logging out of the portals;
- d. the contents of Plaintiffs’ and Class members’ communications relating to appointments with medical providers;



- 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](http://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.

///

///

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 offense 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

1 provision of 42 U.S.C. § 1320d-6 by acquiring the individually identifiable  
2 health information “with intent to sell transfer or use” it for “commercial  
3 advantage [or] personal gain.”

- 4 d. A knowing intrusion upon Plaintiffs’ and Class members’ seclusion;
- 5 e. Trespass upon Plaintiffs’ and Class members’ personal and private  
6 property via the placement of an \_fbp cookie associated with the domains  
7 and patient portals for their health care providers and covered entities on  
8 Plaintiffs’ and Class members’ personal computing devices;
- 9 f. Violation of the California Unfair Competition Law;
- 10 g. Violation of the California Consumer Legal Remedies Act;
- 11 h. Violation of the California Constitution’s right to privacy;
- 12 i. Violation of various state health privacy statutes, including but not limited  
13 to the California Confidentiality of Medical Information Act; the California  
14 Consumer Privacy Protection Act; and the California Consumer Privacy  
15 Act;
- 16 j. Violation of various state computer privacy and property statutes,  
17 including but not limited to the California Comprehensive Computer Data  
18 Access and Fraud Act, Cal. Penal Code § 502;
- 19 k. Violation of Cal. Penal Code § 484 for statutory larceny; and
- 20 l. Violation of the federal wire fraud statutes at 18 U.S.C. §§ 1343 (fraud by  
21 wire, radio, or television) and 1349 (attempt and conspiracy), which  
22 prohibit a person from “devising or intending to devise any scheme or  
23 artifice to defraud, or for obtaining money or property by means of false or  
24 fraudulent pretenses, representations or promises, transmits or causes to be  
25 transmitted by means of wire, radio, or television communication in  
26 interstate ... commerce, any writing, signs, signals, pictures, or sounds for  
27 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 it 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

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

e. A violation of various state health privacy and computer privacy statutes, including the CCPA.

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).

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).

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.

358. Meta's violations of the ECPA were willful and intentional and caused Plaintiffs and Class members the following damages:

- 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;
- b. The diminution in value of Plaintiffs' and Class members' protected health information;
- c. The inability to use their computing devices for the purpose of communicating with their health care providers;
- 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



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 entities 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

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.

370. At all relevant times, Meta's conduct alleged herein was without the authorization and consent of the Plaintiffs and Class members.

371. Meta's actions were designed to learn or attempt to learn the meaning of the contents of Plaintiffs' and Class members' communications exchanged with their health care providers and covered entities.

372. Meta's learning of or attempt to learn the contents of patient communications occurred while they were in transit or in the process of being sent or received.

373. Unless enjoined, Meta will continue to commit the violations of law alleged here. Plaintiffs continue to want to communicate with their health care providers and covered entities 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.

374. Plaintiffs and class members seek all relief available under Cal. Penal Code § 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**

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

376. By collecting and disseminating the contents of Plaintiffs' and Class members' communications with their health care providers and covered entities without their knowledge, Meta intentionally intruded into a realm in which Plaintiffs and Class members have a reasonable expectation of privacy.

377. Plaintiffs and Class members enjoyed objectively reasonable expectations of privacy in their communications with their medical providers and covered entities relating to the respective patient portals, appointments, and health information and communications based on:

- a. The health care providers' or covered entities' status as their health care providers or a covered entity and the reasonable expectations of privacy that attach to patient-provider relationships;

- b. HIPAA;
- c. the ECPA;
- d. Meta’s promise that it would “require” Partners to have the right to share their data before Meta would collect it; and
- e. California medical and computer privacy laws

378. Furthermore, Plaintiffs and Class Members maintained a reasonable expectation of privacy when providing their patient medical data to their health care providers and covered entities and when communicating with their health care providers and covered entities online.

379. Patient medical data is widely recognized by society as sensitive information that cannot be shared with third parties without the patients’ consent.

380. For example, 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.”<sup>53</sup>

381. Meta obtained unwanted access to Plaintiffs’ and Class members’ data, including but not limited to their patient status, the dates and times Plaintiffs and Class members logged in or out of patient portals, and the communications Plaintiffs and Class members exchanged while logged in to patient portals.

382. Meta’s intrusion was also accomplished by placing the “fbp” cookie on the Plaintiffs’ and Class members’ computing devices through the web-servers of the Plaintiffs’ and Class members’ health care providers.

383. By disguising the third-party “fbp” cookie as a first-party cookie from the Plaintiffs’ health care providers or covered entities, Meta ensure that it could hack its way around attempts that Plaintiffs and Class members might make to prevent Meta’s tracking through the use of cookie blockers.

---

<sup>53</sup> *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>.

1           384. In designing the ‘fbp’ cookie as a disguised first-party cookie, Meta was aware that,  
 2 like other websites that include sections where users’ sign in to an account, any health care provider  
 3 or covered entity website with a patient portal would require first-party cookies to be enabled for  
 4 a patient to access the patient portal or other username / password protected “secure” part of the  
 5 health care provider’s website.

6           385. With first-party cookies being required for use of a patient portal and the Meta  
 7 “fbp” cookie disguised as a first-party cookie, Meta was able to implant its tracking device on the  
 8 computing devices of the Named Plaintiffs and Class members even where Plaintiffs or Class  
 9 members made attempts to stop third-party tracking through the use of cookie blockers.

10           386. Meta’s deployment of the “fbp” cookie as a third-party cookie disguised as a first-  
 11 party cookie that is placed on Plaintiffs and Class members’ computing devices is a highly  
 12 offensive intrusion upon seclusion regardless of whether any information was further re-directed  
 13 from the Plaintiffs or Class members computing devices to Meta.

14           387. Meta’s intrusion into Plaintiffs’ and Class members’ privacy would be highly  
 15 offensive to a reasonable person, namely because it occurred without Plaintiffs’ and Class  
 16 members’ consent or knowledge.

17           388. Meta’s intrusion caused Plaintiffs and Class members the following damages:

- 18           a. Nominal damages;
- 19           b. The interruption or preclusion of Plaintiffs’ and Class members’ ability to  
 20 communicate with their health care providers or covered entities on their  
 21 health care providers’ or covered entity websites;
- 22           c. The diminution in value of Plaintiffs’ and Class members’ protected health  
 23 information;
- 24           d. The inability to use their computing devices for the purpose of  
 25 communicating with their health care providers or covered entities;
- 26           e. The loss of privacy due to Meta making sensitive and confidential  
 27 information such as patient status and appointments that Plaintiffs and Class  
 28 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

covered entity's status as their health care providers or covered entities subject to federal and state health privacy laws, and the reasonable expectations of privacy that attach to such relationships, as evidenced by (among other things) federal laws such as HIPAA and California law protecting health information, and Meta's promise that it would "require" its Partners to have the right to share their data before Meta would collect it.

396. Plaintiffs' and Class members' claims include but are not limited to Meta's unauthorized access to following private facts:

- a. that Plaintiffs and Class members are patients of the various health care providers and covered entities;
- b. the dates and times Plaintiffs and Class members clicked to sign up, log in, or log out of the various health care providers' and covered entity patient portals;
- c. the dates and times that Plaintiffs and Class members scheduled appointments;
- d. the fact that Plaintiffs and Class members were scheduling appointments with their provider or covered entity;
- e. Plaintiffs' and Class members' communications with their health care providers or covered entity;
- f. Other health information associated with Plaintiffs and Class members, including but not limited to doctors, conditions, treatments, prognoses, symptoms, health insurance, and prescription drug information; and
- g. Plaintiffs' and Class members' communications exchanged while logged in to a patient portal.

397. In addition to acquiring Plaintiffs' and Class members' health information without authorization, Meta deposited the \_fbp cookie on Plaintiffs' and Class members' computing devices by disguising it as a first-party cookie associated with their health care provider or covered entity rather than a Meta cookie.

///



398. Meta's intrusion upon seclusion with respect to the \_fbp cookie occurred the moment that Meta caused the \_fbp cookie to be placed on Plaintiffs' and Class members' devices.

399. Meta's conduct was intentional and intruded on Plaintiffs' and Class members' medical communications which constitute private conversations, matters, and data.

400. Meta's conduct in acquiring patient portal, appointment, and other communications would be highly offensive to a reasonable person because:

- a. Meta conspired with Plaintiffs' and Class members' health care providers and covered entities to violate a cardinal rule of the provider-patient relationship;
- b. Meta's conduct violated federal and state laws designed to protect patient privacy, including HIPAA and the CMIA;
- c. Meta's conduct violated the ECPA; and
- d. Meta's conduct violated the express promises it made to Plaintiffs and Class members.

401. Plaintiffs and Class members seek all relief available for invasion of privacy claims under the California Constitution, including:

- a. Nominal damages;
- b. General privacy damages;
- c. The interruption or preclusion of Plaintiffs' and Class members' ability to communicate with their health care providers on their health care providers' or covered entity websites;
- d. The diminution in value of Plaintiffs' and Class members' protected health information;
- e. Plaintiffs and Class members' inability to use their computing devices for the purpose of communicating with their health care providers or covered entities;

///

///

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.

### **SEVENTH CLAIM FOR RELIEF**

#### **(Negligence per se)**

#### **By Plaintiffs on behalf of themselves and the Class**

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;

- c. when Plaintiffs and Class members click a number on a website to call their health care provider;
- d. Plaintiffs' and Class members' Internet Protocol address;
- e. Plaintiffs' and class members' c\_user cookie, which can be easily used to locate that individual's Facebook profile; and
- f. Plaintiffs' and Class members' datr cookie, which identifies the their specific web browser and is therefore a means of identifying Facebook users.

408. Meta also fails to meet the requirements of 45 CFR § 164.502(3) by using protected health information obtained via the Meta Pixel for marketing purposes without prior authorization. 45 CFR § 164.508(a)(3).

409. Plaintiffs and Class members are within the class of persons that HIPAA is intended to protect.

410. Plaintiffs' and Class members' injuries are the type of harm that HIPAA is intended to prevent.

411. Meta's violations of HIPAA therefore constitute negligence per se.

412. As a direct and proximate result of Meta's violations of HIPAA, Plaintiffs and members of the Class have suffered and continue to suffer serious injuries, including but not limited to:

- a. The loss of privacy of Plaintiffs' protected health information
- b. The interruption or preclusion of their ability to communicate with their health care providers on their health care providers' websites;
- c. Damaged relationships with their health care providers;
- d. Time and resources expended to investigate and respond to Meta's violations;
- e. The diminution in value of their protected health information; and
- f. Inability to use their computing devices for the purpose of communicating with their health care providers.

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.

///

1           434. Meta has engaged in unfair acts and practices under section 17200 because Meta  
2 claims it requires businesses to have the right to collect, use, and share Plaintiffs' and Class  
3 members' data before providing any data to Meta, but in reality knows (or should know) that its  
4 Pixel tracking tool is being used on health care provider and covered entity websites to  
5 contemporaneously redirect Plaintiffs' and Class members' communications without their  
6 knowledge or authorization.

7           435. Meta's actions offend public policy.

8           436. Meta's conduct, misrepresentations and omissions have also impaired competition  
9 within the health care market in that they have prevented Plaintiffs and Class members from  
10 making fully informed decisions about whether to communicate online with their health care  
11 providers and covered entities and to use their health care providers' and covered entity websites.

12           437. Plaintiffs and Class members have suffered injuries in fact, including the loss of  
13 money and/or property, as a result of Meta's deceptive, unfair, and unlawful practices. Plaintiffs'  
14 individually identifiable and health data has value, as demonstrated by Meta's use and sale of it.  
15 While only an identifiable "trifle" of injury need be shown, as set forth above Plaintiffs, Class  
16 members, and the public at large value their private health information at more than a trifle. The  
17 sale of this confidential and valuable information has diminished its value to Plaintiffs and the  
18 Class.

19           438. Meta's actions caused damage to and loss of Plaintiffs' and Class members'  
20 property by preventing them from controlling the dissemination and use of their individually  
21 identifiable health information and communications.

22           439. Had Plaintiffs and Class members known that Meta's representation that it requires  
23 businesses to have the right to collect, use, and share their data before providing any data to Meta  
24 was untrue, Plaintiffs and Class members would not have used their health care providers' or  
25 covered entity websites.

26           440. The wrongful conduct alleged herein occurred, and continues to occur, in the  
27 conduct of Meta's business. Meta's wrongful conduct is part of a pattern or generalized course of  
28 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 to 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);

///

///

- c. Treble the loss of value to their computing devices from the inability to use those devices for communicating with their health care providers or covered entities;
- d. The costs of bringing suit; and
- e. Reasonable attorney's fees.

465. Plaintiffs seek declaratory and injunctive relief, and reserve the right to amend to seek actual or statutory damages if Meta does not cure these violations within 30 days of receiving notice.

### **TWELFTH CLAIM FOR RELIEF**

**(Violation of the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502)**

**By Plaintiffs on behalf of themselves and the Class**

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

467. The California Comprehensive Computer Data Access and Fraud Act ("CDAFA") was enacted to provide protection from "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

468. The CDAFA affords a private right of action to owners of computers, systems, networks, programs, and data who suffer as a result of a violation of the Act. Cal. Penal Code § 502(e)(1).

469. The CDAFA imposes civil liability on anyone who:

- a. Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. Cal. Penal Code § 502(c)(1);
- b. Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes

or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2);

c. Knowingly and without permission uses or causes to be used computer services. Cal. Penal Code § 502(c)(3);

d. Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section. Cal. Penal Code § 502(c)(6);

e. Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. Cal. Penal Code § 502(c)(7); and

f. Knowingly introduces any computer contaminant into any computer, computer system, or computer network. Cal. Penal Code § 502(c)(8).

470. “Computer services” under the CDAFA “includes, but is not limited to, computer time, data processing, or storage functions, internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network.” Cal. Penal Code § 502(b)(4).

471. “Computer network” is “any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.” Cal. Penal Code § 502(b)(2).

472. “Computer system” is “a device or collection of devices, including support devices...one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.” Cal. Penal Code § 502(b)(5).

473. “Data” is defined as “a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions” that “may be in any form, in storage

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.

1           480. Plaintiffs' and Class members' data that Meta redirects through the Pixel includes  
 2 nonpublic information related to their communications with their health care providers and  
 3 covered entities, including that Plaintiffs and Class Members registered for and logged into patient  
 4 portals, scheduled health care appointments, and searched for physicians and information about  
 5 medical conditions.

6           481. Meta makes use of Plaintiffs' and Class members' data to obtain money through  
 7 advertising.

8           482. Meta's use of Plaintiffs' and Class members' data is wrongful in that the use is  
 9 prohibited by state and federal laws and Meta's own policies, including but not limited to:

- 10           a. the ECPA and Cal. Penal Code §§ 631 & 632;
- 11           b. HIPAA, including specifically 42 U.S.C. § 1320d-6;
- 12           c. various state health and computer privacy statutes, including but not limited  
 13 to the California Comprehensive Computer Data Access and Fraud Act  
 14 (Cal. Penal Code § 502); and
- 15           d. Meta's Terms of Service, Data Policy, and Cookie Policy.

16           483. Meta's use and access of Plaintiffs' and Class members' data, computers, computer  
 17 services, and computer networks, and Meta's introduction of the Pixel into Plaintiffs' and Class  
 18 members' computers, computer services, and computer networks is without permission because:

- 19           a. Plaintiffs and Class members never authorized Meta to place the \_fbp  
 20 cookie on their browser or otherwise access or use their data, computers,  
 21 computer services, and computer networks;
- 22           b. The Pixel was invisible to Plaintiffs and Class members;
- 23           c. Plaintiffs and Class members were unaware that Meta was using the Pixel  
 24 to surreptitiously access and use their data, computers, computer services,  
 25 and computer networks;
- 26           d. It was impossible for Plaintiffs and Class members to opt out of or prevent  
 27 the functionality of the Pixel;

28 ///



- e. Meta's own policies prohibit Meta from accessing and using Plaintiffs' and Class members' health information;
- f. Meta circumvented technical and code-based barriers to access and use Plaintiffs' and Class members' data, computers, computer services, and computer networks because the Pixel places the \_fbp cookie on Plaintiffs' and Class Members' computing devices, which is designed to disguise itself as a cookie from Plaintiffs and their health care providers and covered entities so that Meta can circumvent password-protected patient portals, cookie blockers, and other technical barriers; and
- g. Plaintiffs' and Class members' data that Meta accesses and uses is not publicly viewable and only became accessible to Meta through Meta's surreptitious and unauthorized placement of the \_fbp cookie on Plaintiffs' and Class members' computing devices.

484. As a result of Meta's violations of CDAFA, Plaintiffs and Class members suffered damages including but not limited to:

- a. The interruption or preclusion of their ability to communicate with their health care providers and covered entities on their health care providers' and covered entity websites;
- b. The diminution in value of their protected health information;
- c. The inability to use their computing devices for the purpose of communicating with their health care providers and covered entities.

485. Meta's violations of CDAFA were willful, fraudulent, or oppressive.

486. For Meta's violations of CDAFA, Plaintiffs and Class members seek actual damages, general damages, unjust enrichment, punitive damages, appropriate injunctive or other equitable relief pursuant to Cal. Penal Code § 502(e)(1) and any other relief the Court deems just.

487. Pursuant to Cal. Penal Code § 502(e)(2), Plaintiffs and Class Members also ask the Court to award them their reasonable attorney's fees.

///

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.

#### **SIGNATURE ATTESTATION**

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 Geoffrey Graber, CSB #211547  
2 Email: ggraber@cohenmilstein.com  
3 Eric Kafka, *Admitted Pro Hac Vice*  
4 Email: ekafka@cohenmilstein.com  
5 Claire Torchiana, CSB #330232  
6 Email: ctorchiana@cohenmilstein.com  
7 COHEN MILSTEIN SELLERS & TOLL PLLC  
8 1100 New York Avenue NW, Fifth Floor  
9 Washington, DC 20005  
10 Telephone: (202) 408-4600  
11 Facsimile: (202) 408-4699

12 Paul R. Kiesel, CSB #119854  
13 Email: kiesel@kiesel.law  
14 Jeffrey A. Koncius, CSB #189803  
15 Email: koncius@kiesel.law  
16 Nicole Ramirez, CSB #279017  
17 Email: ramirez@kiesel.law  
18 KIESEL LAW LLP  
19 8648 Wilshire Boulevard  
20 Beverly Hills, California 90211-2910  
21 Telephone: (310) 854-4444  
22 Facsimile: (310) 854-0812

23 Beth E. Terrell, CSB #178181  
24 Email: bterrell@terrellmarshall.com  
25 Amanda M. Steiner, CSB #190047  
26 Email: asteiner@terrellmarshall.com  
27 Benjamin M. Drachler, *Pro Hac Vice Pending*  
28 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*

# **EXHIBIT “A”**

KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California

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

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

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

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

*Attorneys for Plaintiffs*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

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

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

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

CLASS ACTION

**DECLARATION OF RICHARD M. SMITH IN  
SUPPORT OF PLAINTIFFS' MOTION FOR  
PRELIMINARY INJUNCTION**

Date: October 5, 2022

Time: 2:00 p.m.

Crtrm.: 2, 17th Floor

Judge: Hon. William H. Orrick

**TABLE OF CONTENTS**

1		
2	DECLARATION OF RICHARD M. SMITH .....	3
3	Summary of Opinions and Conclusions.....	3
4	Introduction to the Meta Pixel.....	4
5	How the Meta Pixel Works on a Medical Provider’s Website .....	9
6	Web Technologies.....	26
7	Developer Tools for Observing the Communications Between a Web Browser and Web Servers .....	35
8	Browser Cookies .....	36
9	IP Addresses.....	41
10	Web Page and Web Form Scraping .....	48
11	Cookie Syncing .....	65
12	Cross-device Tracking.....	69
13	How the Meta Pixel operates when not logged into Facebook.....	71
14	Tracking Pixels and HIPAA.....	73
15	Privacy and Security Problems at Facebook.com .....	75
16	The use of the Meta Pixel at other Hospital Web sites .....	79
17	Health-related Ad Targeting at Facebook.com .....	86
18	Hospital Web sites who have recently removed the Meta Pixel .....	104
19	Summary .....	106
20		
21		
22		
23		
24		
25		
26		
27		
28		



## DECLARATION OF RICHARD M. SMITH

1  
2 1. My name is Richard M. Smith and I am of sound mind, over the age of eighteen years  
3 old, capable of making this Declaration, and personally acquainted with the facts stated herein.

4 2. I am currently the owner and a consultant with Boston Software Forensics LLC of  
5 Boston, Massachusetts. For approximately the last 17 years, I have been providing consulting  
6 services to the legal industry. These consulting services primarily involve the analysis of software  
7 systems to understand how they operate. My consulting services have been employed in areas such  
8 as IP-related litigation and privacy and security reviews. Previously I have worked at the Privacy  
9 Foundation as the chief technology officer (CTO) and I was a founder and CEO of Phar Lap  
10 Software, Inc. I have a Bachelor of Science degree in Computer Science from North Carolina State  
11 University, class of 1974. I began working in the computer software field in 1972.

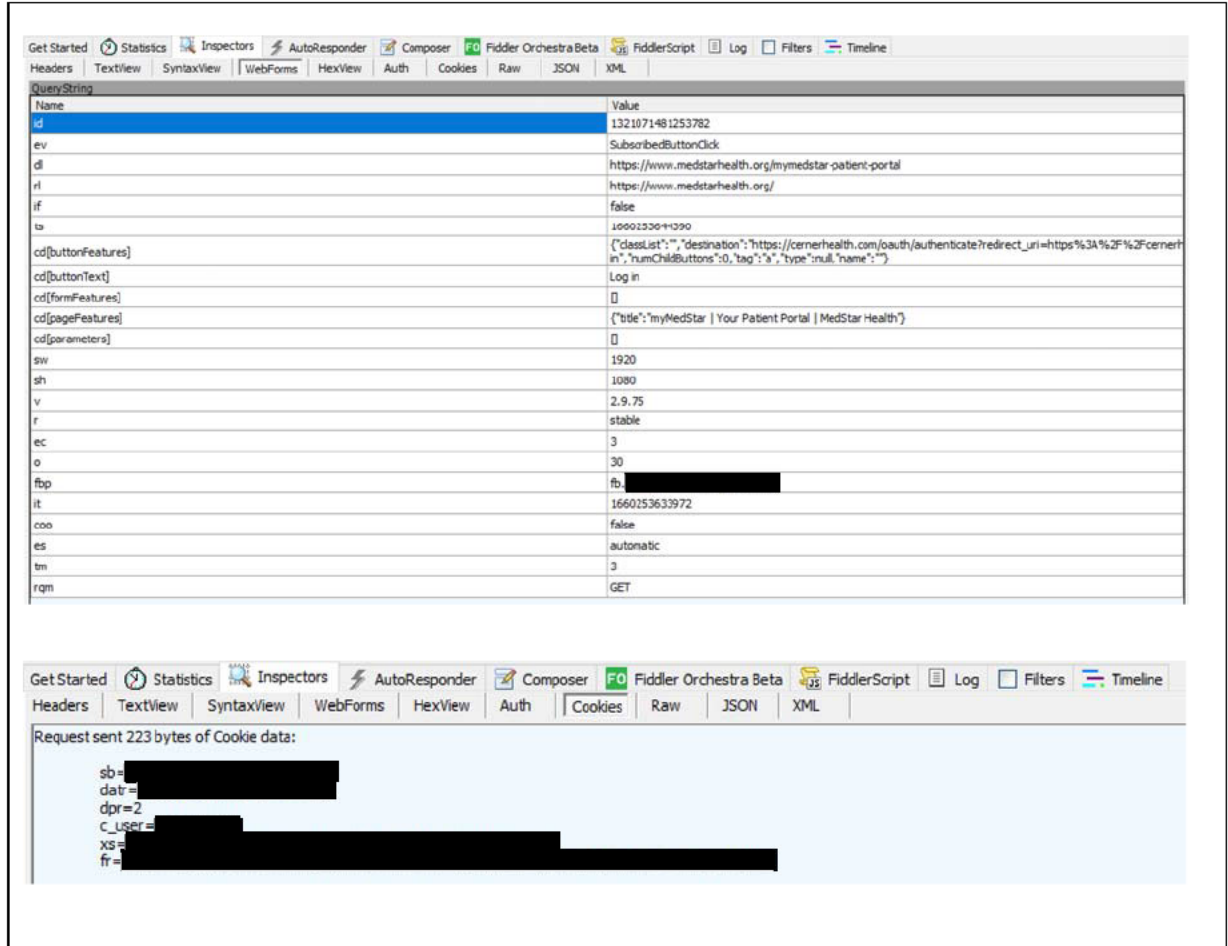
12 3. In this declaration, I have analyzed the tracking of the communications between  
13 patients with the hospitals by Meta using the Meta Pixel.

**Summary of Opinions and Conclusions**

14  
15 4. Meta acquires patient Protected Health Information (PHI) through the use of the  
16 Meta Pixel on the websites of HIPAA-covered entities, including but not limited to:

- 17 a. MedStar Health – medstarhealth.org
- 18 b. Rush University System for Health - rush.edu
- 19 c. Hartford HealthCare - hartfordhospital.org
- 20 d. Summa Health System - www.summahealth.org
- 21 e. University Hospitals - www.uhhospitals.org

22 5. Meta acquires the patient status of individuals logging into the “patient portals” of  
23 their providers through click data, including the Meta Pixel “SubscribedButtonClick” as illustrated  
24 by the following HTTP GET request parameters for a Meta Pixel used on the MedStar Health patient  
25 portal home page:



6. The patient PHI that Meta acquires through the Meta Pixel is used for marketing purposes, including targeted advertising.

### Introduction to the Meta Pixel

7. The Meta Pixel<sup>1</sup> is an Internet marketing tool designed by Meta that developers incorporate into their websites to aid their Internet marketing efforts. Meta explains:

<sup>1</sup> The Meta Pixel is formerly known as the Facebook Pixel. See *How to Set Up Meta Pixel (Formerly Facebook Pixel)* at <https://blog.hootsuite.com/facebook-pixel/>. The Meta Pixel continues to rely on Facebook cookies, Facebook JavaScript code, and Facebook servers.

## About Meta Pixel

53,870 views

If you already set up your Meta Pixel using IMG tags or plan to do so, we recommend that you follow our developer documentation. [Learn more.](#)

The Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website.

You can use the Meta Pixel to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales.** Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.



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.

Source: <https://www.facebook.com/business/help/742478679120153>

8. As Meta explains, “[t]he Meta Pixel is a snippet of JavaScript code that allows you to track visitor activity on your website.”:

## Meta Pixel

The Meta Pixel is a snippet of JavaScript code that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an **event**) that you want to track (called a **conversion**). Tracked conversions appear in the [Ads Manager](#) where they can be used to measure the effectiveness of your ads, to define [custom audiences](#) for ad targeting, for [Advantage+ catalog ads](#) campaigns, and to analyze that effectiveness of your website's conversion funnels.

Source: <https://developers.facebook.com/docs/meta-pixel/>

9. The Meta Pixel has vast capabilities and can collect a large range of user data, including:

The Meta Pixel can collect the following data:

- **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website.
- **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
- **Button Click Data** – Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.
- **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are **conversion value**, **page type** and more.
- **Form Field Names** – Includes website field names like **email**, **address**, **quantity**, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of **Advanced Matching** or optional values.

Source: <https://developers.facebook.com/docs/meta-pixel/>

10. The Pixel works by “loading a small library of functions which you can use whenever a site visitor takes an action (called an **event**) that you want to track (called a **conversion**).” (emphasis in original).

## Meta Pixel

The Meta Pixel is a snippet of JavaScript code that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an **event**) that you want to track (called a **conversion**). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that effectiveness of your website's conversion funnels.

Source: <https://developers.facebook.com/docs/meta-pixel/>

11. The Meta Pixel was announced on October 14, 2015:

# Announcing Facebook Pixel

October 14, 2015

By [Cecile Ho](#)



[Subscribe to Ads news](#)

Today we're announcing the Facebook pixel, a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website. We're also announcing the availability of custom conversions, a new rule-based method to track and report conversions for your Facebook ads.

Facebook pixel makes things simple for advertisers by combining the functionality of the Conversion Tracking pixels and Custom Audience pixels into a single pixel. You only need to place a single pixel across your entire website to report and optimize for conversions. Since it is built on top of the upgraded Custom Audience pixel, all the features announced in our previous blog post ([Announcing Upgrades to Conversion Tracking and Optimization at Facebook](#)) are supported through Facebook pixel as well.

You can use Facebook pixel to track and optimize for conversions by adding [standard events](#) (e.g. Purchase) to your Facebook pixel base code on appropriate pages (e.g. purchase confirmation page).

Source: <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/>

12. The Meta Pixel gained new functionality in May 2017 when Facebook “enhanced” its capabilities such that that it would start transmitting additional information to Facebook, including “actions on your page, like ‘add to cart’ or ‘purchase’ clicks, and will also include information from your page's structure to better understand context associated with these actions:



## What's changing with the Facebook pixel?

We're enhancing the Facebook pixel to improve Facebook's delivery of relevant and useful ads and how those results are measured. The Facebook pixel will start sending more contextual information from your website to better understand and categorize the actions that people take on your site to optimize for ads delivery.

The additional information sent through pixel will include actions on your page, like "add to cart" or "purchase" clicks, and will also include information from your page's structure to better understand context associated with these actions.

If you created your Facebook pixel before April 20, 2017, this new functionality will go into effect on **May 20, 2017**. For Facebook pixels created on **April 20, 2017** or later, this change will take effect immediately.

You can learn more about these changes in the [Facebook Developers site](#).

Source:

<https://web.archive.org/web/20170729045537/https://www.facebook.com/business/help/1292598407460746>

13. Meta programmed these changes so they would occur by default unless the developer deploying the Pixel reconfigures it to "Manual Only mode":

### Automatic Configuration

Starting on **May 19, 2017**, the Facebook Pixel will be able to send button click data and page metadata from your website to improve your ads delivery and measurement with no further code changes required. If you'd like to configure the Facebook Pixel to Manual Only mode, you can add the line `fbq('set', 'autoConfig', 'false', 'FB_PIXEL_ID')` above the `init` call in the Facebook Pixel Base code and the Facebook Pixel will no longer send this additional data. Example below:

Source:

<https://web.archive.org/web/20170827002341/https://developers.facebook.com/docs/facebook-pixel/api-reference>

14. This new enhanced click monitoring, through an event called a `SubscribedButtonClick`, "fire[s] on every click a user performs on your site, sending the button text as a parameter (`buttonText`), together with some other potential data (`buttonFeatures` parameter), like `id`, `tag`, `value`. There's also a `formFeatures` adding additional info."

## The SubscribedButtonClick Event

It will fire on every click a user performs on your site, sending the button text as a parameter (buttonText), together with some other potential data (buttonFeatures parameter), like id, tag, value. There's also a formFeatures adding additional info.

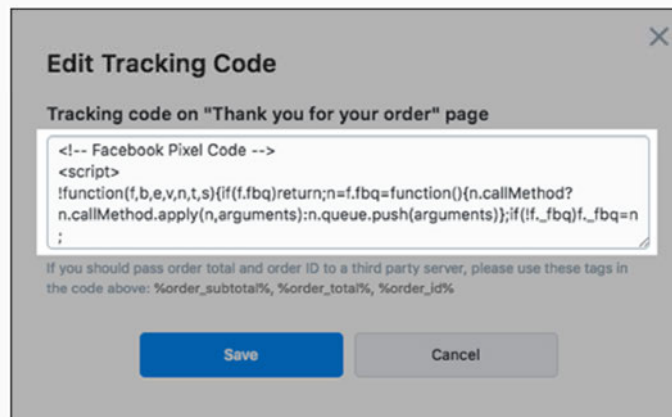
Source: <https://www.pixelyoursite.com/major-facebook-pixel-update-automatic-facebook-pixel-events>

## How the Meta Pixel Works on a Medical Provider's Website

15. The Meta Pixel is an example of a tracking pixel<sup>2</sup>:

### What is a Tracking Pixel?

Marketing pixels, aka tracking pixels, are essentially these tiny snippets of code that allow you to gather information about visitors on a website—how they browse, what type of ads they click on, etc.



This behavior data helps you, as a marketer, send the user paid ads that are likely to be most interesting to them. Tracking pixels are also used to measure a marketing campaign's performance, track conversions, and build an audience base.

Now that you have a general overview of what a pixel is, let's talk about the different types of pixels. Don't stress too much though, there are only 2 that you really need to worry about.

Source: <https://www.digitalmarketer.com/blog/what-is-tracking-pixel/>

16. The "pixel" of a tracking pixel refers to the fact that a tracking pixel can be a 1-by-1

<sup>2</sup> Tracking pixels also go under other names such as Web bugs, Web beacons, pixel tags, and spy pixels.

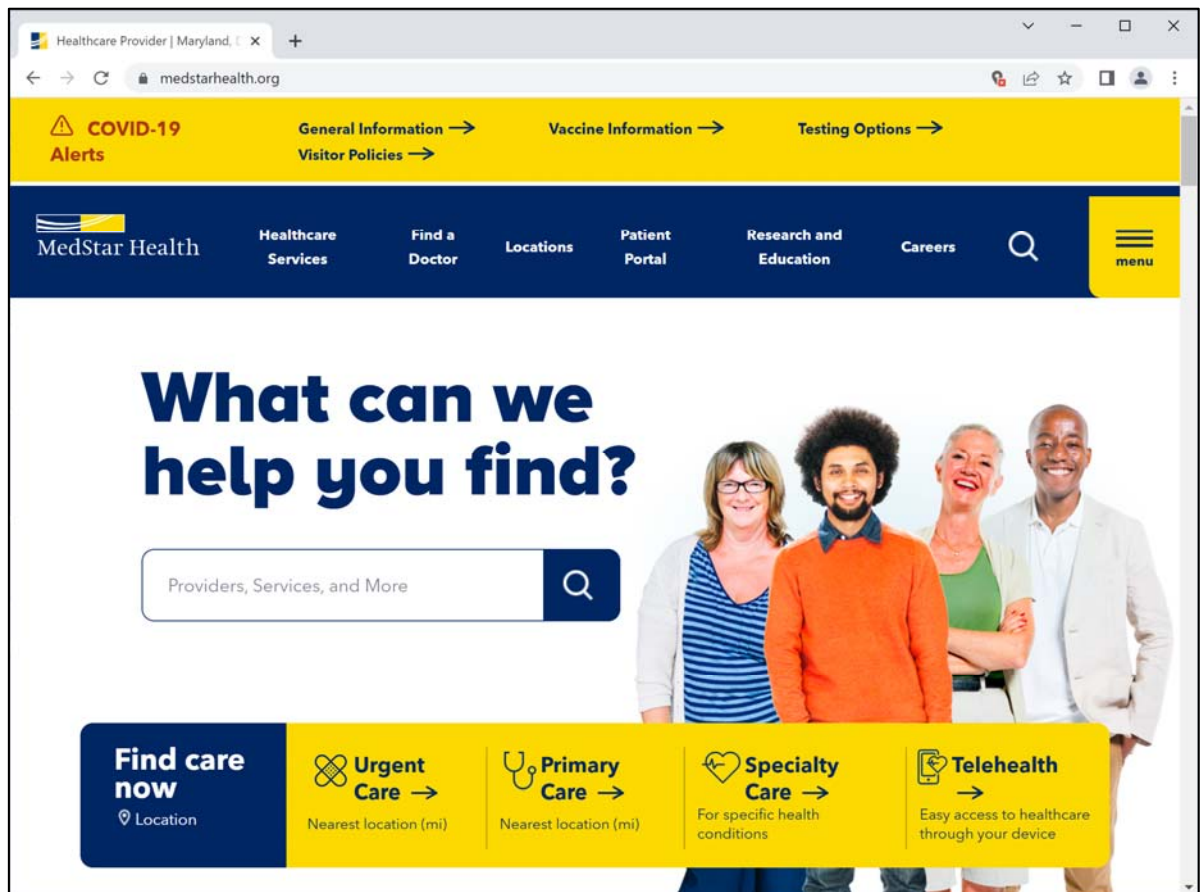


1 pixel image on a Web page which is typically invisible to the human eye.

2 17. The Meta Pixel makes use of Web technologies, which are described later in this  
3 declaration, which include:

- 4 a. The HTTP protocol (See the section *Web Technologies*)
- 5 b. URLs (See the section *Web Technologies*)
- 6 c. Query strings (See the section *Web Technologies*)
- 7 d. JavaScript (See the section *Web Technologies*)
- 8 e. Posted form data (See the section *Web Technologies*)
- 9 f. Browser cookies (See the section *Browser Cookies*)
- 10 g. IP addresses (See the section *IP Addresses*)

11 18. MedStar Health operates a Web site at the host [www.medstarhealth.org](http://www.medstarhealth.org) to  
12 communicate with patients and others. The following screen shot shows the home page of the  
13 MedStar Health Web site from August 2022:



Source: <https://www.medstarhealth.org/>

19. The MedStar Health Web site employs the Meta pixel.<sup>3</sup>

20. For example, MedStar Health includes JavaScript code from Facebook at [www.medstarhealth.org](https://www.medstarhealth.org). The JavaScript file from Facebook that MedStar Health causes to be fetched is named “fbevents.js”. As illustrated in the HTTP GET request, this is fetched from the server connect.facebook.net:

Request #201

GET [https://connect.facebook.net/en\\_US/fbevents.js](https://connect.facebook.net/en_US/fbevents.js) HTTP/1.1

Host: connect.facebook.net

Connection: keep-alive

sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

sec-ch-ua-platform: "Windows"

Accept: \*/\*

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: script

Referer: <https://www.medstarhealth.org/>

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

21. The fbevents.js file includes a Facebook copyright notice:

/\*\*

\* Copyright (c) 2017-present, Facebook, Inc. All rights reserved.

\*

\* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,  
\* copy, modify, and distribute this software in source code or binary form for use  
\* in connection with the web services and APIs provided by Facebook.

\*

\* As with any software that integrates with the Facebook platform, your use of  
\* this software is subject to the Facebook Platform Policy  
\* [<http://developers.facebook.com/policy/>]. This copyright notice shall be  
\* included in all copies or substantial portions of the software.

\*

<sup>3</sup> Prior to November 13, 2021, MedStar Health did not disclose the use of the Meta Pixel on its websites. MedStar’s new “Online Privacy Policy” now directs patients to the advertising settings in their Facebook accounts in order to “unlink” their Facebook account from the MedStar website. <https://www.medstarhealth.org/online-privacy-policy>

1       \* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY  
 2       KIND, EXPRESS OR  
 3       \* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF  
 4       MERCHANTABILITY, FITNESS  
 5       \* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT  
 6       SHALL THE AUTHORS OR  
 7       \* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER  
 8       LIABILITY, WHETHER  
 9       \* IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT  
 10       OF OR IN  
 11       \* CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN  
 12       THE SOFTWARE.  
 13       \*/

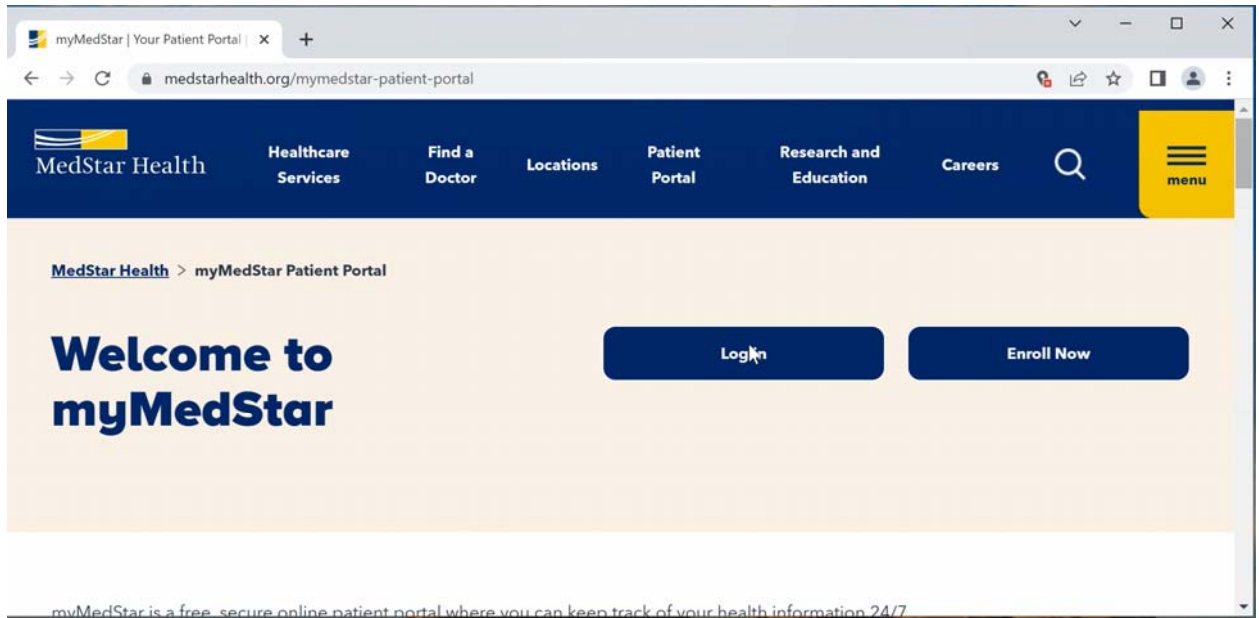
14       22. Unless otherwise noted, the HTTP requests and responses that are shown in this  
 15       declaration for MedStar Health were excerpted from the Fiddler capture file named "MedStar-2022-  
 16       08-11.saz".<sup>4</sup> Fiddler capture files are described in more detail in the section of this declaration  
 17       entitled "Developer Tools for observing the communications between a Web browser and Web  
 18       servers".

19       23. The referer HTTP header ("Referer: <https://www.medstarhealth.org/>") of the HTTP  
 20       GET request for the fbevents.js file indicates that a browser has been instructed to fetch fbevents.js  
 21       by HTML and JavaScript coding in a MedStar Health Web page.

22       24. The Facebook JavaScript code from the fbevents.js then executes inside a patient's  
 23       Web browser in the context of the MedStar Health home page and other pages at the Medstar web  
 24       properties, without any action or knowledge of the patient.

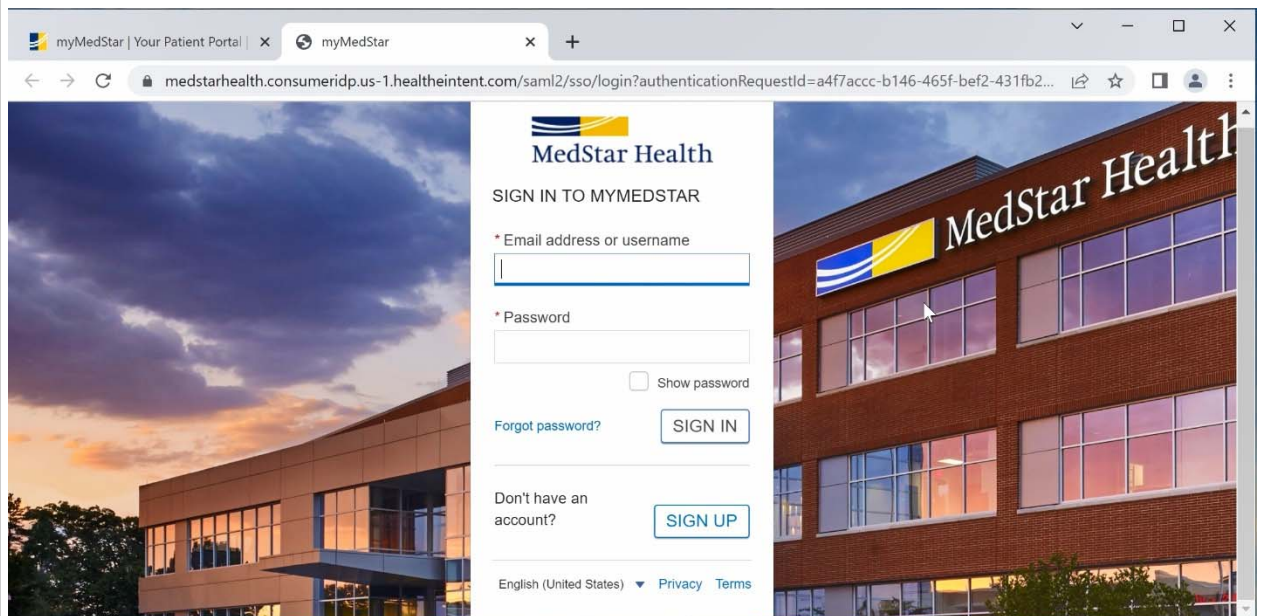
25       25. The following is a screen shot of the myMedStar Patient Portal home page with the  
 26       "Log In" button about to be pushed:

27       <sup>4</sup> This Fiddler capture file, along with those discussed below, have been produced confidentially to  
 28       Meta's counsel and are available to the Court upon request.



Source: <https://www.medstarhealth.org/mymedstar-patient-portal>

26. Pressing the Log In button takes a patient to the login page where they can log into their MedStar patient portal account using their username or email address and a password:



Source: <https://cernerhealth.com/oauth/authenticate>

27. When the Log In button is pressed, from the execution of the Facebook JavaScript code, a patient's Web browser is further redirected by Facebook's source code to fetch an invisible tracking pixel. The following is an example of an HTTP GET request to fetch a Meta Pixel on the MedStar Health patient portal home page:



Request #879

GET

https://www.facebook.com/tr/?id=1321071481253782&ev=SubscribedButtonClick&dl=ht  
tps%3A%2F%2Fwww.medstarhealth.org%2Fmymedstar-patient-  
portal&rl=https%3A%2F%2Fwww.medstarhealth.org%2F&if=false&ts=1660253644390  
&cd[buttonFeatures]=%7B%22classList%22%3A%22%22%2C%22destination%22%3A  
%22https%3A%2F%2Fcernerhealth.com%2Foauth%2Fauthenticate%3Fredirect\_uri%3D  
https%253A%252F%252Fcernerhealth.com%252Fsaml%252Fsso%252Fresponse%252F  
message\_id%2526issuer%253Dhttps%25253A%25252F%25252Fmymedstar.iqhealth.c  
om%25252Fsession-  
api%25252Fprotocol%25252Fsaml2%25252Fmetadata%26sign\_in\_only%3Don%26client  
id%3Dae737c6564c345c2b9ac1294f98c75c0%22%2C%22id%22%3A%22%22%2C%2  
2imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Log%20in%22%2C%22nu  
mChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2  
C%22name%22%3A%22%22%27D&cd[buttonText]=Log%20in&cd[formFeatures]=%5B  
%5D&cd[pageFeatures]=%7B%22title%22%3A%22myMedStar%20%7C%20Your%20P  
atient%20Portal%20%7C%20MedStar%20Health%22%27D&cd[parameters]=%5B%5D&  
sw=1920&sh=1080&v=2.9.75&r=stable&ec=3&o=30&fbp=fb  
&it=1660253633972&coo=false&es=automatic&tm=3&rqm=GET HTTP/1.1

Host: www.facebook.com

Connection: keep-alive

sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36  
(KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

sec-ch-ua-platform: "Windows"

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: image

Referer: https://www.medstarhealth.org/

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Cookie: sb=[REDACTED]; datr=[REDACTED];

dpr=2; c\_user=[REDACTED]; xs=[REDACTED];

[REDACTED];

[REDACTED];

[REDACTED];

[REDACTED];

28. Shown in yellow in the HTTP request are facebook.com cookie values used to track a user. Shown in green is text scraped from the patient portal home page which indicates that the Meta pixel is tracking a login attempt at the MedStar patient portal. The contents of the Meta Pixel are described in more detail below.

29. The returned image file for a tracking pixel is typically 1 by 1 pixel in size, i.e. a single dot on a screen, and either is never displayed or hidden from view. For example, a facebook.com server returns a 44-byte image file which is 1-by-1 pixel in size as highlighted in

1 yellow:

2 HTTP/1.1 200 OK  
 3 Content-Type: image/gif  
 4 Date: Thu, 11 Aug 2022 21:34:04 GMT  
 5 Expires: Thu, 11 Aug 2022 21:34:04 GMT  
 6 Last-Modified: Fri, 21 Dec 2012 00:00:01 GMT  
 7 Cache-Control: no-cache, must-revalidate, max-age=0  
 8 Set-Cookie:  
 Strict-Transport-Security: max-age=31536000; includeSubDomains  
 Cross-Origin-Resource-Policy: cross-origin  
 Server: proxygen-bolt  
 Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
 Connection: keep-alive  
 Content-Length: 44  
 9 File size: 44 bytes  
 10 Dimensions: 1H x 1W  
 No EXIF data

11  
 12 30. The purpose of a tracking pixel is typically to provide tracking information about a  
 13 Web site and a visitor to a third-party, in this case, Facebook. The tracking information is provided  
 14 to the third-party server in the HTTP GET request for the tracking pixel.

15 31. The following information is provided for tracking purposes to a third-party server  
 16 when a Web browser is redirected to fetch a tracking pixel<sup>5</sup>:

- 17 a. The IP address associated with a user's browser. IP addresses are described  
 18 below.
- 19 b. A URL which typically contains coded information about the Web page  
 20 being visited, a user's browser, a user's device, and/or the user of the Web site
- 21 c. The referring URL which is typically the URL containing the host name of  
 22 the Web page being tracked
- 23 d. Identification of the browser, browser version, and device type being used by  
 24 the visitor in the "user-agent" HTTP header; and
- 25 e. Any browser cookies which have been set previously by the third-party server

26  
 27 <sup>5</sup> Information associated with a tracking pixel can be combined in a process known as device,  
 28 system, or browser fingerprinting to uniquely identify a particular user.

1 (optional).

2 32. In the URL for the Meta Pixel, examples of parameters sent in the query string of the  
3 URL include:

4 https://www.facebook.com/tr/?id=1321071481253782&ev=SubscribedButtonClick&dl=https  
5 %3A%2F%2Fwww.medstarhealth.org%2Fmymedstar-patient-  
6 portal&rl=https%3A%2F%2Fwww.medstarhealth.org%2F&if=false&ts=1660253644390&cd[  
7 buttonFeatures]=%7B%22classList%22%3A%22%22%2C%22destination%22%3A%22https  
8 %3A%2F%2Fcernerhealth.com%2Foauth%2Fauthenticate%3Fredirect\_uri%3Dhttps%253A%  
9 252F%252Fcernerhealth.com%252Fsaml%252Fsso%252Fresponse%253Fmessage\_id%  
10 %2526issuer%253Dhttps%25253A%25252F%25252Fmymedstar.iqhealth.com  
11 %25252Fsession-  
12 api%25252Fprotocol%25252Fsaml2%25252Fmetadata%26sign\_in\_only%3Don%26client\_id  
13 %3Dae737c6564c345c2b9ac1294f98c75c0%22%2C%22id%22%3A%22%22%2C%22image  
14 Url%22%3A%22%22%2C%22innerText%22%3A%22Log%20in%22%2C%22numChildButt  
15 ons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22  
16 %3A%22%22%7D&cd[buttonText]=Log%20in&cd[formFeatures]=%5B%5D&cd[pageFeatu  
17 res]=%7B%22title%22%3A%22myMedStar%20%7C%20Your%20Patient%20Portal%20%7  
18 C%20MedStar%20Health%22%7D&cd[parameters]=%5B%5D&sw=1920&sh=1080&v=2.9.  
19 75&r=stable&ec=3&o=30&fbp=fb [REDACTED]&it=1660253633972&coo=f  
20 else&es=automatic&tm=3&rqm=GET

21 The following is a chart of many of the data parameters included in the above URL and their  
22 values:

Parameter name	Value
id	Id number of the tracking pixel
ev	SubscribedButtonClick event type
dl	URL of the MedStar Health patient portal home page: https://www.medstarhealth.org/mymedstar-patient-portal
rl	The referring URL to the patient portal home page https://www.medstarhealth.org/
destination	URL of the MedStar Health patient port login page: https://cernerhealth.com/oauth/authenticate ...
innerText	“Log in” button text
cd[buttonText]	“Log in” button text
title	Title of the Web page “myMedStar   Your Patient Portal   MedStar Health”



fbp	_fbp first-party cookie value (Described below in the section <i>Cookie Syncing</i> )
sw	Screen width: 1920 pixels
sh	Screen height: 1080 pixels

33. Third-party Facebook.com names and cookie values sent with the Meta Pixel HTTP GET request are:

Cookie: sb=[REDACTED]; datr=[REDACTED];  
dpr=2; c\_user=[REDACTED]; xs=[REDACTED]  
[REDACTED];

fr=[REDACTED]  
[REDACTED]

34. The “c\_user” cookie contains a numerical value, known as a Facebook ID or FBID, which uniquely identifies a Facebook user. Each Facebook account holder has a single, unique c\_user value associated with the account.

35. The c\_user cookie allows Meta to correlate a particular visitor’s use of the MedStar Health Web site with the visitor’s Facebook profile, their use of the Facebook Web site, and their use of other Web sites which also employ Meta Pixels.

36. Any Facebook account can be identified, by name, through the c\_user value. For example, the c\_user cookie value for Mark Zuckerberg is 4. Logging in to Facebook and typing www.facebook.com/4 in the web browser automatically redirects the browser to Mark Zuckerberg’s Facebook page: www.facebook.com/zuck.

37. Another cookie is the “datr” cookie, which is a unique id number for the browser which visited the MedStar Health Web site which Meta associates with each Facebook user’s account.

38. Facebook account holders can now use the “Download Your Information” (“DYI”) tool to view each datr cookie associated with their account. The DYI tool also allows users to see additional information associated with their account, including IP addresses, event information, and

login/logout information.<sup>6</sup>

39. See also Appendix 1 of *Facebook Technical Analysis Report* by Dave O'Reilly and *Facebook Tracking Through Social Plug-ins* (24 June 2015). These two reports provide a technical analysis of Facebook tracking cookies such as the “datr”, “xs”, and “fr” cookies. For example:

**Table 2:** The list of cookies sent to Facebook when a logged in user visits a page with social plug-ins.

Name	Sample Value	Contains	Expires	Secure <sup>†</sup>
c_user	100004223456398	Facebook ID	Session/ 1 Month <sup>†</sup>	Yes
datr	S3fJVgeTh7_ikK5frtHsHPmE	Browser ID	2 Years	No
fr	0goRJJKaszKOLdKz8.AWXGHlRrxSLM3P HeHxfrORv10H8.BCVChV.Sj.FUJ.0.AW WSuv8a	Encrypted Facebook ID and Browser ID*	1 Month	No
xs	244%3AjIZKp45fK9ceMA%3A2%3A14267 05088%3A3455	Session number and secret*	Session/ 1 Month <sup>†</sup>	Yes

Source: *Facebook Tracking Through Social Plug-ins* (24 June 2015), page 14

40. On the Facebook Web site, Meta also discloses at a high-level how it uses cookies at the Web page *Cookies & other storage technologies* for “personalizing content”, “tailoring and measuring ads”, “show you the appropriate experience and features”, “show ads”, “make recommendations for businesses”, “help deliver ads”, “deliver, measure and improve the relevancy of ads”, “measure how often people do things”, “calculate the cost of those ads”, “providing advertising and site analytics services”, and “our business partners may also choose to share information with Meta”:

<sup>6</sup> <https://www.zdnet.com/article/europe-versus-facebook-new-download-tool-is-not-enough/>

## Why do we use cookies?

Cookies help us provide, protect and improve the Meta Products, such as by personalising content, tailoring and measuring ads, and providing a safer experience. The cookies that we use include session cookies, which are deleted when you close your browser, and persistent cookies, which stay in your browser until they expire or you delete them. While the cookies that we use may change from time to time as we improve and update the Meta Products, we use them for the following purposes:

### Authentication

We use cookies to verify your account and determine when you're logged in so that we can make it easier for you to access the Meta Products and show you the appropriate experience and features.

*For example:* We use cookies to keep you logged in as you navigate between Facebook Pages. Cookies also help us remember your browser so you don't have to keep logging in to Facebook and so you can more easily log in to Facebook via third-party apps and websites. For example, we use the "c\_user" and "xs" cookies, including for this purpose, which have a lifespan of 365 days.

**Security, site and product integrity**

We use cookies to help us keep your account, data and the Meta Products safe and secure.

*For example:* Cookies can help us identify and impose additional security measures when someone may be attempting to access a Facebook account without authorisation, for instance, by rapidly guessing different passwords. We also use cookies to store information that allows us to recover your account in the event that you forget your password or to require additional authentication if you tell us that your account has been hacked. This includes, for example, our "sb" and "dbln" cookies, which enable us to identify your browser securely.

We also use cookies to combat activity that violates our policies or otherwise degrades our ability to provide the Meta Products.

*For example:* Cookies help us fight spam and phishing attacks by enabling us to identify computers that are used to create large numbers of fake Facebook accounts. We also use cookies to detect computers infected with malware and to take steps to prevent them from causing further harm. Our "csrf" cookie, for example, helps us prevent cross-site request forgery attacks. Cookies also help us prevent underage people from registering for Facebook accounts.



**Advertising, recommendations, insights and measurement**

We use cookies to help us show ads and to make recommendations for businesses and other organisations to people who may be interested in the products, services or causes they promote.

*For example:* Cookies allow us to help deliver ads to people who have previously visited a business's website, purchased its products or used its apps and to recommend products and services based on that activity. Cookies also allow us to limit the number of times that you see an ad so you don't see the same ad over and over again. For example, the "fr" cookie is used to deliver, measure and improve the relevancy of ads, with a lifespan of 90 days.

We also use cookies to help measure the performance of ad campaigns for businesses that use the Meta Products.

*For example:* We use cookies to count the number of times that an ad is shown and to calculate the cost of those ads. We also use cookies to measure how often people do things, such as make a purchase following an ad impression. For example, the "\_fbp" cookie identifies browsers for the purposes of providing advertising and site analytics services and has a lifespan of 90 days.

Cookies help us serve and measure ads across different browsers and devices used by the same person.

*For example:* We can use cookies to prevent you from seeing the same ad over and over again across the different devices that you use.

1 Cookies also allow us to provide insights about the people who use the  
2 Meta Products, as well as the people who interact with the ads, websites  
3 and apps of our advertisers and the businesses that use the Meta  
4 Products.

5 *For example:* We use cookies to help businesses understand  
6 the kinds of people who like their Facebook Page or use their  
7 apps so that they can provide more relevant content and  
8 develop features that are likely to be interesting to their  
9 customers.

10 We also use cookies, such as our "oo" cookie, which has a lifespan of five  
11 years, to help you opt out of seeing ads from Meta based on your activity  
12 on third-party websites. Learn more about the information we receive,  
13 how we decide which ads to show you on and off the Meta Products and  
14 the controls that are available to you.  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**Site features and services**

We use cookies to enable the functionality that helps us provide the Meta Products.

*For example:* Cookies help us store preferences, know when you've seen or interacted with Meta Products' content and provide you with customised content and experiences. For instance, cookies allow us to make suggestions to you and others, and to customise content on third-party sites that integrate our social plugins. If you are a Facebook Page administrator, cookies allow you to switch between posting from your personal Facebook account and the Facebook Page. We use cookies such as the session-based "presence" cookie to support your use of Messenger chat windows.

We also use cookies to help provide you with content relevant to your locale.

*For example:* We store information in a cookie that is placed on your browser or device so that you will see the site in your preferred language.



**Performance**

We use cookies to provide you with the best experience possible.

*For example:* Cookies help us route traffic between servers and understand how quickly Meta Products load for different people. Cookies also help us record the ratio and dimensions of your screen and windows and know whether you've enabled high-contrast mode, so that we can render our sites and apps correctly. For example, we set the "dpr" and "wd" cookies, each with a lifespan of 7 days, for purposes including to deliver an optimal experience for your device's screen.

**Analytics and research**

We use cookies to better understand how people use the Meta Products so that we can improve them.

*For example:* Cookies can help us understand how people use the Facebook service, analyse which parts of our Products people find most useful and engaging, and identify features that could be improved.

**Third-party websites and apps**

Our business partners may also choose to share information with Meta from cookies set in their own websites' domains, whether or not you have a Facebook account or are logged in. Specifically, cookies named \_fbclid or \_fbp may be set on the domain of the business partner whose site you're visiting. Unlike cookies that are set on Meta's own domains, these cookies aren't accessible by Meta when you're on a site other than the one on which they were set, including when you are on one of our domains. They serve the same purposes as cookies set in Meta's own domain, which are to personalise content (including ads), measure ads, produce analytics and provide a safer experience, as set out in this Cookies Policy.

## Where do we use cookies?

We may place cookies on your computer or device and receive information stored in cookies when you use or visit:

- The Meta Products;
- Products provided by other members of the Meta Companies; and
- Websites and apps provided by other companies that use the Meta Products, including companies that incorporate Meta technologies into their websites and apps. Meta uses cookies and receives information when you visit those sites and apps, including device information and information about your activity, without any further action from you. This occurs whether or not you have a Facebook account or are logged in.

Source: <https://www.facebook.com/policy/cookies>

41. In order to access the *Cookies & other storage technologies* Web page, I was required to log into the Facebook Web site.

42. Meta describes for developers on their Web site information sent to Facebook servers by the Meta Pixel including button click data:

# Meta Pixel

The Meta Pixel is a snippet of JavaScript code that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an **event**) that you want to track (called a **conversion**). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that effectiveness of your website's conversion funnels.

The Meta Pixel can collect the following data:

- **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website.
- **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
- **Button Click Data** – Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.
- **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
- **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.

Source: <https://developers.facebook.com/docs/meta-pixel>

43. The same kind of tracking information provided with tracking pixels can also be included in other kinds of HTTP requests such as:

- a. HTTP POST requests used for making API calls from a browser to a server;
- b. HTTP GET requests for JavaScript files;
- c. HTTP GET requests for hidden IFRAMEs;
- d. HTTP GET requests for visible IFRAMEs; or
- e. HTTP GET requests for visible images

## Web Technologies

44. Internet users use Web browsers to send, receive, and view electronic communications on the Internet. Web browsers are software applications which run on computing devices such as laptop computers, desktop computers, smartphones, and tablet computers.

45. Examples of popular Web browsers include Chrome, Safari, Firefox, and Edge.

46. A Web site is hosted by a computer server through which the Web site sends and receives communications with Internet users via their Web browsers to display Web pages on users'

monitors and screens of their chosen computing devices.

47. At the MedStar Health Web site (<https://www.medstarhealth.org>), visitors, including current and prospective patients, can get information about the hospital and its services such as:

- a. Conditions and treatments;
- b. Hospital departments and centers;
- c. Doctors who work at the hospital;
- d. News about the hospital; and
- e. Patient and visitor information.

48. The communications between a patient and MedStar Health begin when the patient arrives at a MedStar Health Web site. The communications continue as the patient clicks on links at the Web site, visits associated MedStar Web sites, and enters information into Web forms or their toolbar. The communications would end when the patient closes their browser or goes to an unrelated Web site. Communications would restart if a patient returns to [www.medstarhealth.org](http://www.medstarhealth.org) or an associated Web site.

49. Web pages and component files of Web pages are identified by Uniform Resource Locators (URLs). The URL of a Web page is typically shown in the address bar of a browser.<sup>7</sup>

50. An example of a URL is <https://www.medstarhealth.org/doctors/paul-a-sack-md>. This URL contains the following fields:

Protocol – https:	The protocol field specifies that the URL is accessed by a browser using the Hypertext Transfer Protocol (HTTP). Browsers and Web servers typically use HTTP to transfer files and other resources. They may also use the HTTPS protocol which is an extension of HTTP that uses encryption to provide secure communications between browsers and Web servers. The HTTP protocol is specified in the document RFC7231, <i>Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content</i> which is available at <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a> .
-------------------	---

<sup>7</sup> The syntax of URLs is described in the document RFC3986, *Uniform Resource Identifier (URI): Generic Syntax*, which is available at <https://tools.ietf.org/html/rfc3986>.



Host name – <a href="http://www.medstarhealth.org">www.medstarhealth.org</a>	The host name identifies a Website where a file or resource can be found. In this case, the host name is <a href="http://www.medstarhealth.org">www.medstarhealth.org</a> which identifies the Web server for the MedStar Health Web site.
Path - doctors/dr-paul-a-sack-md.	<p>The path identifies where a file or resource can be found on a Web server. It is typical practice for Web sites to include a plain-language description of the contents of a Web page in the path. In this example, the path identifies a Web page which provides information about Dr. Paul A. Sack of MedStar Health.</p> <p>Search engines, such as Google, index words found in paths in addition to the content of pages. See <i>Understanding SEO Friendly URL Syntax Practices</i> at <a href="https://searchengineland.com/seo-friendly-url-syntax-practices-134218">https://searchengineland.com/seo-friendly-url-syntax-practices-134218</a>.</p>
Query string	<p>A query string provides a list of parameters which a Web server can use for a variety of purposes such as:</p> <ol style="list-style-type: none"> <li>1. Retrieve information from a database based on the query string parameters.</li> <li>2. Save information provided by a Web form; or</li> <li>3. Save information provided by a Web page or another Web server</li> </ol> <p>A query string is optional in a URL. If a query string is present, it starts with a question mark (“?”) character. The question mark character is followed by a list of one or more name/value pairs which are separated by ampersand (“&amp;”) characters. Each name/value pair includes an equal sign (“=”). The name of the parameter appears on the left side of the equal sign while the string on the right side of the equal sign is the associated value.</p> <p>In the example URL above, no query string is present.</p> <p>An example of a URL which contains a query string is <a href="https://www.medstarhealth.org/sxa/search/results/?q=diabetes">https://www.medstarhealth.org/sxa/search/results/?q=diabetes</a></p> <p>For this second URL, the query string parameters indicate that a search was done at the MedStar Health search site for information about diabetes. The name of the search string is “q” and the value of the search string is “diabetes”.</p> <p>The meaning of parameter names and values of a query</p>

string are determined by the software which generates a URL and the software at a Web server which processes the URL.

In a query string, spaces can be represented as the string "%20" or as a plus sign ("+"). See *HTML URL Encoding Reference* at [https://www.w3schools.com/tags/ref\\_urlencode.asp](https://www.w3schools.com/tags/ref_urlencode.asp).

51. The path and query string fields are part of the communication between a patient and MedStar Health.

52. In the HTTP and HTTPS protocols, a GET request is used by a Web browser to retrieve a file or resource identified by a URL. The following shows an HTTP GET request used by the Google Chrome browser to fetch the example URL <https://www.medstarhealth.org/doctors/paul-a-sack-md>:

Request #601

```
GET https://www.medstarhealth.org/doctors/paul-a-sack-md HTTP/1.1
Host: www.medstarhealth.org
Connection: keep-alive
sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.medstarhealth.org/doctors
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: sxa_site=Medstar; sessionUniqueId=[REDACTED];
_gcl_au=[REDACTED]; _ga=[REDACTED];
_gid=[REDACTED]; _session_UA-[REDACTED]=true;
_fbp=fb; _cebs=1;
_ce.s=[REDACTED];
_CEFT=Q%3D%3D%3D; _hjFirstSeen=1; _hjIncludedInSessionSample=1;
_hjSession=[REDACTED]
```

;\_hjIncludedInPageviewSample=1;\_hjAbsoluteSessionInProgress=1;  
 hjSessionUser [REDACTED]  
 [REDACTED];\_tq\_id [REDACTED]-  
 1.42b0=[REDACTED];cebsp=4;\_dc\_gtm\_UA-  
 43394204-1=1

53. In some cases, HTTP requests and responses that have been excerpted from Fiddler capture files have been reformatted (“pretty printed”) for improved readability.

54. An HTTP GET request includes user communications to a Web site in the form of URLs, file paths, query strings, cookies, and information including identifiers appended to the end of a request as I will describe.

55. The HTTP GET request consists of a series of text lines. The first text line specifies that a GET request is being made and includes the URL of the Web page being requested without the protocol and host name fields.

56. The remaining text lines of the request are known as HTTP headers. These headers specify additional information for the request. For example, the “Host” header indicates that a request is directed to MedStar Health at “www.medstarhealth.org”

57. The “User-Agent” HTTP header identifies the browser making the request which is Chrome version 104. It also indicates that the Chrome browser is running on a Windows 10 PC.

58. Other HTTP headers, such as “Accept”, “Accept-Encoding”, and “Accept-Language” tell a Web server the format of a Web page to be returned by the server to the browser.

59. Other HTTP headers, such as “Connection” and “Upgrade-Insecure-Requests” are used to control the network connection between a browser and Web server.

60. The “Referer”<sup>8</sup> header specifies the URL of the Web page that contained the clicked link to Dr. Sack’s Web page. In this case, the link was on the doctors page

<sup>8</sup> Note that in the HTTP protocol, the “referer” header is misspelled. The correct spelling is “referrer”.



1 <https://www.medstarhealth.org/doctors>. The “Referer” header may also contain the URL of a Web  
 2 page or IFRAME that an HTTP request is made from. The URL in the “Referer” header is called  
 3 the referrer or referring URL.<sup>9</sup>

4 61. The “Cookie” HTTP header is described below.

5 62. The following is what the HTTP response from MedStar Health Web server looks  
 6 like when the URL <https://www.medstarhealth.org/doctors/paul-a-sack-md> has been requested:

```

7 HTTP/1.1 200 OK
8 Cache-Control: no-cache, no-store
9 Pragma: no-cache
10 Content-Length: 69008
11 Content-Type: text/html; charset=utf-8
12 Expires: -1
13 Vary: Accept-Encoding
14 Set-Cookie: sxa_site=Medstar; path=/
15 Request-Context: appId=[REDACTED]
16 X-Cache: CONFIG_NOCACHE
17 X-Azure-Ref: [REDACTED]
18 Date: Thu, 11 Aug 2022 21:33:15 GMT
  
```

15 63. An HTTP response includes communications from a Web site to a user in the  
 16 response file as described in this section. The communications may also include the setting of one  
 17 or more cookies as described in the section *Browser Cookies*.

18 64. An HTTP response consists of a series of lines of text similar to an HTTP request.  
 19 The first line of the HTTP response is called a status line which indicates if a file has been  
 20 successfully fetched by a Web server or not, and if not, what kind of error has occurred.

21 65. A status code of 200 indicates that a Web page exists and was successfully returned  
 22 in the HTTP GET response.

23 66. The status line is followed by HTTP header lines which provide information about  
 24 the file being returned in the HTTP response. The following table describes these HTTP header  
 25 lines in more detail:

27 <sup>9</sup> The referrer URL may sometimes be shortened so that it does not include the full URL, such that  
 28 the content of the communication after the .com or .org is not present in the referrer header.

Content-Type	Indicates what kind of file has been returned in the response. In this case, it is an HTML file which uses the “UTF-8” character set.
Content-Length	Indicates that the returned HTML file is 69,008 bytes in length.
Date	Indicates the date and time of the HTTP response.
Set-Cookie	Used to set browser cookies as described below.

67. After the final HTTP header, the response includes a blank line followed by the contents of the returned file. In this example, the following file is returned by the MedStar Health Web server:

```
<!DOCTYPE html>
<!--[if lt IE 7]>    <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->
<!--[if IE 7]>      <html class="no-js lt-ie9 lt-ie8"> <![endif]-->
<!--[if IE 8]>      <html class="no-js lt-ie9"> <![endif]-->
<!--[if gt IE 8]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->
<head>
<link href="/-/media/base-themes/core-libraries/styles/optimized-
min.css?t=20220603T125909Z" rel="stylesheet" /><link href="/-/media/base-
themes/main-theme/styles/optimized-min.css?t=20220603T125917Z" rel="stylesheet"
/><link href="/-/media/themes/mho/medstar/mho-theme/styles/optimized-
min.css?t=20220802T104118Z" rel="stylesheet" />
<title>Paul A Sack, MD| Endocrinology | MedStar Health</title>
<link rel="canonical" href="//www.medstarhealth.org/doctors/paul-a-sack-md" />
<link href="/-/media/project/mho/medstar/icons/favicon.png" rel="shortcut icon" />
<meta property="og:description" content="Paul A. Click here for more information and
to make an appointment." /><meta property="og:type" content="website" /><meta
property="og:image" content="https://www.medstarhealth.org/-
/media/project/mho/medstar/doctors/sack-paul-1598707606.jpg" /><meta
property="og:title" content="Paul A Sack, MD| Endocrinology | MedStar Health"
/><meta property="og:url" content="https://www.medstarhealth.org/doctors/paul-a-sack-
md" />
<meta name="description" content="Paul A. Click here for more information and to
make an appointment." />
...
</head>
<body class="default-device bodyclass">
...
<ul>
<li class="item0 odd first">
```

```

1 <div class="default-button field-link"><a href="/services" data-
2 variantitemid="{A3EFE2D7-2C5F-472C-8F8D-981BC3A3A114}" role="button" data-
3 variantfieldname="Link">Healthcare Services</a></div> </li>
4 <li class="item1 even">
5 <div class="default-button field-link"><a href="/doctors" data-
6 variantitemid="{83B8F34B-0D5C-47F1-A100-A38804407907}" role="button"
7 class="fad-url" data-variantfieldname="Link">Find a Doctor</a></div> </li>
8 <li class="item2 odd">
9 <div class="default-button field-link"><a href="/locations" data-
10 variantitemid="{1279CAFE-6DCD-4425-B6CC-1BA973E1EA04}" role="button"
11 class="fal-url" data-variantfieldname="Link">Locations</a></div> </li>
12 <li class="item3 even">
13 <div class="default-button field-link"><a href="/mymedstar-patient-portal" data-
14 variantitemid="{E43AC2DC-6E7E-45F9-8C3F-29864E17891D}" role="button" data-
15 variantfieldname="Link">Patient Portal</a></div> </li>
16 <li class="item4 odd">
17 <div class="default-button field-link"><a href="/innovation-and-research" data-
18 variantitemid="{CFB383EB-B1D6-47AE-8758-ABD5A84B7B37}" role="button" data-
19 variantfieldname="Link">Research and Education</a></div> </li>
20 <li class="item5 even last">
21 <div class="default-button field-link"><a href="https://careers.medstarhealth.org"
22 target=" blank" rel="noopener noreferrer" data-variantitemid="{DB8FA77A-8022-457A-
23 B33E-3813B61D8A0C}" role="button" data-
24 variantfieldname="Link">Careers</a></div> </li>
25 </ul>

```

...

```

15 <div class="field-maintitle">
16 <h2>About me</h2>
17 </div>

```

```

18 <div class="field-about-the-provider list-content">

```

```

19 <p> <p>Paul A. Sack, MD, has been at MedStar Union Memorial Hospital since 2005
20 after completing his medical training at the University of Maryland, School of Medicine.
21 He is the Chief in the Division of Endocrinology and Metabolism at MedStar Union
22 Memorial Hospital and Good Samaritan Hospital as well as the MedStar Regional
23 Director for Endocrinology in Baltimore.Â In addition, he is the President of the MedStar
24 Union Memorial Medical staff after having served as Vice-President from 2020-2022. He
25 is involved in patient care, clinical research, and the education of medical students,
26 residents, and endocrinology fellows. Â </p>

```

```

27 <p>Dr. Sack's clinical interests include the management of Type 1 and Type 2 Diabetes,
28 Thyroid Disease, Adrenal Disorders, and Pituitary Diseases. He performs diagnostic
29 thyroid and parathyroid ultrasounds and performs fine needle aspiration of thyroid
30 nodules. Â </p>

```

```

31 <p>Dr. Sack currently serves on the Board of the Maryland Chapter of the American
32 Diabetes Association.Â </p>

```

```

33 <p>Dr. Sack has been named a Top Doctor in Baltimore magazine for Diabetes Care in
34 2013, 2016, 2017, 2019, 2020, and 2021.</p>
35 </p>

```

...

```
</body>
</html>
```

68. Note that the entire HTML file is not shown above. Only the beginning and ending of the HTML file have been excerpted here because the entire HTML file is approximately 2,000 lines of text in length.

69. HTML (“Hypertext Markup Language”) is a standard markup language which tells a Web browser what content is to be displayed for a Web page and how to format the content on the screen.

70. An HTML file consists of a series of HTML tags which are denoted by angle brackets (“<>”) which enclose text or other HTML tags. The following table shows examples of HTML tags from the HTML file for the MedStar Health prostate cancer Web page:

<!DOCTYPE html> <html class="no-js" lang="en">	Marks the beginning and end of the HTML.
<head> ... </head>	Marks the beginning and end of the head section of the HTML. An HTML head section typically contains information about a Web page and formatting information.
<title>Paul A Sack, MD  Endocrinology   MedStar Health</title>	Specifies the title of the Web page which is “Paul A Sack, MD  Endocrinology   MedStar Health”
<link href="/-/media/base-themes/core-libraries/styles/optimized-min.css?t=20220603T125909Z" rel="stylesheet" />	Specifies a link to formatting information
<body class="default-device bodyclass">	Marks the beginning of the HTML body of the Web page.
<p> ... </p>	Marks the beginning and end of a paragraph within the body that contains text.
<a>	Used to create a link to another Web page.

...	
</a>	

71. JavaScript code can also be used in a Web page to provide additional functionality in a Web page. For example, JavaScript code may be used to:

- a. Format a Web page based on the characteristics of the device displaying the Web page
- b. Validate form data before it is sent to a Web server
- c. Provide user-interface elements such as menus, animated buttons, etc., or
- d. Provide tracking of user activity as described in this declaration

72. HTTP requests may also be used to disclose hidden tracking information to third parties as described above in the section entitled *The Meta Pixel*. The tracking information typically is disclosed to third parties via JavaScript code hidden in a Web page. The tracking information can be sent while a Web page is being loaded and while a user interacts with a Web page such as scrolling the Web page or clicking on a link on the Web page.

73. In addition to GET requests, the HTTP protocol also supports HTTP POST requests. An HTTP POST request is used on a Web page to send information to a Web site. This information can come from a form on a Web page which has been filled out by a user or from information collected by JavaScript code running on a Web page. The destination on the Web site where the information is to be sent is identified in a HTTP POST request as a URL. The information to be submitted to the Web site is placed after the final HTTP header line of a POST request. A blank text line is used to separate the HTTP header and the submitted information.

### **Developer Tools for Observing the Communications Between a Web Browser and Web Servers**

74. HTTP requests made by Web browsers and HTTP responses received by Web browsers are typically not visible to a user.

75. However, there are a variety of developer tools available for computer professionals to capture and save HTTP requests and responses as a user's Web browser communicates with Web servers. One such tool is the Fiddler Web debugging proxy. Fiddler is available for download and

1 documented at the Web site: <https://www.telerik.com/fiddler>. Fiddler can save HTTP requests and  
2 responses in a variety of file formats for later analysis. One such format for saving HTTP request  
3 and responses is the SAZ file format.

4 76. Most of the HTTP requests and responses shown in this declaration were captured  
5 by Fiddler.

6 77. Most Web browsers also include built-in developer tools for analyzing HTTP  
7 requests and responses.

8 78. For example, Google's Chrome browser includes DevTools for analyzing Web pages  
9 that are being displayed by a Chrome browser. These tools are documented by Google at  
10 <https://developers.google.com/web/tools/chrome-devtools/>.

#### 11 **Browser Cookies**

12 79. A feature of the HTTP protocol called cookies is implemented in most Web browsers  
13 and used by many Web sites. The cookie feature allows a Web site to save small pieces of text,  
14 known as cookies, in a user's Web browsers and in the file system of a user's computer. Once set,  
15 cookies are returned to a Web site in future HTTP requests. The purpose of a cookie is to allow a  
16 Web site to remember information specific to a returning user to the Web site.

17 80. To set a cookie, a Web site includes a Set-Cookie HTTP response header in an HTTP  
18 response. In its simplest form, the Set-Cookie HTTP response includes a cookie name and cookie  
19 value separated by an equal sign ("=") character. For example:

20  
21 Set-Cookie: id=84798432753

22  
23 This example instructs a browser to save a cookie named "id" with a value of "84798432753". In  
24 future HTTP requests to the Web site that set the "id" cookie, the cookie name and value will be  
25 returned to the Web site using a Cookie HTTP request header:

26  
27 Cookie: id=84798432753

28 81. Some of the uses of cookies by a Web site include:

- a. Track login status of a user at a Web site
- b. Track the state of a shopping cart at a Web site
- c. Gather statistics about how an individual user is using a Web site
- d. Gather aggregate statistics about how multiple users are using a Web site
- e. Customize the content of Web pages for individual users based on their past usage of a Web site; or
- f. Provide user-specific information held by a Web site to Web pages. Such information might include account information, doctor appointments, test results, email messages, and so on.

82. Cookies also have options associated with them which a Web site can set when a cookie is created. These options include:

Expires= <i>date</i>	Specifies a time and date when a cookie expires and is to be deleted by a Web browser
Max-age= <i>seconds</i>	An alternative to “Expires” which specifies the maximum number of seconds a cookie exists before it expires and is to be deleted by a Web browser.
Secure	Indicates that a cookie is only to be transmitted in a secure HTTPS request
HttpOnly	Indicates that a cookie is not available from JavaScript. Used to mitigate cross-site scripting attacks.
Domain= <i>domain</i>	Specifies the domains that a cookie can be sent to.
Path= <i>path</i>	Limits the sending of a cookie to a particular URL path of a Web site

83. Documentation for the Set-Cookie header can be found at the Mozilla Web site: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie>.

84. JavaScript code can also create, read, update, and delete cookies associated with the domain of the Web page in which the JavaScript is executing. See *Document.cookie* at <https://developer.mozilla.org/en-US/docs/Web/API/Document/cookie>.

85. If neither an Expires or Max-age option is specified for a cookie, then the cookie is called a session cookie. A session cookie automatically expires when a browser is closed or if



1 someone leaves a Web site and does not return in a short time.

2 86. Unlike a session cookie, a persistent cookie is designed to stay around for some time  
3 even if a user exits their browser or turns off their computer. A persistent cookie is specified using  
4 the Expires and/or Max-age options.

5 87. A persistent cookie allows a user to be tracked over a period of time beyond a single  
6 session.

7 88. The following is an example of a cookie being set at the MedStar Health patient  
8 portal by a Set-Cookie HTTP response header:

9 Set-Cookie: iqh\_csrf=[REDACTED]; expires=Thu, 10-Aug-  
10 2023 21:33:56 GMT; Max-Age=31449600; Path=/; secure  
11

12  
13 89. The following parameters are set for the cookie by the Set-Cookie response header:

14 iqh_csrf	Name of the cookie
15 [REDACTED]	Value of the cookie
16 expires=Thu, 10-Aug-2023 21:33:56 GMT Max-Age=31449600	When the cookie is to expire which is approximately 1 year after it was set
17 path=/	Indicates that the cookie is to be used on all Web pages at 18 medstarhealth.org Web sites.
19 secure	Indicates that the cookie is only to be sent on a secure HTTPS network 20 connection 21

22  
23 90. A Web browser can hold cookies from many different Web sites. Each Web site can  
24 set multiple cookies, each identified by a unique name.

25 91. A Web browser will only send back a cookie in an HTTP header to a Web site that  
26 set the cookie or to a related Web site. For example, the MedStar Health cookie will only be sent  
27 in an HTTP request to medstarhealth.org server. The MedStar Health cookie will not be sent to other  
28 Web sites such as [www.facebook.com](https://www.facebook.com), [www.google.com](https://www.google.com) and [www.amazon.com](https://www.amazon.com). However, as

1 explained below, some third-party JavaScript files placed in a Web site's source code may be able  
2 to extract and send first-party cookie data to companies such as Facebook.

3 92. When additional content of a Web page is fetched from the same server as the Web  
4 page itself, the HTTP GET requests for the additional content will include the same cookies as the  
5 Web page. These cookies are called "first-party cookies".

6 93. See for example:

7 Request #904

8 GET https://mymedstar.iqhealth.com/session-api/realm/[REDACTED]  
9 [REDACTED]=https%3A%2F%2Fmymedstar.iqhealth.com%2Fhome HTTP/1.1  
10 Host: mymedstar.iqhealth.com  
11 Connection: keep-alive  
12 Upgrade-Insecure-Requests: 1  
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,  
14 like Gecko) Chrome/104.0.0.0 Safari/537.36  
15 Accept:  
16 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*  
17 ;q=0.8,application/signed-exchange;v=b3;q=0.9  
18 Sec-Fetch-Site: cross-site  
19 Sec-Fetch-Mode: navigate  
20 Sec-Fetch-Dest: document  
21 sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"  
22 sec-ch-ua-mobile: ?0  
23 sec-ch-ua-platform: "Windows"  
24 Referer: https://cernerhealth.com/  
25 Accept-Encoding: gzip, deflate, br  
26 Accept-Language: en-US,en;q=0.9  
27 Cookie: iqh-iframe=[REDACTED];  
28 iqh=[REDACTED]; iqh\_csrf=[REDACTED]; iqh\_csrf-  
iframe=[REDACTED]; \_ga=[REDACTED];  
\_gid=[REDACTED]; \_gat=1; \_gat\_client=1

22 The \_\_cfduid cookie name and value are highlighted in yellow.

23 94. When a user's communication with a first party is redirected to a third-party by  
24 source code on the Web page, the disclosure to the third-party will include the cookies for the third-  
25 party. These cookies are called "third-party cookies".

26 95. In addition, JavaScript code from a third-party which runs inside of a Web page is  
27 able to access the first-party cookies associated with the domain of the Web page that have not been  
28 marked as "httponly".

# About Cookie Settings for Meta Pixel

5,635 views

Cookies are small pieces of code stored in internet browsers that are often used to distinguish between website visitors.

You can now use both first and third-party cookies with your Meta Pixel. The difference between first and third-party cookies is who owns the cookie.

First-party cookies are owned by the website a person is currently viewing, while third-party cookies belong to a website other than the one a person is currently viewing.

Compared to third-party cookies, first-party cookies are more widely accepted by browsers and stored for longer periods of time.

To give you more control over your advertising outcomes, the options for using cookies with your Meta Pixel are:

## 1. Use the Meta Pixel with both first and third-party cookies

This is the default option and is most likely your current Meta Pixel setting. With this option, you will use first-party cookie data with your Meta Pixel, in addition to third-party cookie data. Using both first and third-party cookies will allow you to reach more customers on Meta and to be more accurate in measurement and reporting.

## 2. Use the Meta Pixel with third-party cookies only

You can disable first-party cookies and use the Meta Pixel with third-party cookies only. With this option, your Meta Pixel will be less effective in reaching customers on Meta and less accurate in measurement and reporting.

96. Third-party JavaScript code can also create, read, and update its own first-party cookies associated with the domain of the Web page. These first-party cookies can be used as a replacement for third-party cookies if a user has configured their Web browser to block third-party cookies as a privacy measure. Meta designed the Meta Pixel for this purpose:

Source: <https://www.facebook.com/business/help/471978536642445>

97. For example, the MedStar Health Dr. Sacks Web page will also command patients' browsers to make redirected HTTP GET requests to [www.facebook.com](http://www.facebook.com). As the following redirected HTTP GET request shows, a re-direction includes information about the substance of

the Web page and Facebook cookies.

Request #658

GET

https://www.facebook.com/tr/?id=1321071481253782&ev=PageView&dl=https%3A%2F%2Fwww.medstarhealth.org%2Fdoctors%2Fpaul-a-sack-md&rl=https%3A%2F%2Fwww.medstarhealth.org%2Fdoctors&if=false&ts=1660253596912&sw=1920&sh=1080&v=2.9.75&r=stable&ec=0&o=30&fbp=fb[REDACTED]  
it=1660253596879&coo=false&rqm=GET HTTP/1.1

Host: www.facebook.com

Connection: keep-alive

sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

sec-ch-ua-platform: "Windows"

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: image

Referer: https://www.medstarhealth.org/

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Cookie: sb=[REDACTED] .datr=[REDACTED]

dpr=2; c\_user=[REDACTED] .xs=[REDACTED]

it=[REDACTED]

98. The cookies marked in green above do not contain MedStar Health cookies because the redirected HTTP GET request is going to the [www.facebook.com](https://www.facebook.com) Web server as specified in the HTTP Host header and not the www.medstarhealth.org Web server.

99. This HTTP GET request to the Facebook server by the MedStar Health Web page is an example of a hidden tracker as described above in the section entitled *The Meta Pixel*.

100. The Facebook cookies marked in green are examples of third-party cookies.

### IP Addresses

101. IP addresses are used to route messages on the Internet.

102. An IP address is a number which identifies a computer which is attached on the Internet.

103. IP addresses come in two forms: IPv4 or IPv6. An IPv4 address is a 32-bit number while an IPv6 address is a 128-bit number. There are two forms of IP addresses because there are

1 not enough IPv4 addresses for all of the computing devices that now exist. The larger IPv6 identifier  
2 was created to address this problem.

3 104. A 32-bit IPv4 address is made human-readable by writing out four decimal numbers  
4 separated by periods. Example: 172.217.12.164.

5 105. When a Web browser makes an HTTP request to a Web server, it must send the  
6 request to the IP address of the server. To learn the IP address of the Web server, a Web browser  
7 will first lookup the IP address of the server based on the host name of the URL being requested.  
8 This lookup process uses a service called the Domain Name System (DNS). This service, typically  
9 offered by an ISP, maps host names to IP addresses. This lookup process is automatically handled  
10 by a browser and is not visible to a user.

11 106. Examples of IPv4 addresses assigned to Web sites include:

12 www.medstarhealth.org	13.107.213.40
13 www.facebook.com	31.13.66.35

14  
15 107. For large Web sites such as Facebook, a single Web server cannot possibly service  
16 all the users that come to a Web site. Therefore, these sites use multiple Web servers to service all  
17 of their users. Each Web server is assigned its own unique IP address. To share the load between  
18 different users, the DNS system sometimes is configured to return different Ipv4 addresses for the  
19 same host name.

20 108. For a home computer user, a public Ipv4 address is typically assigned to the cable or  
21 DSL modem being used in the home. The IP address is assigned to the home modem when it is  
22 powered on. The public IP address of a modem is assigned by the home-owner's Internet Service  
23 Provider (ISP). Examples of popular ISPs include Comcast, AT&T, Charter, and Verizon.

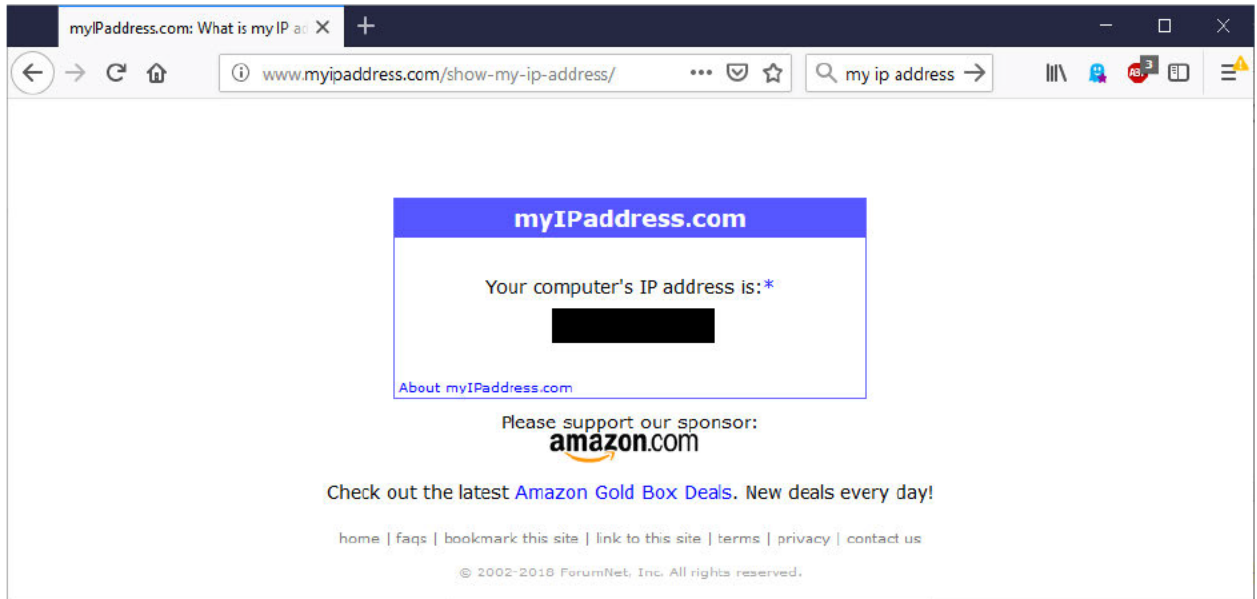
24 109. The same Ipv4 address might be assigned to a modem each time it is powered up or  
25 a different Ipv4 address can be assigned to the modem. How Ipv4 addresses get assigned is a policy  
26 decision made by individual ISPs.

27 110. When assigning a IPv4 address to a modem, an ISP typically keeps a record of the  
28 IPv4 address and which customer account the IP address has been associated with.

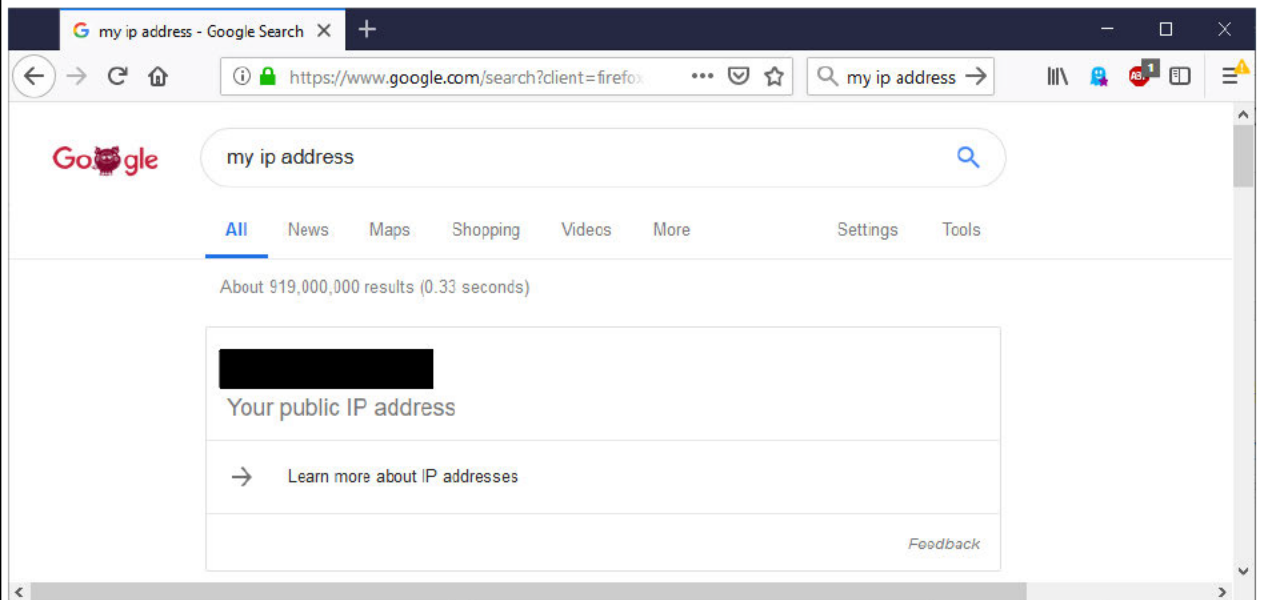


111. When a Web browser makes an HTTP request, the public IPv4 address is sent as part of the request to the Web site. The IP address is needed so that the Web site knows where the HTTP response is to be sent back to.

112. A public IPv4 address is not typically visible to a user. However, there are Web sites which will provide a public IP address. Once such Web site is [www.myIPAddress.com](http://www.myIPAddress.com) which shows the IPv4 address of [REDACTED]:



113. Google will also provide a public IPv4 address when searching for “my ip address”:



114. In a typical home Internet setup, all Internet-connected devices share the public IP

1 address of the modem of the house. Examples of Internet-connected devices include:

- 2 a. Personal computers
- 3 b. Smartphones
- 4 c. Tablets such as iPads
- 5 d. Smart TVs
- 6 e. Video streaming devices
- 7 f. Smart speakers such as Amazon Echo
- 8 g. Smart watches

9 115. These devices typically communicate with a home WiFi access point/router either  
10 through a wireless WiFi connection or wired Ethernet connection. The WiFi access point in turn is  
11 attached to the home-owner's cable modem in order to access the Internet outside of the home.

12 116. Each device attached to a WiFi access point is assigned its own unique internal IPv4  
13 address by the access point. These internal IPv4 addresses are typically not seen by Web sites and  
14 are selected from reserved IPv4 addresses which are called non-routable addresses. Examples of  
15 IPv4 address ranges which are not routable include 10.0.0.0 – 10.255.255.255, 172.16.0.0 –  
16 172.31.255.255, and 192.168.0.0 – 192.168.255.255.

17 117. As explained in this 2018 blog article from Data Dynamix, an Internet marketing  
18 company, individual homes can be tracked and targeted via the public IPv4 address assigned to their  
19 home modem:

20 IP Targeting: The Future of Advertising?

21 With this development in marketing, advertisers can now send customized ads to people in  
22 specific locations matching specific demographics. Displaying an ad in this fashion – ultra-  
23 targeted to someone who most likely wants to see it, has shown to [increase click-throughs](#)  
24 [by as much as 300%!](#) The ads can also be displayed to businesses, as well. IP targeting  
25 allows for both B2B and B2C marketing. **Once an IP address is assigned to a person or a  
business, it almost acts as a tracking number where a business can collect information  
about them.** IP targeting gives marketers an easy and effective way to target people, all  
while providing them with information that is beneficial to their business.

26 If you are looking to mix things up and try a different method, IP targeting could very well  
27 be worth a shot. Data-Dynamix can help you with IP targeting. [Please contact us](#) for more  
information on this exciting new technology for digital marketing!

28 Source: <https://www.data-dynamix.com/ip-targeting-future-advertising/>



Note: Yellow highlighting added.

118. See also:

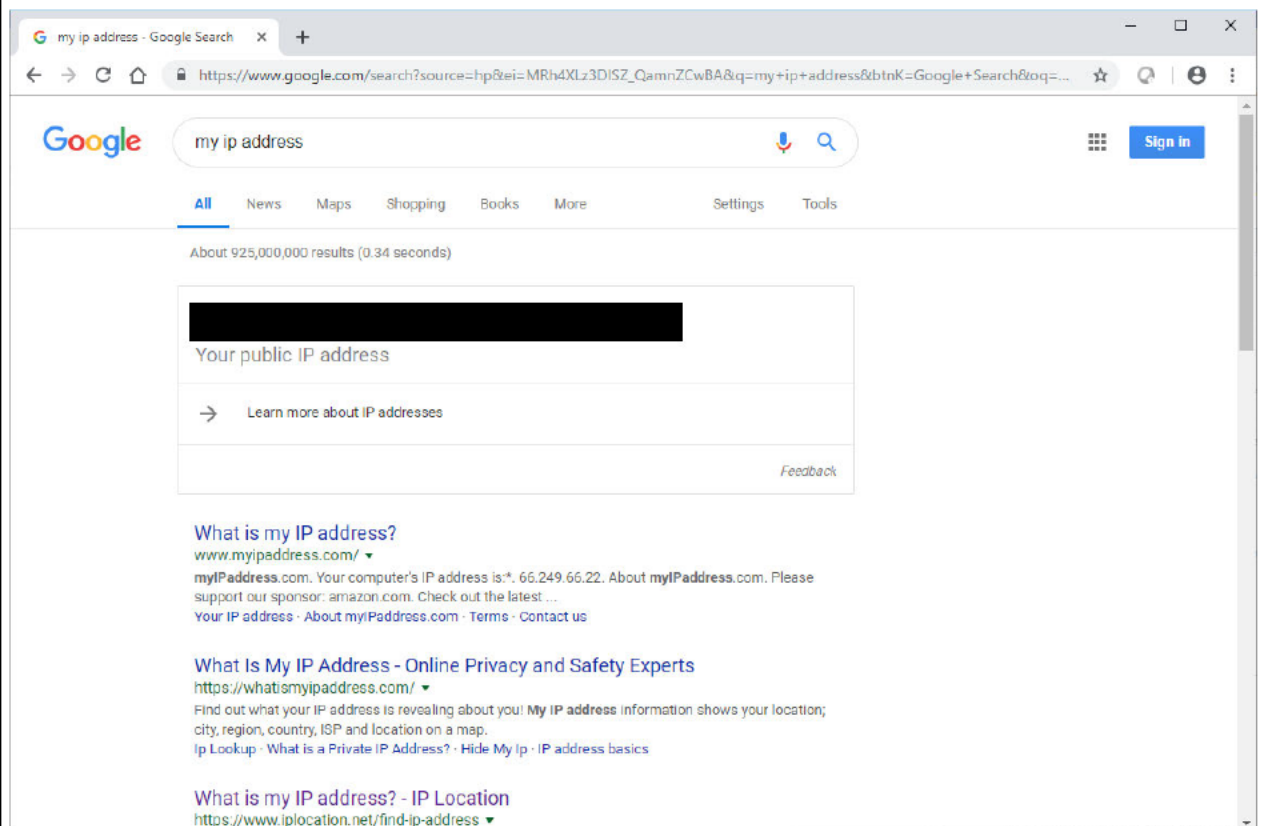
Using our unique technology, we have **tied an individual's household address to a unique IP address** with the purpose of delivering targeted marketing messages. This means we can deliver an ad via a mobile device, table, PC, laptop or connected television.

Source: <https://www.data-dynamix.com/solutions/ip-address-targeting/>

Note: Bold highlighting is original.

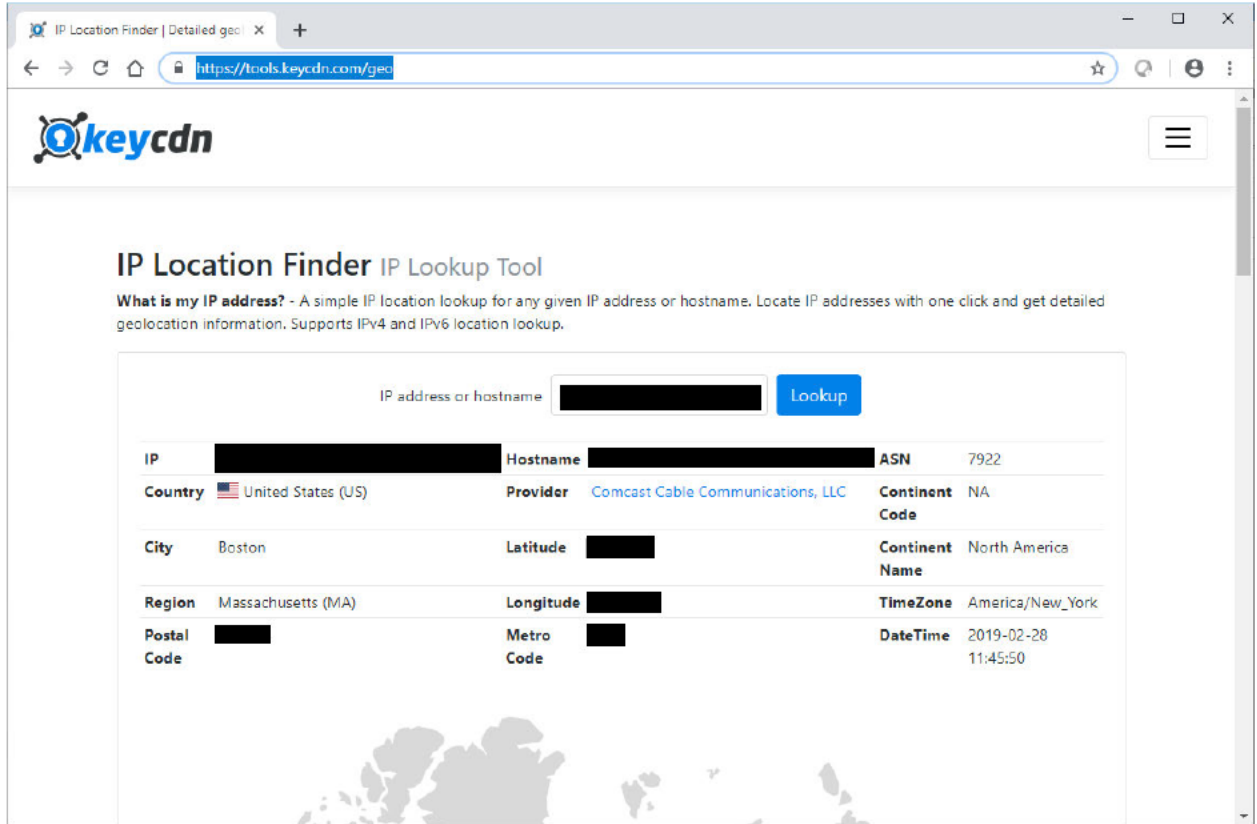
119. A computing device may also be assigned an IPv6 address which it can use to communicate with Web sites that support IPv6 networking. In order for a device to obtain an IPv6 address, its networking software, the local networking hardware being used by the device, and the ISP being used by the device must support IPv6 networking.

120. The following screen shot from a Google search of “my IP address” shows a 128-bit IPv6 address assigned to my Windows PC being displayed by Google as a series of 8 hexadecimal numbers separated by colon characters:



Source: <https://www.google.com>

121. IPv6 addresses allow geolocation typically down to the city level as well as identification of an ISP. See for example the following screen shot which shows that my Comcast IPv6 address is located in Boston, Massachusetts:



Source: <https://tools.keycdn.com/geo>

122. In Windows 10, my IPv6 address [Redacted] is known as a temporary IPv6 address as shown in the following ipconfig command output:

Wireless LAN adapter Wi-Fi:

```

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : [Redacted]
Temporary IPv6 Address. . . . . : [Redacted]

```

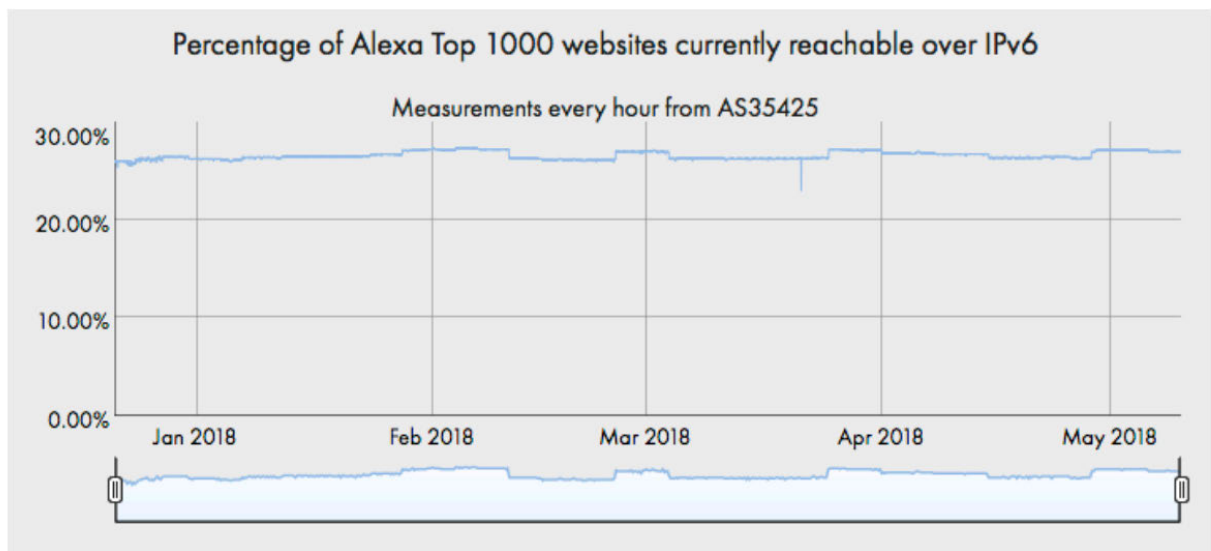
123. A temporary IPv6 address is reassigned periodically by Windows 10 or when reconnecting to an IPv6-capable network. Part of the temporary IPv6 address is a random number. Temporary IPv6 addresses are designed to provide some level of privacy protections versus a fixed IPv6 address. However, even temporary IPv6 addresses still allow geolocation and can be associated with personally-identifiable information such as the Facebook c\_user cookie and other

third-parties that have personally identifiable information associated with a cookie id.

124. In order for a browser to use an IPv6 address to communicate with a Web site, the Web site must be IPv6-enabled. Otherwise, a browser will instead use an IPv4 address to communicate with a Web site.

125. According to a 2018 survey of the Alexa Top 1000 Web sites, somewhat less than 30% of the sites are reachable via IPv6 address:

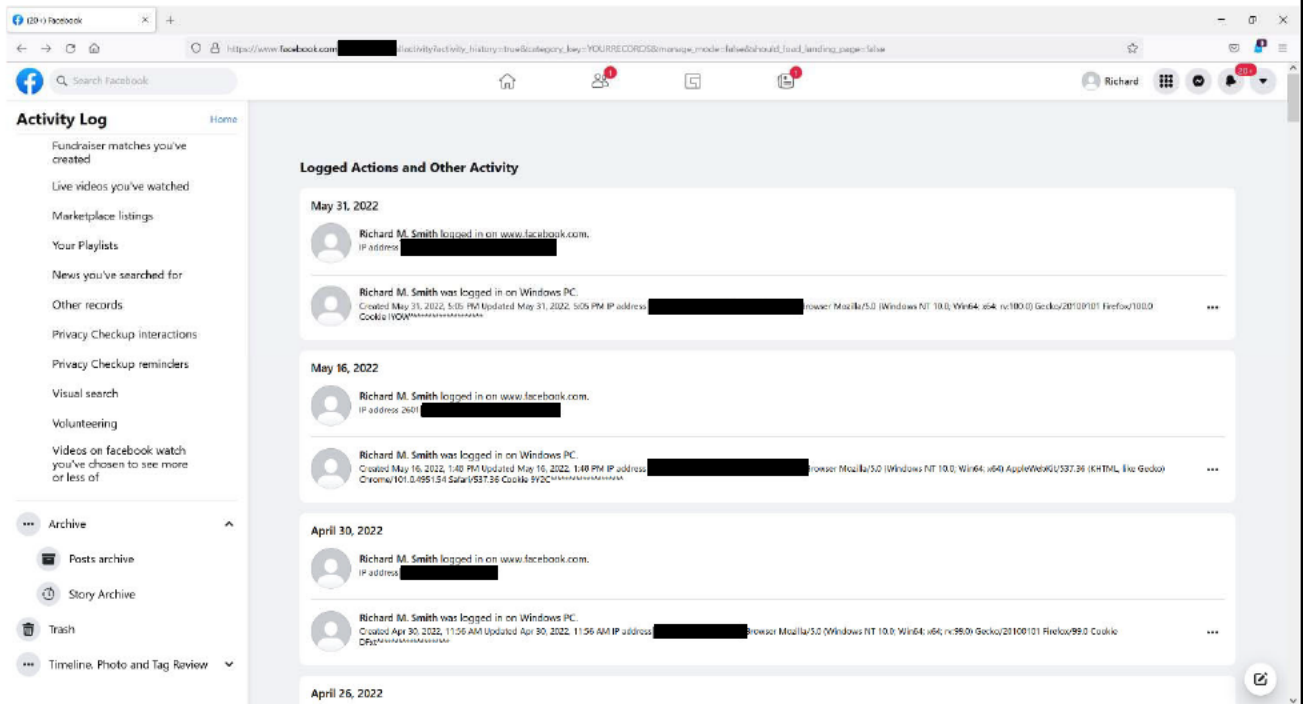
- **Alexa Top 1,000 Websites:** 28% with working IPv6 (up from 23% in 2017)



**Figure 2 – Percentage of Alexa Top 1000 websites reachable over IPv6**

Source: *State of IPv6 Deployment 2018*, Internet Society

126. Meta allows a logged-in user to view previous logins to the Facebook Web site in the Activity Log section of the Facebook Web site. Login information includes IP address, browser user agent, and a cookie value as shown in the following screen shot from my own Facebook account:



Source:

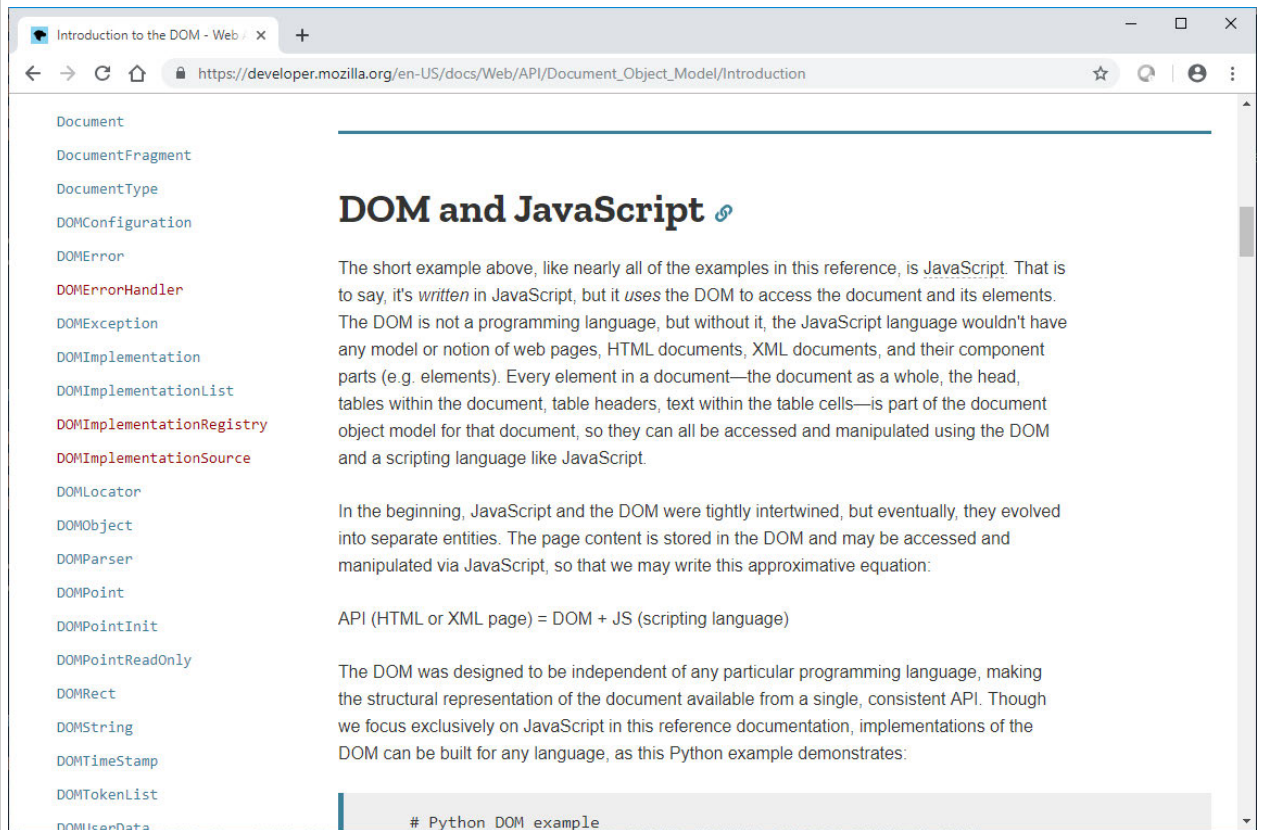
[https://www.facebook.com/\[REDACTED\]/allactivity?activity\\_history=true&category\\_key=YOURRECORDS&manage\\_mode=false&should\\_load\\_landing\\_page=false](https://www.facebook.com/[REDACTED]/allactivity?activity_history=true&category_key=YOURRECORDS&manage_mode=false&should_load_landing_page=false)

127. This activity log shows that Meta correlates IP addresses, user agent type, and cookie values (including datr) with a user's Facebook Id.

### Web Page and Web Form Scraping

128. A technique known as Web page scraping can be used to extract communications from the HTML tags and text of a Web page. One method of implementing Web page scraping is to use JavaScript code running inside of the Web page. The JavaScript code can come from the Web site itself or from third parties. JavaScript scraping relies on the Document Object Model (DOM) of a Web page to locate and extract communications from the Web page. Once the communication has been extracted, it can be uploaded to a third-party Web site using a tracking pixel or API call.

129. Extensive documentation is available on the Web and in books which describes how JavaScript uses the DOM to access the full content of Web pages. See for example *DOM and JavaScript*:



Source: [https://developer.mozilla.org/en-US/docs/Web/API/Document\\_Object\\_Model/Introduction](https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model/Introduction)

130. At the diabetes Web page for Medstar's St. Mary's hospital, a Facebook API call is made that contains communications describing the full contents of the page. This communication appears to have been scraped from the contents of the Web page. The following is an example of the API call with the communications marked in yellow:

Request #663

POST https://www.facebook.com/tr/ HTTP/1.1

Host: www.facebook.com

Connection: keep-alive

Content-Length: 2070

Cache-Control: max-age=0

sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Upgrade-Insecure-Requests: 1

Origin: https://www.medstarhealth.org

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;



1 q=0.8,application/signed-exchange;v=b3;q=0.9  
 2 Sec-Fetch-Site: cross-site  
 3 Sec-Fetch-Mode: navigate  
 4 Sec-Fetch-Dest: iframe  
 5 Referer: https://www.medstarhealth.org/  
 6 Accept-Encoding: gzip, deflate, br  
 7 Accept-Language: en-US,en;q=0.9  
 8 Cookie: sb=[REDACTED]; datr=[REDACTED]; dpr=2;  
 9 c\_user=[REDACTED]; xs=[REDACTED];  
 10 fr=[REDACTED]  
 11 Pretty-printed form data  
 12 id=1321071481253782  
 13 ev=Microdata  
 14 dl=https://www.medstarhealth.org/doctors/paul-a-sack-md  
 15 rl=https://www.medstarhealth.org/doctors  
 16 if=false  
 17 ts=1660253597415  
 18 cd[DataLayer]=[]  
 19 cd[Meta]={ "title": "Paul+A+Sack,+MD|+Endocrinology|+MedStar+Health", "meta:description":  
 20 "Paul+A.++Click+here+for+more+information+and+to+make+an+appointment." }  
 21 cd[OpenGraph]={ "og:description": "Paul+A.++Click+here+for+more+information+and+to+ma  
 22 ke+an+appointment.", "og:type": "website", "og:image": "https://www.medstarhealth.org/-  
 23 /media/project/mho/medstar/doctors/sack-paul-  
 24 1598707606.jpg", "og:title": "Paul+A+Sack,+MD|+Endocrinology|+MedStar+Health", "og:url":  
 25 "https://www.medstarhealth.org/doctors/paul-a-sack-  
 26 md", "twitter:image": "https://www.medstarhealth.org/-/media/project/mho/medstar/doctors/sack-  
 27 paul-  
 28 1598707606.jpg", "twitter:description": "Paul+A.++Click+here+for+more+information+and+to+  
 make+an+appointment.", "twitter:title": "Paul+A+Sack,+MD|+Endocrinology|+MedStar+Healt  
 h", "twitter:card": "summary" }  
 cd[Schema.org]=[]  
 cd[JSON-  
 LD]=[ { "@context": "https://schema.org", "@type": "Physician", "name": "Paul+A+Sack,+MD|+En  
 doocrinology|+MedStar+Health", "url": "https://www.medstarhealth.org/doctors/paul-a-sack-  
 md", "description": "Paul+A.++Click+here+for+more+information+and+to+make+an+appointm  
 ent.", "image": "https://www.medstarhealth.org/-/media/project/mho/medstar/doctors/sack-paul-  
 1598707606.jpg", "aggregateRating": { "@context": "https://schema.org", "@type": "AggregateRati  
 ng", "ratingValue": 4.9, "reviewCount": 820 } } ]  
 sw=1920  
 sh=1080  
 v=2.9.75  
 r=stable  
 ec=1  
 o=30  
 fbp=fb [REDACTED]  
 it=1660253596879  
 coo=false  
 es=automatic  
 tm=3  
 rqm=formPOST

131. The data redirected by MedStar Health to Facebook appears to have been extracted from the HTML content sent to my browser from the MedStar Health Web site:

```
<title>Paul A Sack, MD| Endocrinology | MedStar Health</title>

<meta property="og:description" content="Paul A. Click here for more information and to
make an appointment." /><meta property="og:type" content="website" /><meta
property="og:image" content="https://www.medstarhealth.org/-
/media/project/mho/medstar/doctors/sack-paul-1598707606.jpg" /><meta property="og:title"
content="Paul A Sack, MD| Endocrinology | MedStar Health" /><meta property="og:url"
content="https://www.medstarhealth.org/doctors/paul-a-sack-md" />

<meta name="description" content="Paul A. Click here for more information and to make an
appointment." />

<script type="application/ld+json">
{
    "@context": "https://schema.org",
    "@type": "Physician",
    "name": "Paul A Sack, MD| Endocrinology |
MedStar Health",
    "url":
    "https://www.medstarhealth.org/doctors/paul-a-sack-md",
    "description": "Paul A. Click here for more
information and to make an appointment.",
    "image": "https://www.medstarhealth.org/-
/media/project/mho/medstar/doctors/sack-paul-1598707606.jpg",
    "aggregateRating": {"@context":
    "https://schema.org", "@type": "AggregateRating", "ratingValue": 4.9, "reviewCount": 820}
}
```



132. The Facebook JavaScript file at URL <https://connect.facebook.net/signals/config/1321071481253782?v=2.9.75&r=stable> contains functions for scraping communications on MedStar Health Web pages. The following are examples of these JavaScript scraping functions:



```

1      f.ensureModuleRegistered("SignalsFBEvents.plugins.microdata", function() {
2          return function(g, b, c, d) {
3              var e = {
4                  exports: {}
5              };
6              e.exports;
7              (function() {
8                  "use strict";
9                  var a = Object.assign || function(a) {
10                      for (var b = 1; b < arguments.length; b++) {
11                          var c = arguments[b];
12                          for (var d in c) Object.prototype.hasOwnProperty.call(c, d) && (a[d] =
13                          c[d])
14                      }
15                      return a
16                  },
17                  c = f.getFbeventsModules("SignalsFBEventsLogging"),
18                  d = f.getFbeventsModules("SignalsFBEventsPlugin"),
19                  h = f.getFbeventsModules("SignalsFBEventsQE"),
20                  i = f.getFbeventsModules("SignalsFBEventsShared"),
21                  j = i.signalsGetValueFromHTMLElement,
22                  k = i.unicodeSafeTruncate;
23                  i = f.getFbeventsModules("SignalsFBEventsUtils");
24                  var l = i.filter,
25                      m = i.some,
26                      n = i.keys,
27                      o = i.FBSet;
28                  i = f.getFbeventsModules("SignalsFBEventsEvents");
29                  var p = i.fired,
30                      q = i.getCustomParameters,
31                      r = 500,
32                      s = 1e3,
33                      t = 12e4,
34                      u = ["og:image"],
35                      v = [{
36                          property: "image",
37                          type: "Product"
38                      }];
39
40                  function w(a) {
41                      return l(u, function(b) {
42                          return b === a
43                      })[0] != null
44                  }
45
46                  function x(a, b) {
47                      return l(v, function(c) {

```

```

1         return (a === "https://schema.org/" + c.type || a === "http://schema.org/" +
2         c.type) && c.property === b
3         }))[0] != null
4     }
5
6     function y() {
7         var a = b.querySelectorAll("[itemscope]"),
8             c = [],
9             d = new o();
10        for (var e = 0; e < a.length; e++) d.add(a[e]);
11        for (var e = a.length - 1; e >= 0; e--) {
12            var f = a[e],
13                g = f.getAttribute("itemtype");
14            if (typeof g !== "string" || g === "") continue;
15            var h = {},
16                i = f.querySelectorAll("[itemprop]");
17            for (var k = 0; k < i.length; k++) {
18                var l = i[k];
19                if (!d.has(l)) {
20                    d.add(l);
21                    var m = l.getAttribute("itemprop");
22                    if (typeof m === "string" && m !== "") {
23                        l = j(l);
24                        if (l != null) {
25                            var n = h[m];
26                            n != null && x(g, m) ? Array.isArray(n) ? h[m].push(l) : h[m] =
27                                [n, l] : h[m] = l
28                        }
29                    }
30                }
31            }
32            c.unshift({
33                schema: {
34                    dimensions: {
35                        h: f.clientHeight,
36                        w: f.clientWidth
37                    },
38                    properties: h,
39                    subscores: [],
40                    type: g
41                },
42                scope: f
43            })
44        }
45        n = [];
46        m = [];
47        for (var l = 0; l < c.length; l++) {
48            k = c[l];

```

```

1      i = k.scope;
2      h = k.schema;
3      for (var g = m.length - 1; g >= 0; g--)
4          if (m[g].scope.contains(i)) {
5              m[g].schema.subscopes.push(h);
6              break
7          } else m.pop();
8      m.length === 0 && n.push(h);
9      m.push({
10         schema: h,
11         scope: i
12     })
13 }
14 return n
15 }
16
17 function z() {
18     var a = [],
19         d = b.querySelectorAll('script[type="application/ld+json"]'),
20         e = 0;
21     for (var f = 0; f < d.length; f++) {
22         var g = d[f];
23         if (g.innerText != null && g.innerText != "") try {
24             e += g.innerText.length;
25             if (e > t) return [];
26             var h = JSON.parse(g.innerText.replace(/\n\r\t/g, " "));
27             a.push(h)
28         } catch (a) {
29             c.logUserError({
30                 jsonLd: g.innerText,
31                 type: "INVALID_JSON_LD"
32             })
33         }
34     }
35     return a
36 }
37
38 function A() {
39     var a = new o(["og", "product", "music", "video", "article", "book", "profile",
40 "website", "twitter"]),
41         c = {},
42         d = b.querySelectorAll("meta[property]");
43     for (var e = 0; e < d.length; e++) {
44         var f = d[e],
45             g = f.getAttribute("property");
46         f = f.getAttribute("content");
47         if (typeof g === "string" && g.indexOf(":") !== -1 && typeof f ===
48 "string" && a.has(g.split(":")[0])) {

```

```

1          f = k(f, r);
2          var h = c[g];
3          h != null && w(g) ? Array.isArray(h) ? c[g].push(f) : c[g] = [h, f] : c[g]
4          = f
5          }
6          }
7          return c || void 0
8          }
9          var B = {
10             description: !0,
11             keywords: !0
12         };
13
14         function C() {
15             var a = b.querySelector("title");
16             a = {
17                 title: k(a && a.innerText, r)
18             };
19             var c = b.querySelectorAll("meta[name]");
20             for (var d = 0; d < c.length; d++) {
21                 var e = c[d],
22                     f = e.getAttribute("name");
23                 e = e.getAttribute("content");
24                 typeof f === "string" && typeof e === "string" && (B[f] && (a["meta:" +
25                 f] = k(e, r)))
26             }
27             return a || void 0
28         }
29
30         function D(b) {
31             var c = b.id,
32                 d = b.includeJsonLd,
33                 e = d === void 0 ? !1 : d,
34                 f = b.instance;
35             d = b.retries;
36             var i = d === void 0 ? 1 : d;
37             b = A();
38             d = C();
39             var j = y(),
40                 k = e ? z() : [],
41                 l = h.get("logDataLayer");
42             l = l && l.isInExperimentGroup;
43             l = l === !0 ? g.dataLayer || [] : [];
44             if (j.length === 0 && k.length === 0 && n(b).length === 0 && i > 0) {
45                 setTimeout(function() {
46                     return D({
47                         id: c,
48                         includeJsonLd: e,

```

```

1         instance: f,
2         retries: i - 1
3     })
4     }, s);
5     return
6     } else if (j.length > 0 || k.length > 0 || n(b).length > 0 || n(d).length > 0 ||
7     l.length && l.length > 0) {
8         l = {
9             DataLayer: l,
10            Meta: d,
11            OpenGraph: b,
12            "Schema.org": j
13        };
14        e && (l = a({}, l, {
15            "JSON-LD": k
16        }));
17        f.trackSingleSystem("automatic", c, "Microdata", l)
18    }
19    }
20    var E = 500,
21        F = "microdata_wait";
22    e.exports = new d(function(a, b) {
23        a = g.performance != null && g.performance.timing.loadEventEnd != null ?
24        g.performance.timing.loadEventEnd : Date.now();
25        var c = a !== 0 ? a : Date.now(),
26            d = h.get(F);
27        q.listen(function(a, b) {
28            return d != null && b === "Microdata" ? {
29                exp: d.code
30            } : {}
31        });
32        var e = {};
33        p.listen(function(a, f) {
34            var g = f.get("id");
35            if (g == null || typeof g !== "string" ||
36            Object.prototype.hasOwnProperty.call(e, g)) return;
37            a = m(b.getOptedInPixels("Microdata"), function(a) {
38                return a.id === g
39            });
40            if (a) {
41                var h = m(b.getOptedInPixels("MicrodataJsonLd"), function(a) {
42                    return a.id === g
43                });
44                e[g] = !0;
45                f = d != null && d.isInExperimentGroup ? c + E - Date.now() : E;
46                f <= 0 ? D({
47                    id: g,
48                    includeJsonLd: h,

```

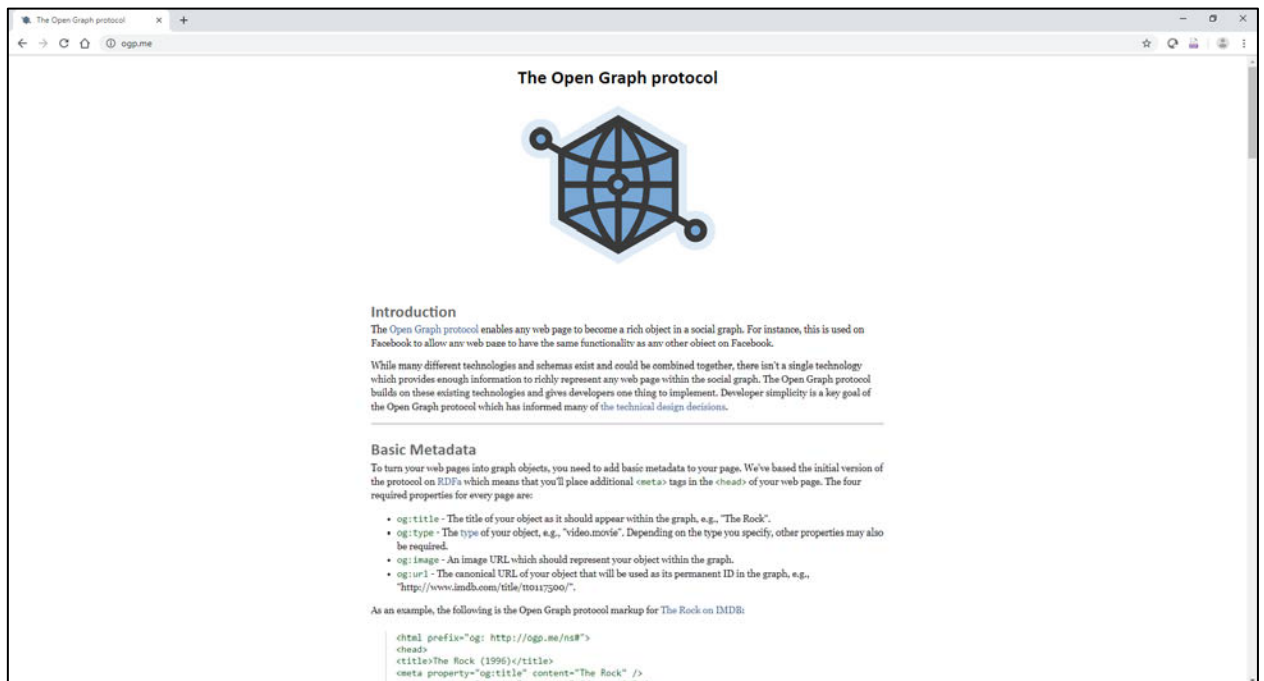
```

        instance: b
      }) : setTimeout(function() {
        D({
          id: g,
          includeJsonLd: h,
          instance: b
        })
      }, f)
    }
  })
  })();
  return e.exports
}(a, b, c, d)
});
e.exports = f.getFbeventsModules("SignalsFBEvents.plugins.microdata");
f.registerPlugin && f.registerPlugin("fbevents.plugins.microdata", e.exports);
f.ensureModuleRegistered("fbevents.plugins.microdata", function() {
  return e.exports
})

```

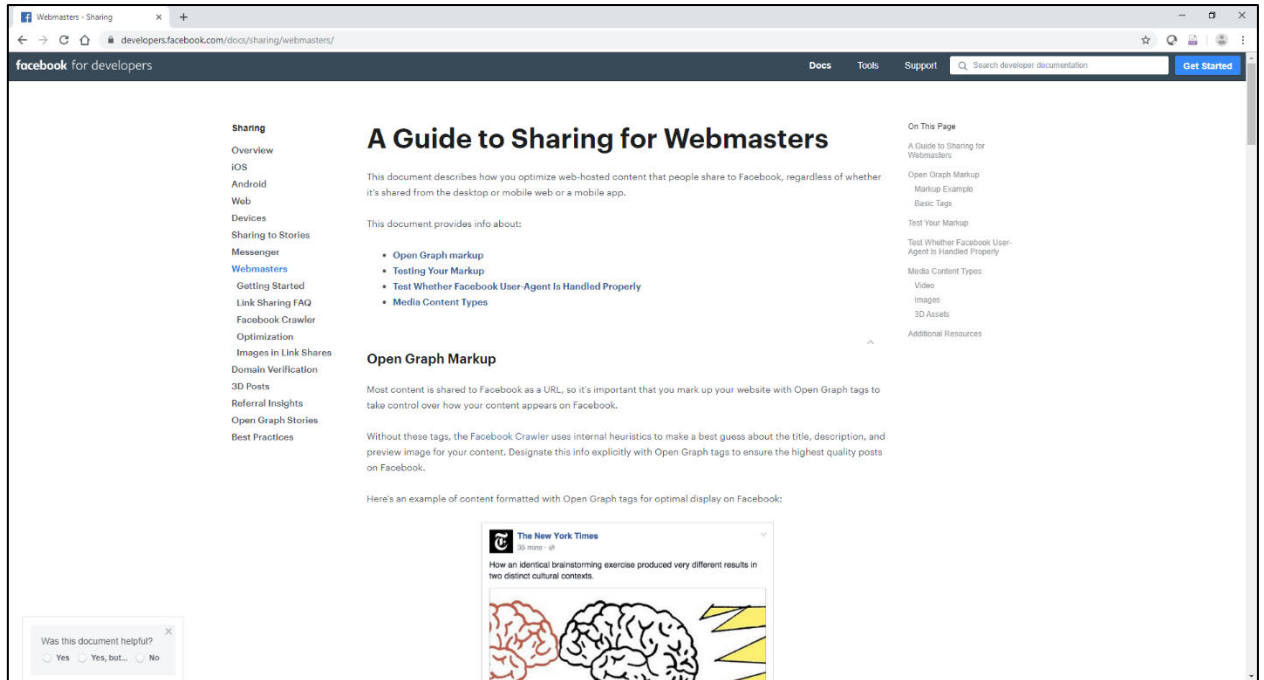
133. These functions use DOM methods such as `querySelector` and `getAttribute` to locate information on the Web page of interest.

134. Scraped information from MedStar Health Web pages is sent to the Facebook server using conventions by the Open Graph Protocol:



Source: <https://ogp.me/>





Source: <https://developers.facebook.com/docs/sharing/webmasters/>

135. Personally-identifiable information (PII) sent as part of the communications from a Web site to a Web browser is accessible and can be scraped from third-party JavaScript code running inside of the Web page that contains the personally-identifiable information.

136. In addition, personally-identifiable information that a user has entered into a Web form as part of their communications with a Web site is also accessible and can be scraped by third-party JavaScript running in the Web page that contains the form.

137. For example, Meta documents for developers the ability of the Meta Pixel to scrape personally-identifiable information, such as an email address, from forms of a Web site:

## Meta Pixel

The Meta Pixel is a snippet of JavaScript code that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an **event**) that you want to track (called a **conversion**). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that effectiveness of your website's conversion funnels.

The Meta Pixel can collect the following data:

- **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website.
- **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
- **Button Click Data** – Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.
- **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are **conversion value**, **page type** and **more**.
- **Form Field Names** – Includes website field names like **email**, **address**, **quantity**, etc., for when you purchase a product or service. **We don't capture field values unless you include them as part of Advanced Matching or optional values.**

Source: <https://developers.facebook.com/docs/meta-pixel/>

138. The Facebook JavaScript file used by MedStar Health, <https://connect.facebook.net/signals/config/1321071481253782?v=2.9.75&r=stable>, defines a module named “signalsFBEventsExtractFormFieldFeatures”. This module includes a function which references an option named “extractPIIFields” and a module named “SignalsPixelPIIUtils”. Because the Facebook JavaScript has been obfuscated<sup>10</sup>, it is difficult to understand the purpose of this module. Regardless, the option name strongly suggest that Facebook has included form scraping code that is capable of extracting personally-identifiable information (PII) from form fields on the MedStar Health Web site.

```
f.ensureModuleRegistered("signalsFBEventsExtractFormFieldFeatures", function() {
  return function(g, h, i, j) {
    var e = {
      exports: {}
    };
  };
});
```

<sup>10</sup> “Obfuscation is the deliberate act of creating obfuscated code, i.e. source or machine code that is difficult for humans to understand. It is something similar to encryption, but a machine can understand the code and is able to execute: it.” *What Is JavaScript Obfuscation and When Is it Used?* at <https://dzone.com/articles/obfuscation-what-is-obfuscation-in-javascript-why>

```

1      e.exports;
2      (function() {
3          "use strict";
4          var a = f.getFbeventsModules("SignalsPixelPIIUtils"),
5              b = a.extractPIIFields;
6
7          function c(a, c) {
8              var d = {
9                  id: a.id,
10                 name: a.name,
11                 tag: a.tagName.toLowerCase()
12             },
13             e = {};
14             (a instanceof HTMLInputElement || a instanceof HTMLTextAreaElement) &&
15             a.placeholder !== "" && (d.placeholder = a.placeholder);
16             if (d.tag === "input") {
17                 d.inputType = a.getAttribute("type");
18                 if (c && (a instanceof HTMLInputElement || a instanceof
19 HTMLTextAreaElement)) {
20                     c = b(d, a);
21                     c !== null && (e = c)
22                 }
23             }
24             a instanceof HTMLButtonElement === !1 && a.value === "" &&
25             (d.valueMeaning = "empty");
26             return [d, e]
27         }
28         e.exports = c
29     })();
30     return e.exports
31 }(a, b, c, d)
32 });
33
34 ...
35
36 f.ensureModuleRegistered("SignalsFBEventsPixelPIISchema", function() {
37     return function(f, g, h, i) {
38         var j = {
39             exports: {}
40         };
41         j.exports;
42         (function() {
43             "use strict";
44             j.exports = {
45                 "default": {
46                     type: "string",
47                     typeParams: {
48                         lowercase: !0,
49                         strip: "whitespace_only"
50                     }
51                 },
52                 ph: {
53                     type: "phone_number"
54                 },
55                 em: {

```

```

1      type: "email"
2    },
3    fn: {
4      type: "string",
5      typeParams: {
6        lowercase: !0,
7        strip: "whitespace_and_punctuation"
8      }
9    },
10   ln: {
11     type: "string",
12     typeParams: {
13       lowercase: !0,
14       strip: "whitespace_and_punctuation"
15     }
16   },
17   zp: {
18     type: "postal_code"
19   },
20   ct: {
21     type: "string",
22     typeParams: {
23       lowercase: !0,
24       strip: "all_non_latin_alpha_numeric",
25       test: "^[a-z]+"
26     }
27   },
28   st: {
29     type: "string",
30     typeParams: {
31       lowercase: !0,
32       truncate: 2,
33       strip: "all_non_latin_alpha_numeric",
34       test: "^[a-z]+"
35     }
36   },
37   dob: {
38     type: "date"
39   },
40   doby: {
41     type: "string",
42     typeParams: {
43       test: "^[0-9]{4,4}$"
44     }
45   },
46   ge: {
47     type: "enum",
48     typeParams: {
49       lowercase: !0,
50       options: ["f", "m"]
51     }
52   },
53   dobm: {
54     type: "string",
55     typeParams: {

```

```

1      test: "^(0?[1-
2      9]|1[012])$|^jan|^feb|^mar|^apr|^may|^jun|^jul|^aug|^sep|^oct|^nov|^dec"
3      },
4      dobd: {
5          type: "string",
6          typeParams: {
7              test: "^(([0]?[1-9])|([1-2][0-9])|(3[01]))$"
8          }
9      }
10     }
11     }));
12     return j.exports
13     }(a, b, c, d)
14     });

```

139. In June 2022, Novant Health, a hospital system in North Carolina, discovered that the Meta Pixel that they were using on their Web site was possibly sending protected health information (PHI) to Meta due to the Meta Pixel being misconfigure:

## What happened:

Novant Health, in an effort to be as transparent as possible, mailed letters to some patients following possible disclosure of protected health information (PHI) resulting from an incorrect configuration of pixel, an online tracking tool.

In May 2020, as our nation confronted the beginning of the COVID-19 pandemic, Novant Health launched a promotional campaign to connect more patients to the Novant Health MyChart patient portal, with the goals of improving access to care through virtual visits and to provide increased accessibility to counter the limitations of in-person care. This campaign involved Facebook advertisements and a Meta (Facebook parent company) tracking pixel placed on the Novant Health website to help understand the success of those advertisement efforts on Facebook. However, the pixel was configured incorrectly and may have allowed certain private information to be transmitted to Meta from the Novant Health website and MyChart portal.

Immediately upon becoming aware that the pixel had the capability to transmit unintended information to Meta, Novant Health disabled and removed the pixel as a precaution and began an investigation to learn whether, and to what extent, information was transmitted. Based on that investigation, Novant Health determined on June 17, 2022, that it was possible PHI might have been disclosed to Meta, depending upon a user's activity within the Novant Health website and MyChart portal. This information potentially included an impacted patient's: demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes. The information did not include Social Security numbers or other financial information unless it was typed into a free text box by the user. The letter sent to each patient impacted will specifically state whether such financial information may have been involved.

Source: <https://www.novanthealth.org/home/privacy-statement/pixel.aspx>

140. PHI which Novant Health identified as being disclosed to Meta included:



- a. email address
- b. phone number
- c. computer IP address
- d. contact information entered into Emergency Contacts or Advanced Care

#### Planning

- e. appointment type and date
- f. physician selected
- g. button/menu selections
- h. content typed into free text boxes

141. Much of this PHI identified by Novant Health appears to be form data which was scraped by the Meta pixel.

142. Novant Health goes onto state that they were unable to receive any help from Meta “for the information to be returned or destroyed”.

## Did Novant Health ask Facebook for the information to be returned or destroyed?

We reached out to Meta Facebook several times and through different channels, but never got a response.

Source: <https://www.novanthealth.org/home/privacy-statement/pixel.aspx>

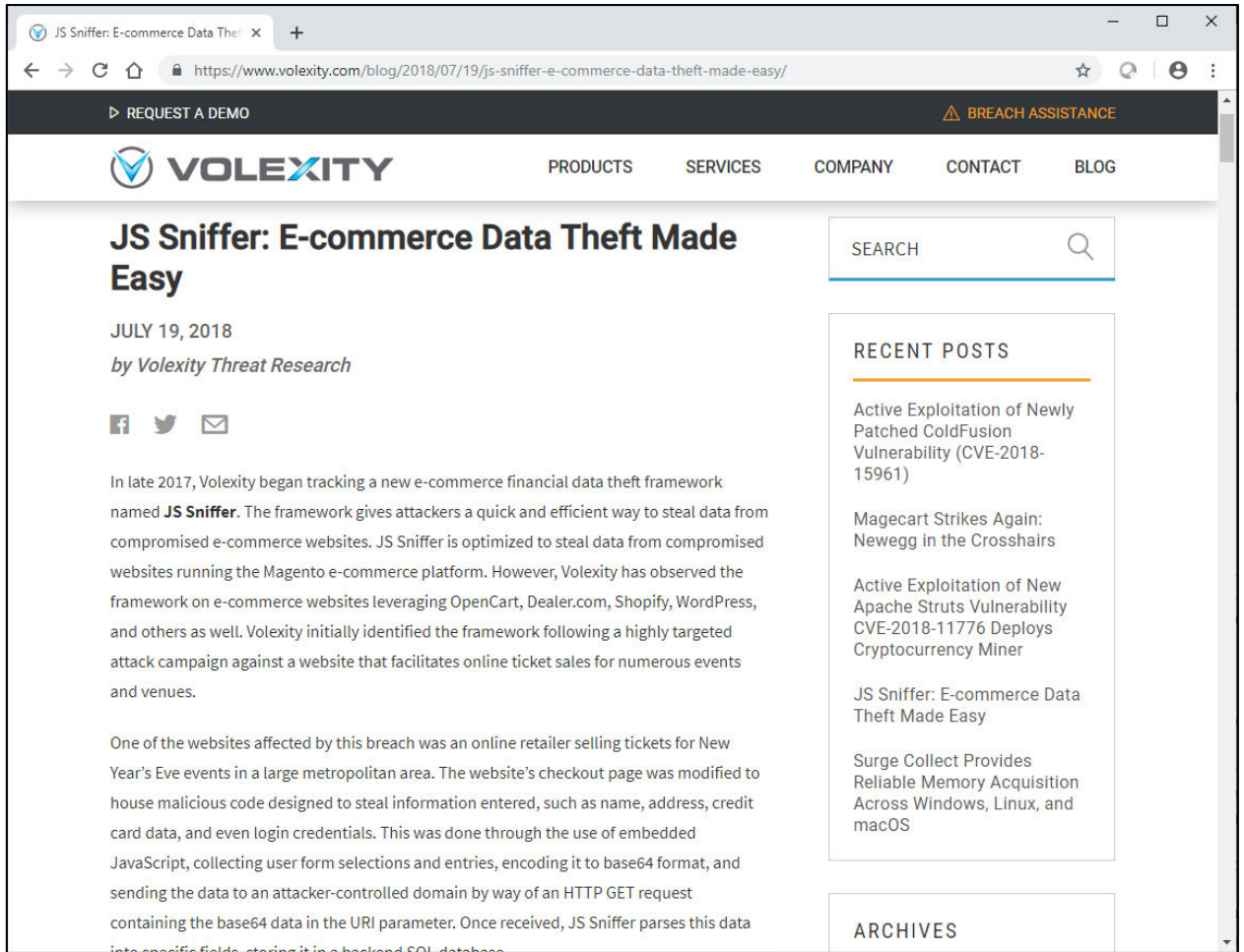
143. According to Novant Health the disclosure of PHI happened over a two year period. Apparently Facebook never notified Novant Health that Meta was receiving PHI from Novant Health.

## When did Novant Health discover this problem?

We first learned of the possibility in May of this year when a reporter called and asked about the use of MetaPixel. We immediately removed the MetaPixel and launched an investigation, during which we tried to determine what, if any, information may have been shared with Meta.

Source: <https://www.novanthealth.org/home/privacy-statement/pixel.aspx>

144. Cybercriminals also use JavaScript form scraping to steal personal information, credit card details, and login information including passwords. See for example *JS Sniffer: E-commerce Data Theft Made Easy*:



Source: <https://www.volexity.com/blog/2018/07/19/js-sniffer-e-commerce-data-theft-made-easy/>

145. The JS Sniffer article goes on to explain how scraped form data is sent to a server controlled by cybercriminals using a tracking pixel:



JS Sniffer JavaScript will typically perform the following actions:

1. Looks for onchange events occurring for the following elements and captures element values.
  - <input>
  - <select>
  - <textarea>
2. Calls the functions responsible for checking element value modifications at an interval of every 1.5 seconds.
3. Captures the current hostname of the compromised URL in order to track where the data originates from.
4. Uses the JSON.stringify() method to convert the captured element values into JSON formatting.
5. Base64 encodes element values with the btoa() method.
6. Creates an image element with a width and height of one pixel, specifying the following values as the source:
  - Base64-encoded version of a malicious URL within the atob() method, or in plaintext
  - Appends "?image\_id=" to the URI string of the URL
  - Appends the base64-encoded data captured to the URL

### Cookie Syncing

146. Based on a security policy known as same-origin policy, Web browsers prevent one Web site from accessing the cookies of another Web site. For example, Google is prevented from receiving Facebook cookies in the HTTP headers of an HTTP request.

147. See for example, *Same-origin policy*:

## Cross-origin data storage access

Access to data stored in the browser such as `localStorage` and `IndexedDB` are separated by origin. Each origin gets its own separate storage, and JavaScript in one origin cannot read from or write to the storage belonging to another origin.

Cookies use a separate definition of origins. A page can set a cookie for its own domain or any parent domain, as long as the parent domain is not a public suffix. Firefox and Chrome use the [Public Suffix List](#) to determine if a domain is a public suffix. Internet Explorer uses its own internal method to determine if a domain is a public suffix. The browser will make a cookie available to the given domain including any sub-domains, no matter which protocol (HTTP/HTTPS) or port is used. When you set a cookie, you can limit its availability using the Domain, Path, Secure and Http-Only flags. When you read a cookie, you cannot see from where it was set. Even if you use only secure https connections, any cookie you see may have been set using an insecure connection.

Source: [https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin\\_policy](https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy)

148. However, JavaScript code running in a Web page can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to an unrelated Web site. This technique is known in the Internet advertising business as “cookie syncing”. The technique allows two cooperating Web sites to learn each other’s cookie id numbers for the same user. Once the cookie syncing operation is completed, the two Web sites can exchange information that they have collected and hold about a user and that is associated with a cookie id number. The technique can also be used to track an individual if third-party cookies are being blocked by a browser.

149. Cookie syncing is used at the MedStar Health Web site. For example, the first-party “\_fbp” www.medstarhelth.com cookie which appears to contain a unique identified number is sent to a Facebook server in a tracking pixel URL as the following two HTTP GET requests illustrate:

### Request #366

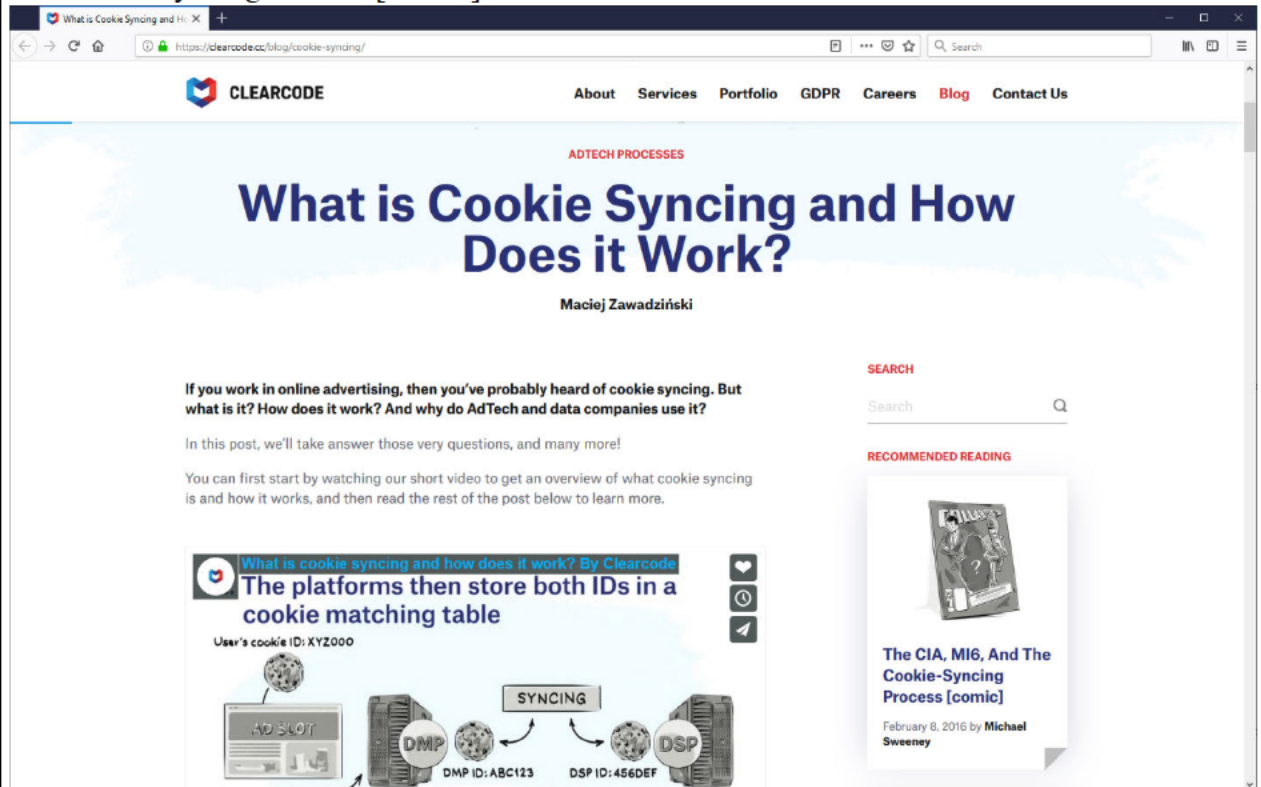
```
GET https://www.medstarhealth.org/global-search HTTP/1.1
Host: www.medstarhealth.org
Connection: keep-alive
sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
```

1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
 2 Gecko) Chrome/104.0.0.0 Safari/537.36  
 3 Accept:  
 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;  
 4 q=0.8,application/signed-exchange;v=b3;q=0.9  
 Sec-Fetch-Site: same-origin  
 5 Sec-Fetch-Mode: navigate  
 Sec-Fetch-User: ?1  
 Sec-Fetch-Dest: document  
 6 Referer: https://www.medstarhealth.org/  
 Accept-Encoding: gzip, deflate, br  
 Accept-Language: en-US,en;q=0.9  
 7 Cookie: sxa\_site=Medstar: sessionUniqueId=[REDACTED]; gcl au=[REDACTED];  
 \_tq\_id=[REDACTED]; ga=[REDACTED]; gid=[REDACTED]; dc gtm UA-  
 8 [REDACTED]=1; session=[REDACTED]=true; fbp=[REDACTED];  
 9 cebs=1; \_ce.s=[REDACTED];  
 CEFT=Q%3D%3D%3D%3D;  
 10 \_hiSessionUser=[REDACTED];  
 11 \_hjFirstSeen=1; \_hjIncludedInSessionSample=1;  
 \_hjSession=[REDACTED];  
 12 \_hjIncludedInPageviewSample=1; \_hjAbsoluteSessionInProgress=1; cebsp=1  
 13  
 14 Request #397  
 15 GET  
 16 https://www.facebook.com/tr/?id=1321071481253782&ev=PageView&dl=https%3A%2F%2F  
 www.medstarhealth.org%2Fglobal-  
 17 search%23globalprovider\_e%3D0%26globalservice\_e%3D0%26globalallocation\_e%3D0%26glo  
 balce\_e%3D0%26globalnews\_e%3D0%26globalblog\_e%3D0%26globalpatient\_e%3D0%26gl  
 18 obalarticle\_e%3D0%26globalother\_e%3D0%26globalprovider\_q%3Ddiabetes%26globalservic  
 e\_q%3Ddiabetes%26globalallocation\_q%3Ddiabetes%26globalce\_q%3Ddiabetes%26globalnews  
 19 \_q%3Ddiabetes%26globalblog\_q%3Ddiabetes%26globalpatient\_q%3Ddiabetes%26globalarticl  
 e\_q%3Ddiabetes%26globalother\_q%3Ddiabetes%26globalprovider\_g%3D%26globalallocation\_  
 20 g%3D%26globalprovider\_distance%2520by%2520miles%3D25000%26globalallocation\_distan  
 e%2520by%2520miles%3D25000&rl=https%3A%2F%2Fwww.medstarhealth.org%2F&if=fals  
 e&ts=1660253547858&sw=1920&sh=1080&v=2.9.75&r=stable&ec=0&o=30&fbp=[REDACTED]  
 21 &it=1660253547783&coo=false&rqm=GET HTTP/1.1  
 Host: www.facebook.com  
 22 Connection: keep-alive  
 sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"  
 23 sec-ch-ua-mobile: ?0  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
 24 Gecko) Chrome/104.0.0.0 Safari/537.36  
 sec-ch-ua-platform: "Windows"  
 25 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8  
 Sec-Fetch-Site: cross-site  
 26 Sec-Fetch-Mode: no-cors  
 Sec-Fetch-Dest: image  
 27 Referer: https://www.medstarhealth.org/  
 Accept-Encoding: gzip, deflate, br  
 28 Accept-Language: en-US,en;q=0.9

1 Cookie: sb= : datr= : dpr=2:  
 2 c\_user= : xs=  
 3 fr=

4 150. The first HTTP GET request shows the \_fbp cookie value being sent to  
 5 www.medstarhealth.org in a HTTP Cookie header. The second HTTP GET request shows the \_fbp  
 6 cookie value being sent to a Facebook server in a tracking pixel URL. The \_fbp cookie values are  
 7 marked in yellow. The Facebook server also receives in the second HTTP GET request, its c\_user  
 8 cookie which is marked in green.

9 151. See also, What is Cookie Syncing and How Does it Work? and The CIA, MI6, and  
 10 the Cookie Syncing Process [Comic]:



23 Source: <https://clearcode.cc/blog/cookie-syncing/>





Source: <https://clearcode.cc/blog/the-cia-mi6-and-the-cookie-syncing-process-comic/>

### Cross-device Tracking

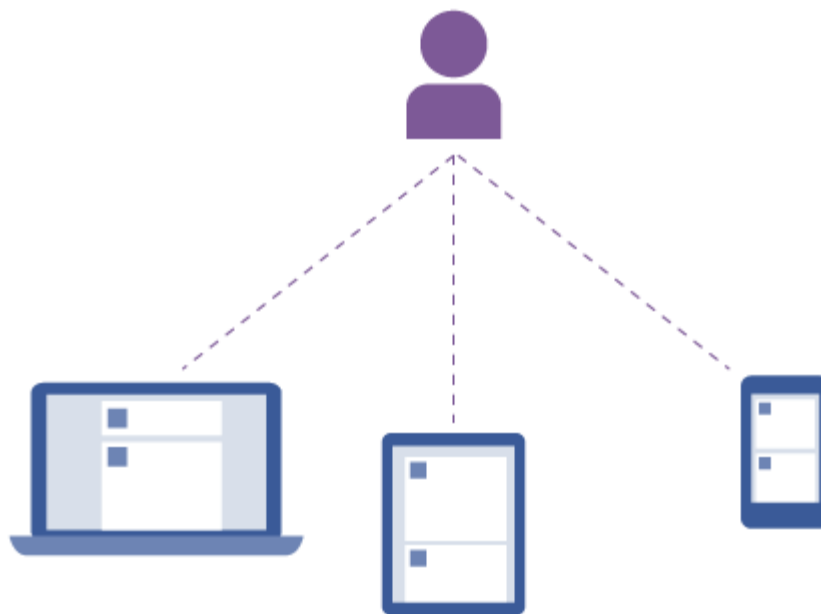
152. Today it is not uncommon for people to access Web sites from multiple devices such as personal computers, smartphones, and tablets. In addition, apps on smartphones and tablets are now used regularly to access services as a replacement for using Web sites.

153. In order to provide targeted advertising to a specific individual, regardless of which one of their devices they are using, the Internet advertising industry has adopted a technology called cross-device tracking.

154. Meta is an example of an Internet company which does cross-device tracking. See for example *Advertise to real people cross-device*:

**The solution:** Instead of relying on search interests based on cookies, which can cause overlap, target real individuals. This is where Facebook has it's biggest advantage over competitors. It's the only platform where you can actively target individuals who might be interested in your products (instead of hoping that you show up in search).

One great way to reach real people is with *Custom Audiences from your website*. These identify people with Facebook IDs who have visited specific product pages or added products to a cart. Once a Custom Audience pixel is placed on your website, you can use that data to remarket to visitors across all their devices.



Source: <https://www.facebook.com/business/a/performance-marketing-strategies>

155. As the Facebook Web page describes above, unique Facebook IDs and tracking pixels (called here Custom Audience Pixel) enable cross-device tracking and ad targeting.

156. Meta's cross-device tracking is also described in the 2015 article *2015 Edition: A Marketer's Guide To Cross-Device Identity*:

With the relaunch of its Atlas ad server, Facebook entered the cross-device scene in a big way with a persistent tracking mechanism that trades on the company's relationship with users who are logged in across devices. It also recently released cross-device reports and audience extension tools.



Facebook claims to be able to place display, video and mobile ads in nearly any environment currently served by Google's DoubleClick for Advertisers, a chief competitor to Atlas. Atlas can identify and serve ads to users across devices both on Facebook's owned and operated properties, including its mobile app, Facebook.com and Instagram, as well as on thousands of other sites and apps via a combination of its Facebook ID, the Facebook SDK and device ad IDs like Apple's IDFA and Google's own Advertising ID. That means that as long as users stay logged in on multiple devices, Atlas will be able to target them – even if those users are engaging with apps that don't use a social login from Facebook.

Source: <https://adexchanger.com/data-exchanges/a-marketers-guide-to-cross-device-identity/>

### How the Meta Pixel operates when not logged into Facebook

157. When a user logs out of their Facebook account, some of their Facebook cookies are deleted. These cookies are c\_user, xs, and presence.

158. During the Facebook logout process other cookies are not deleted. These cookies are the datr, and sb. As described previously, the datr cookie identifies a user's browser.

159. The following HTTP request and response for the logout process shows the Facebook cookies which are deleted and the cookies which are preserved<sup>11</sup>:

#### Request #12

```
POST
https://www.facebook.com/logout.php?button_location=settings&button_name=logout
HTTP/1.1
Host: www.facebook.com
Connection: keep-alive
Content-Length: 28
Cache-Control: max-age=0
viewport-width: 960
sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-ch-prefers-color-scheme: light
Upgrade-Insecure-Requests: 1
Origin: https://www.facebook.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

<sup>11</sup> HTTP requests and responses in this section are from the Fiddler capture file All-No-FB-SignIn-2022-08-17.saz.

Sec-Fetch-Mode: navigate  
 Sec-Fetch-User: ?1  
 Sec-Fetch-Dest: document  
 Referer: https://www.facebook.com/  
 Accept-Encoding: gzip, deflate, br  
 Accept-Language: en-US,en;q=0.9  
 Cookie: sb=[REDACTED]; datr=[REDACTED]  
 dpr=2; locale=en\_US; wd=[REDACTED]; c\_user=[REDACTED]  
 xs=[REDACTED]  
 fr=[REDACTED]  
 presence=[REDACTED]  
 Pretty-printed form data  
 h=AfcJGHJ0cx8CaijoobE  
 ref=mb  
 HTTP/1.1 302 Found  
 Set-Cookie: c\_user=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=-1660761823; path=/; domain=.facebook.com  
 Set-Cookie: xs=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=-1660761823; path=/; domain=.facebook.com; httponly  
 Set-Cookie: presence=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=-1660761823; path=/; domain=.facebook.com  
 Location:  
 https://www.facebook.com/?stype=lo&jlou=[REDACTED]  
 &lh=[REDACTED]  
 x-robots-tag: noindex, nofollow  
 Access-Control-Expose-Headers: X-FB-Debug, X-Loader-Length  
 Access-Control-Allow-Methods: OPTIONS  
 Access-Control-Allow-Credentials: true  
 Access-Control-Allow-Origin: https://www.facebook.com  
 Vary: Origin  
 Strict-Transport-Security: max-age=15552000; preload  
 Content-Type: text/html; charset="utf-8"  
 X-FB-Debug:  
 [REDACTED]  
 Date: Wed, 17 Aug 2022 18:43:44 GMT  
 Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
 Connection: keep-alive  
 Content-Length: 0

160. Deleted Facebook cookies are marked in yellow, while preserved Facebook cookies are marked in green.

161. The preservation of the datr cookie still allows Meta to track a logged-out Facebook user at a Web hospital's Web site as shown in the following HTTP request for the Meta Pixel at the MedStar Health Web site:

Request #146

GET

https://www.facebook.com/tr/?id=1321071481253782&ev=SubscribedButtonClick&dl=http  
s%3A%2F%2Fwww.medstarhealth.org%2Fmymedstar-patient-  
portal&rl=https%3A%2F%2Fwww.medstarhealth.org%2F&if=false&ts=1660761846242&c  
d[buttonFeatures]=%7B%22classList%22%3A%22%22%2C%22destination%22%3A%22h  
ttps%3A%2F%2Fcernerhealth.com%2Foauth%2Fauthenticate%3Fredirect\_uri%3Dhttps%2  
53A%252F%252Fcernerhealth.com%252Fsaml%252Fsso%252Fresponse%253Fmessage\_i  
d%253D\_b8d84877-f619-437f-83f2-  
6019833eafd5%2526issuer%253Dhttps%25253A%25252F%25252Fmymedstar.iqhealth.co  
m%25252Fsession-  
api%25252Fprotocol%25252Fsaml2%25252Fmetadata%26sign\_in\_only%3Don%26client\_  
id%3Dae737c6564c345c2b9ac1294f98c75c0%22%2C%22id%22%3A%22%22%2C%22im  
ageUrl%22%3A%22%22%2C%22innerText%22%3A%22Log%20in%22%2C%22numChil  
dButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22na  
me%22%3A%22%22%7D&cd[buttonText]=Log%20in&cd[formFeatures]=%5B%5D&cd[  
pageFeatures]=%7B%22title%22%3A%22myMedStar%20%7C%20Your%20Patient%20P  
ortal%20%7C%20MedStar%20Health%22%7D&cd[parameters]=%5B%5D&sw=1920&sh  
=1080&v=2.9.75&r=canary&ec=2&o=30&ttf=5433.200000000186&ttts=583.70000000018  
63&ttse=648.1000000000931&fbp=fb[REDACTED]&it=1660761841391&  
coo=false&es=automatic&tm=3&rqm=GET HTTP/1.1

Host: www.facebook.com

Connection: keep-alive

sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/104.0.0.0 Safari/537.36

sec-ch-ua-platform: "Windows"

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: image

Referer: https://www.medstarhealth.org/

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Cookie: sb=[REDACTED]; datr=[REDACTED];

dpr=2; locale=en\_US;

fr=[REDACTED]

162. Marked in yellow in this HTTP GET for the Meta Pixel which remain unchanged  
after logging out of a Facebook account.

### Tracking Pixels and HIPAA

163. Under HIPAA privacy rules, certain kinds of identifiers are considered Protected  
Health Information (PHI). See 45 C.F.R. § 164.514:

#### 1. Names

2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to currently publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of 90 or older;

4. Telephone numbers;

5. Fax numbers;

6. Electronic mail addresses;

7. Social Security numbers;

8. Medical record numbers;

9. Health plan beneficiary numbers;

10. Account numbers;

11. Certificate/license numbers;

12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);

15. Internet Protocol (IP) address numbers;

16. Biometric identifiers, including finger and voice prints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code.

In addition, data is considered HIPAA PHI if the covered entity has actual knowledge “that the

1 information could be used alone or in combination with other information to identify an individual  
2 who is a subject of the information.”

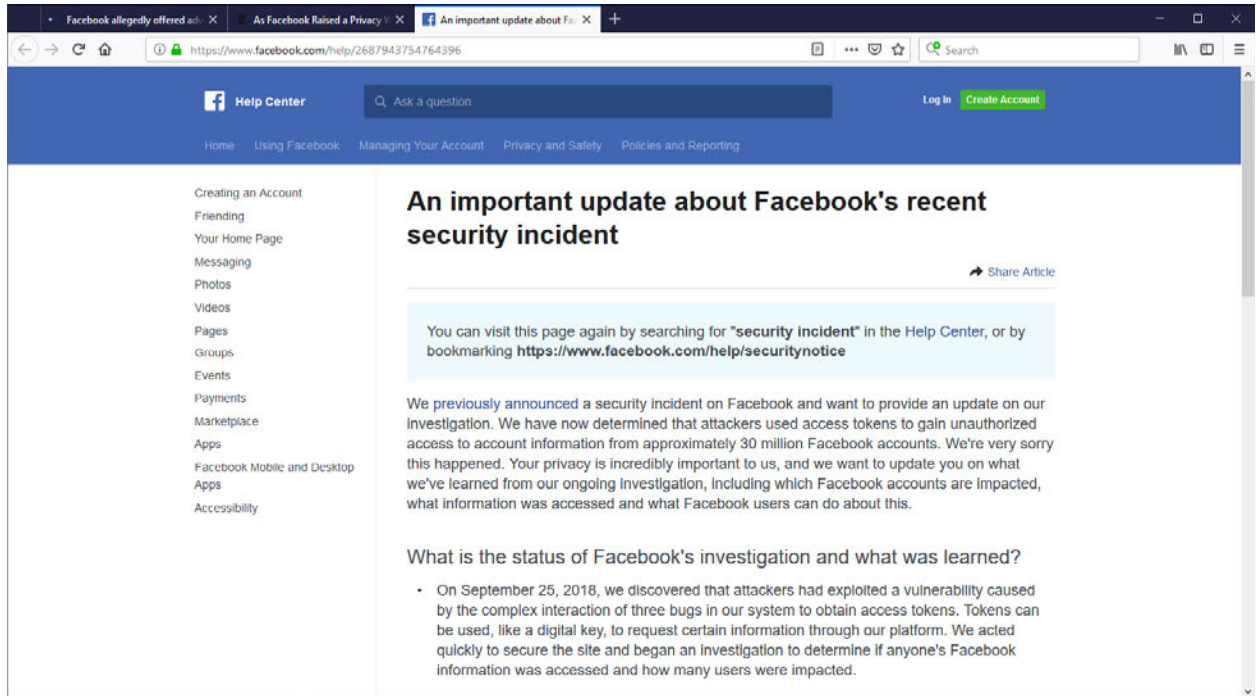
3 164. Of these Protected Health Information identifiers, at least five identifiers are  
4 routinely sent to third-parties in tracking pixels when a MedStar Health patient is communicating  
5 with a MedStar Health hospital at a MedStar Health Web site:

- 6 a. Web URL
- 7 b. IP address
- 8 c. Account number in the form of cookie id numbers or in a URL query string
- 9 parameter
- 10 d. Device identifiers and serial numbers
- 11 e. Any other characteristic that could uniquely identify the individual

#### 12 **Privacy and Security Problems at Facebook.com**

13 165. Over the past few years, various privacy and security problems have come to light at  
14 Facebook and how it handles data collected as people use the Web and run apps.

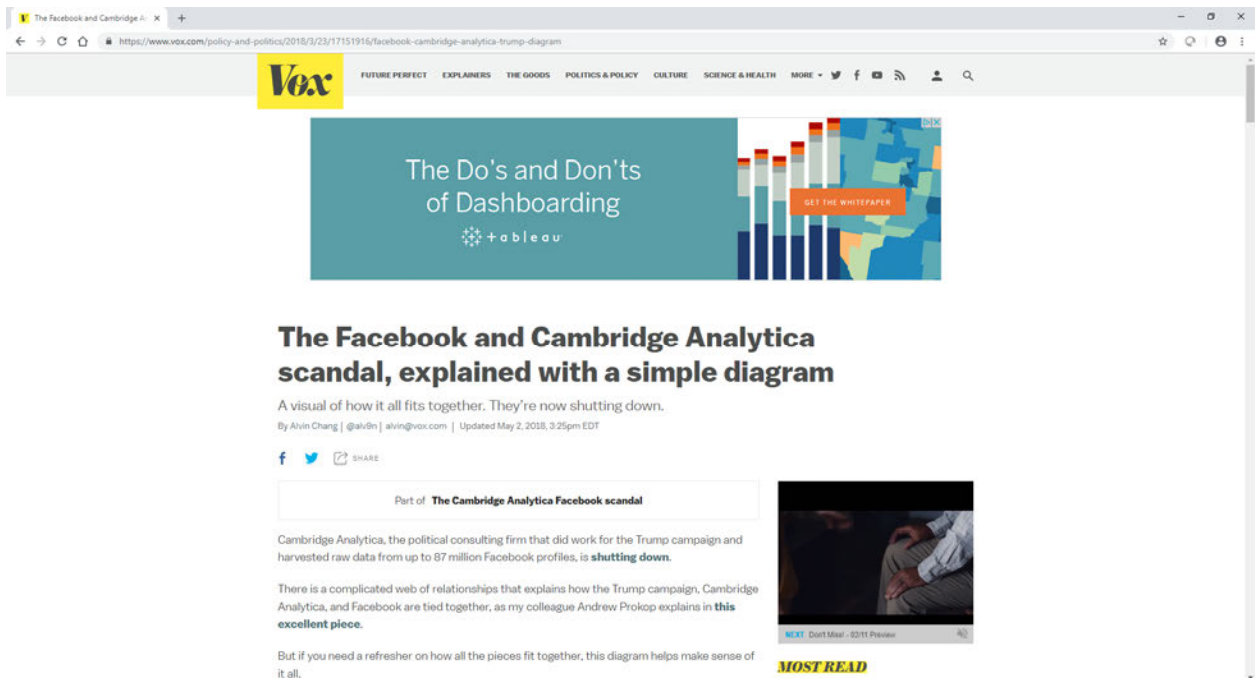
15 166. For example, on September 25, 2018, Facebook discovered that access tokens were  
16 obtained by attackers for almost 90 million Facebook users. These access tokens permitted the  
17 unknown attackers to obtain information about Facebook users associated with the stolen access  
18 tokens. Facebook describes the incident on this Web page:



Source: <https://www.facebook.com/help/2687943754764396>

167. In the spring of 2018, it was revealed that a political consulting company based in the UK, named Cambridge Analytica, had used a quiz app to secretly extract information for 87 million Facebook profiles. The security breach generated extensive press coverage in the United States and has been called the Facebook and Cambridge Analytica scandal. The security breach only came to light because of a whistleblower named Aleksandr Kogan who worked with Cambridge Analytica. The following is an example of one of the press articles which describes how the security breach was allowed to happen:





Source: <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>

168. According to press reports, Facebook is being investigated by the DOJ, SEC, FTC, and FBI because of the Cambridge Analytica data breach. See for example:



Source: <https://www.engadget.com/2018/07/02/fbi-sec-ftc-facebook-cambridge-analytica-probe/>

169. Based on internal Facebook documents obtained by the British government, the New York Times and Washington Post report in December 2018 that Facebook gave special access to user data to large advertisers in spite of previous claims to the contrary:



Source: <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

170. In a March 6, 2019 post entitled *A Privacy-Focused Vision for Social Networking*, by Facebook's CEO, Mark Zuckerberg, no mention is made of Facebook's third-party tracking and data collection at Web sites such as the MedStar Health Web site:



Source: <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/>

### **The use of the Meta Pixel at other Hospital Web sites**

171. In addition to testing the Meta Pixel at the MedStar Health Web site, I also did Meta Pixel testing at these four additional hospital Web sites:

- a. Rush University System for Health - rush.edu
- b. Hartford HealthCare - hartfordhospital.org
- c. Summa Health System - www.summahealth.org
- d. University Hospitals - www.uhhospitals.org

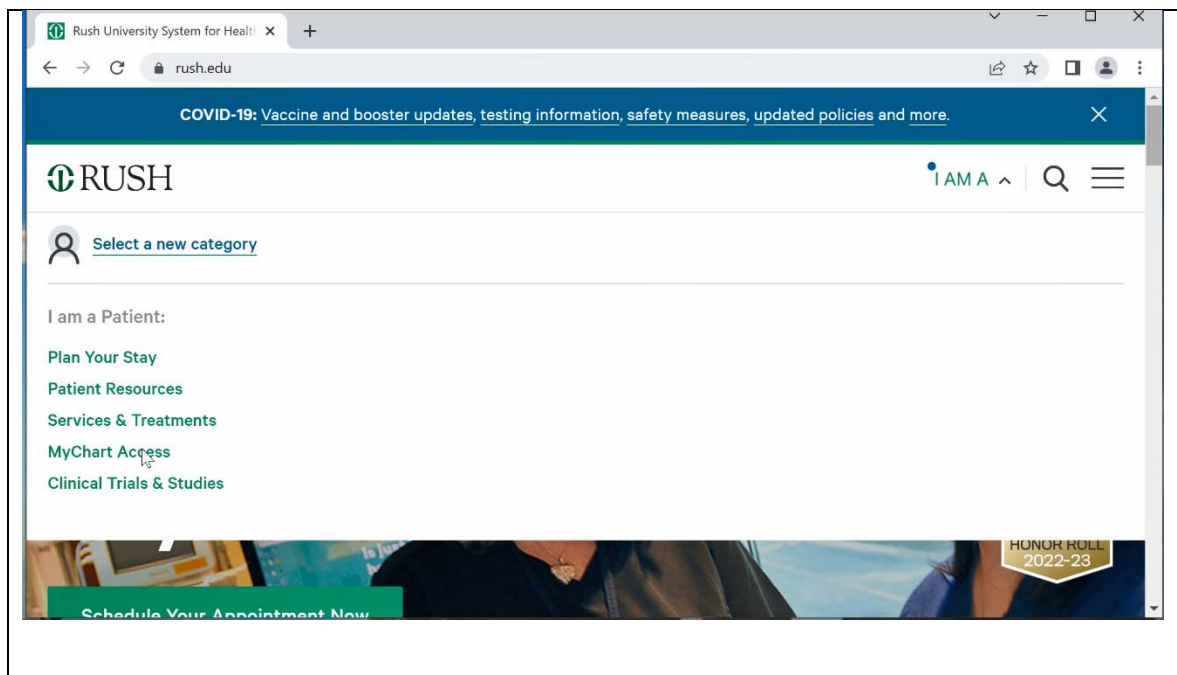
172. I found that the Meta Pixel operated in the same manner at these four hospital Web sites as the MedStar Health Web site.

173. In particular, I found that Meta Pixel SubscribedButtonClick tracking events were sent to Facebook Web servers when clicking on links or buttons for the patient portals of the four Web sites.

174. Information sent to the Facebook Web servers with the HTTP GET requests with each SubscribedButtonClick tracking events include:

- a. The IP address of my computer
- b. My Facebook c\_user, datr, sb, fr, and xs cookies
- c. The \_fbp cookie stored as a hospital Web site cookie, but transmitted to Facebook in the query string of a Meta Pixel URL
- d. Identification of the event as a SubscribedButtonClick event
- e. The URL of the Web page with the button or linked that was clicked
- f. The URL of the patient portal login page
- g. The text of the login link or button

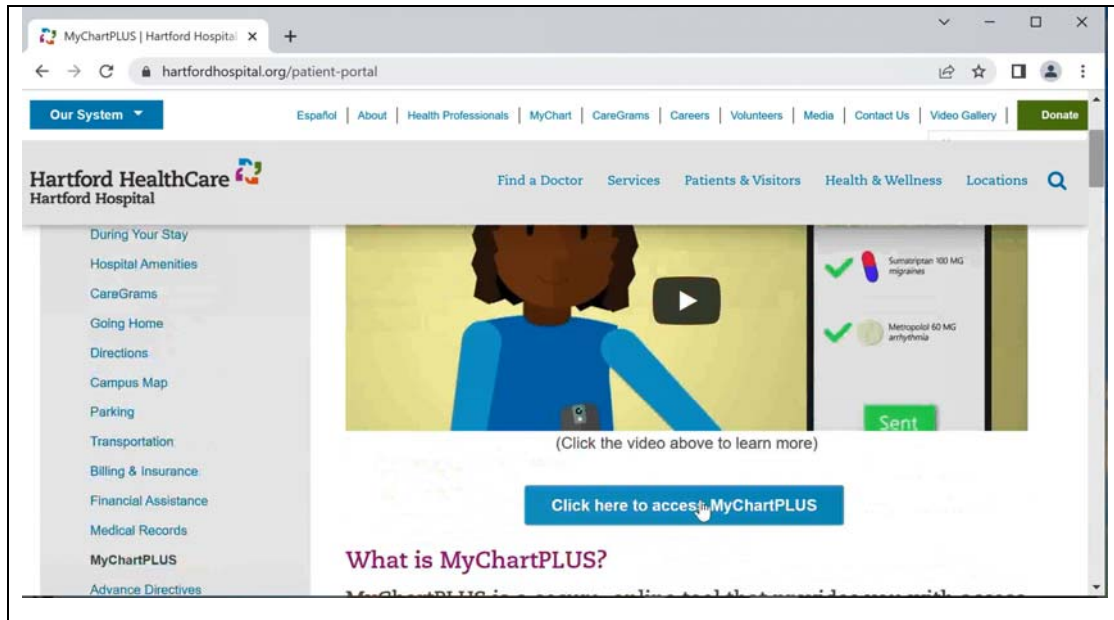
175. The following screen shot from the Rush University System for Health Web site shows how the “I am a Patient” menu can be used to access the MyChart patient portal:







178. The following screen shot from the Hartford HealthCare Web site shows how the MyChartPLUS patient portal can be accessed from the patient portal home page:



Source: <https://hartfordhospital.org/patient-portal>

179. The following HTTP GET request from the Fiddler capture file hartfordhospital-2022-08-16.saz, shows the clicking of the “Click here to access MyChartPLUS” link in the above screen shot being tracked by Meta using the Meta Pixel:

Request #400

GET

```
https://www.facebook.com/tr/?id=813018392549117&ev=SubscribedButtonClick&dl=https%3A%2F%2Fhartfordhospital.org%2Fpatient-portal&rl=https%3A%2F%2Fhartfordhospital.org%2Fpatients-and-visitors%2Ffor-patients%2Fbefore-you-arrive&if=false&ts=1660683910169&cd[buttonFeatures]=%7B%22classList%22%3A%22button%22%2C%22destination%22%3A%22https%3A%2F%2Fmychartplus.org%2F%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Click%20here%20to%20access%20MyChartPLUS%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=Click%20here%20to%20access%20MyChartPLUS&cd[formFeatures]=%5B%7B%22id%22%3A%22_EVENTTARGET%22%2C%22name%22%3A%22_EVENTTARGET%22%2C%22tag%22%3A%22input%22%2C%22inputType%22%3A%22hidden%22%2C%22valueMeaning%22%3A%22empty%22%7D%2C%7B%22id%22%3A%22_EVENTARGUMENT%22%2C%22name%22%3A%22_EVENTARGUMENT%22%2C%22tag%22%3A%22input%22%2C%22inputType%22%3A%22hidden%22%2C%22valueMeaning%22%3A%22empty%22%7D%2C%7B%22id%22%3A%22servicelinebtn%22%2C%22name%22%3A%22%22%2C%22tag%22%3A%22button%22%7D%2C%7B%22id%22%3A%22hfSearchUrl%22%2C%22name%22%3A%22ctl01%24ppheader_2_0%24hfSearchUrl%22%2C%22tag
```

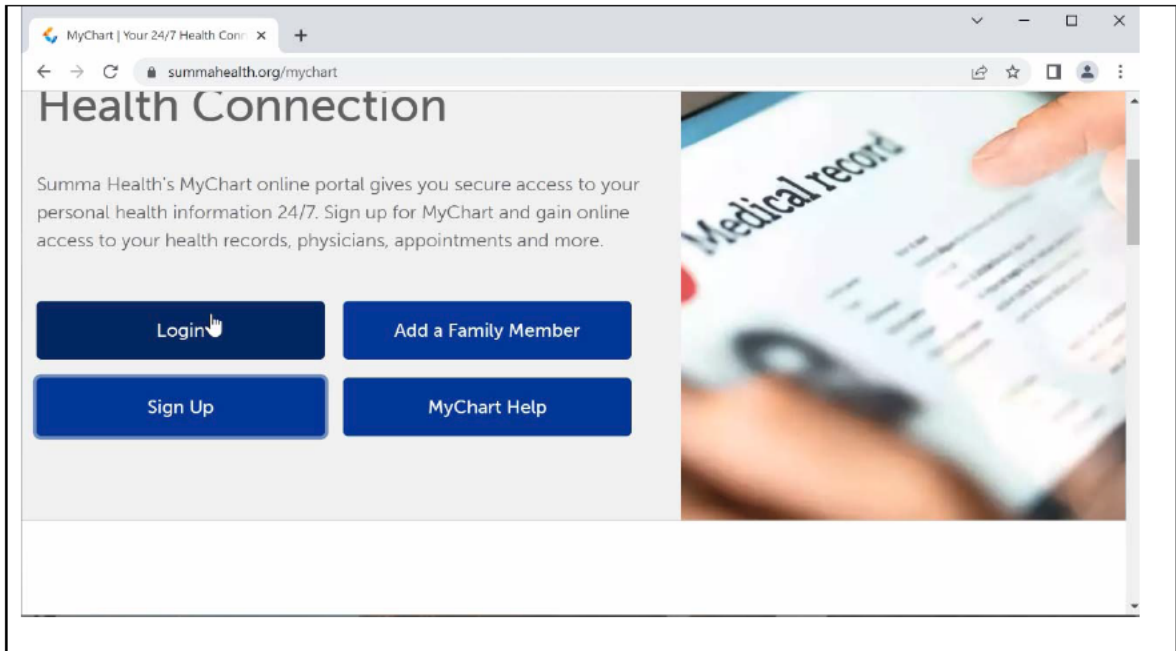


%22%3A%22input%22%2C%22inputType%22%3A%22hidden%22%7D%2C%7B%22id%22%3A%22inputSearch%22%2C%22name%22%3A%22ctl01%24ppheader\_2\_0%24inputSearch%22%2C%22tag%22%3A%22input%22%2C%22placeholder%22%3A%22Search%20by%20keyword...%22%2C%22inputType%22%3A%22search%22%2C%22valueMeaning%22%3A%22empty%22%7D%2C%7B%22id%22%3A%22\_VIEWSTATE%22%2C%22name%22%3A%22\_VIEWSTATE%22%2C%22tag%22%3A%22input%22%2C%22inputType%22%3A%22hidden%22%7D%5D&cd[pageFeatures]=%7B%22title%22%3A%22MyChartPLUS%20%7C%20Hartford%20Hospital%20%7C%20Hartford%2C%20CT%22%7D&cd[parameters]=%5B%5D&sw=1920&sh=1080&v=2.9.75&r=stable&ec=2&o=30&fbp=fb [REDACTED]&it=1660683899734&coo=false&es=automatic&tm=3&rqm=GET HTTP/1.1

Host: www.facebook.com  
 Connection: keep-alive  
 sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"  
 sec-ch-ua-mobile: ?0  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36  
 sec-ch-ua-platform: "Windows"  
 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8  
 Sec-Fetch-Site: cross-site  
 Sec-Fetch-Mode: no-cors  
 Sec-Fetch-Dest: image  
 Referer: https://hartfordhospital.org/  
 Accept-Encoding: gzip, deflate, br  
 Accept-Language: en-US,en;q=0.9  
 Cookie: sb=[REDACTED]; datr=[REDACTED]; dpr=2;  
 c\_user=[REDACTED]; xs=[REDACTED]  
 fr=[REDACTED]

180. Cookie values sent to the Facebook server as part of the Meta Pixel are marked in yellow.

181. The following screen shot from the Summa Health Web site shows how the MyChart patient portal login page can be accessed from the patient portal home page:



Source: <https://www.summahealth.org/mychart>

182. The following HTTP GET request from the Fiddler capture file summahealth-2022-08-16.saz, shows the clicking of the “Login” button in the above screen shot being tracked by Meta using the Meta Pixel:

Request #851

GET

[https://www.facebook.com/tr/?id=185622915408092&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.summahealth.org%2Fmychart&rl=https%3A%2F%2Fwww.summahealth.org%2Fpatientvisitor&if=false&ts=1660684600607&cd\[buttonFeatures\]=%7B%22classList%22%3A%22btn%20btn-primary%20d-block%20%22%2C%22destination%22%3A%22https%3A%2F%2Fchp.epicweb.health-partners.org%2Fmychart%2F%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Login%22%2C%22numChildButtons%22%3A%22%2C%22tag%22%3A%22a%22%2C%22type%22%3A%22null%2C%22name%22%3A%22%22%2C%22%7D&cd\[buttonText\]=Login&cd\[formFeatures\]=%5B%5D&cd\[pageFeatures\]=%7B%22title%22%3A%22MyChart%20%7C%20Your%2024%2F7%20Health%20Connection%20%7C%20Summa%20Health%20%22%2C%22%7D&cd\[parameters\]=%5B%5D&sw=1920&sh=1080&v=2.9.75&r=stable&ec=3&o=30&fbp=fb\[REDACTED\]&it=1660684584517&coo=false&es=automatic&tm=3&rqm=GET HTTP/1.1](https://www.facebook.com/tr/?id=185622915408092&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.summahealth.org%2Fmychart&rl=https%3A%2F%2Fwww.summahealth.org%2Fpatientvisitor&if=false&ts=1660684600607&cd[buttonFeatures]=%7B%22classList%22%3A%22btn%20btn-primary%20d-block%20%22%2C%22destination%22%3A%22https%3A%2F%2Fchp.epicweb.health-partners.org%2Fmychart%2F%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Login%22%2C%22numChildButtons%22%3A%22%2C%22tag%22%3A%22a%22%2C%22type%22%3A%22null%2C%22name%22%3A%22%22%2C%22%7D&cd[buttonText]=Login&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22MyChart%20%7C%20Your%2024%2F7%20Health%20Connection%20%7C%20Summa%20Health%20%22%2C%22%7D&cd[parameters]=%5B%5D&sw=1920&sh=1080&v=2.9.75&r=stable&ec=3&o=30&fbp=fb[REDACTED]&it=1660684584517&coo=false&es=automatic&tm=3&rqm=GET HTTP/1.1)

Host: www.facebook.com

Connection: keep-alive

sec-ch-ua: "Chromium";v="104", "Not A;Brand";v="99", "Google Chrome";v="104"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

sec-ch-ua-platform: "Windows"

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8

Sec-Fetch-Site: cross-site

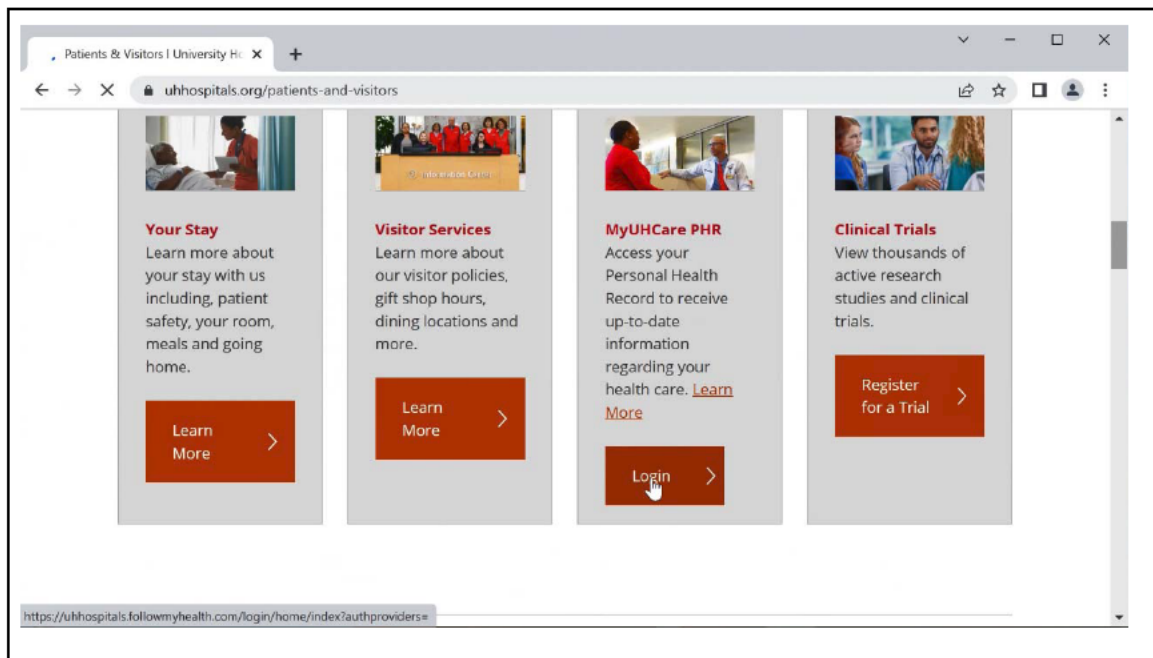
Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: image

Referer: https://www.summahealth.org/  
 Accept-Encoding: gzip, deflate, br  
 Accept-Language: en-US,en;q=0.9  
 Cookie: sb=[REDACTED]; datr=[REDACTED]; dpr=2;  
 c\_user=[REDACTED]; xs=[REDACTED]  
 fr=[REDACTED]

183. Cookie values sent to the Facebook server as part of the Meta Pixel are marked in yellow.

184. The following screen shot from the University Hospitals Web site shows how the MyUHCare patient portal login page can be accessed from the patient and visitors Web page:



Source: <https://www.uhhospitals.org/patients-and-visitors>

185. The following HTTP GET request from the Fiddler capture file uh-2022-08-16.saz, shows the clicking of the “Login” button in the above screen shot being tracked by Meta using the Meta Pixel

Request #1119  
 GET  
<https://www.facebook.com/tr/?id=1560987200878878&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.uhhospitals.org%2Fpatients-and-visitors&rl=https%3A%2F%2Fwww.uhhospitals.org%2Fdoctors&if=false&ts=166068557216>

9&cd[buttonFeatures]=%7B%22classList%22%3A%22%22%2C%22destination%22%3A%22https%3A%2F%2Fuhhospitals.followmyhealth.com%2Flogin%2Fhome%2Findex%3Fauthproviders%3D%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Login%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=Login&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Patients%20%26%20Visitors%20%20University%20Hospitals%20%20Cleveland%2C%20OH%20%7C%20University%20Hospitals%22%7D&cd[parameters]=%5B%5D&sw=1920&sh=1080&v=2.9.75&r=stable&ec=2&o=30&fbp=fb[REDACTED]&it=1660685564326&coo=false&es=automatic&tm=3&rqm=GET HTTP/1.1

Host: www.facebook.com

Connection: keep-alive

sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

sec-ch-ua-platform: "Windows"

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: image

Referer: https://www.uhhospitals.org/

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Cookie: sb=[REDACTED]; datr=[REDACTED]; dpr=2;

c user=[REDACTED]; xs=[REDACTED]

tr=[REDACTED]

186. Cookie values sent to the Facebook server as part of the Meta Pixel are marked in yellow.

### Health-related Ad Targeting at Facebook.com

187. After visiting the four additional Hospital Web sites, I returned to the Facebook Web site. I found in my feed many new health-related advertisements. Previously, I had seen very few health-related advertisements in my feed.

188. The following are examples of the health-related ads which appeared in my Facebook feed during a number of Facebook sessions:

///

///

///

///



KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California



Dexcom

Sponsored ·

Get easier diabetes management without fingersticks\*. Dexcom G6 is easy to use†, discreet, and covered by Medicare‡.

\*Fingersticks required for diabetes treatment decisions if symptoms or expectations do not match readings.

†Patients must meet coverage criteria.

‡Dexcom, data on file, 2020. dQ&A Diabetes... See more

**"Dexcom G6  
makes living with  
diabetes so  
much easier."**

**Earl G.**  
Real Dexcom user



**Dexcom G6**  
covered by Medicare


**1 (800) 380-5331**

///

///


KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California

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



**Fallon Health**  
 Sponsored · 🌐

Where do you need to go? Rides to the doctor, grocery store and more are free with Fallon's NaviCare® HMO SNP and SCO plans.



FCHP.ORG  
**Free rides.**  
 See if you qualify today.

[Learn more](#)

///  
///  
///



KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California

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

The screenshot shows a social media post from the American Heart Association, marked as 'Sponsored'. The text of the post reads: 'Listen to the HCM podcasts anytime. Hear from experts on diagnosing and managing hypertrophic cardiomyopathy at any age.' Below the text is a large graphic. On the left is the American Heart Association logo (a red heart with a white torch). In the center, there is a red audio waveform. To the right of the waveform is a large, black silhouette of a microphone. Below the waveform, the text 'HYPERTROPHIC CARDIOMYOPATHY PODCASTS' is written in bold, black, uppercase letters. Underneath that, a red rectangular box contains the text 'HCM Information on Demand' in white, italicized font.

///  
///  
///  
///  
///

KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California

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



**American Diabetes Association – DiabetesPro**  

Focus on Diabetes™ provides free continuing education courses so you can better understand the connection between diabetes and eye health.

**Learn how to**  
**help your patients**  
**manage their**  
**eye health.**

///  
///  
///  
///  
///  
///

KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California



Tufts Health Plan

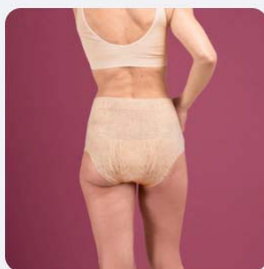
Sponsored · 🌐



Smile! For those 65+ qualifying for MassHealth Standard, Tufts Health Plan Senior Care Options (HMO-SNP) offers free dental benefits.



**\$0 dental, including crowns,  
implants, and more**




**Don't Buy Adult Diapers  
Until You Read This!**


[worldnewsyou.com](http://worldnewsyou.com)



KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California


**Myomo**  
Sponsored ·


After stroke, Jay Jay was left with a partially paralyzed arm. Thanks to MyoPro, he's back under the hood.



**JAY JAY,  
STROKE SURVIVOR**

**MyoPro powered arm  
brace**  
FREE virtual screening



[Learn more](#)






**INDEPENDENCE  
WITHIN REACH**

**Regain arm function**  
FREE virtual screening

[Learn more](#)

  2K

278 Comments 115 Shares

 Like     Comment     Share

19 ///  
20 ///  
21 ///  
22 ///  
23 ///  
24 ///  
25 ///  
26 ///  
27 ///  
28 ///





Overcoming PTSD

Sponsored · 🌐



Are you ready to leave the past behind and take your life to the next level?

If so, click below to get a FREE copy of my newest book that teaches you 9 powerful relief tools for trauma and PTSD. (just cover s&h)

## YOUR BRAIN ON TRAUMA:

- Suspicious & untrusting
- Negative & pessimistic
- Addictive
- Self sabotaging
- Scattered & distracted
- Demotivated & drained of energy
- Self critical
- Judgmental of yourself & others
- Emotionally cut off

///

///

///

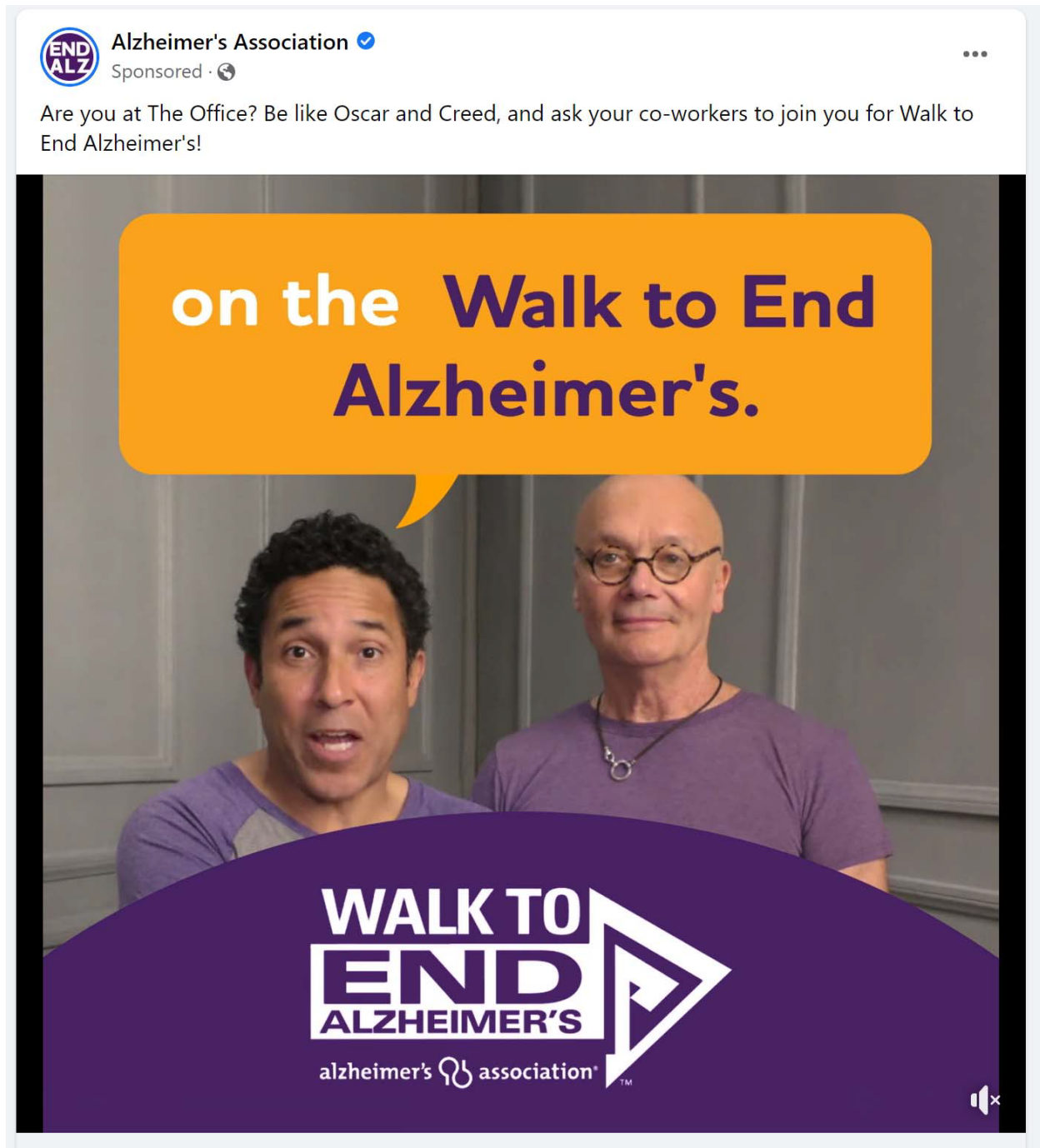
///

///



KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California


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



///  
///  
///  
///  
///


KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California

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



**The Michael J. Fox Foundation for Parkinson's Research**

Sponsored · 🌐

The Michael J. Fox Foundation donors are accelerating the most promising Parkinson's science to bring new and improved treatments to people with the disease.



**THE MICHAEL J. FOX FOUNDATION  
FOR PARKINSON'S RESEARCH**






MICHAELJFOX.ORG

**Help Fund Critical Parkinson's Research**

Not affiliated with Meta

Donate now




 1.7K

19 Comments 75 Shares

///  
///  
///

KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California

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



**Pfizer Clinical Trials** ✓  
Sponsored · ⚙️

Enjoying the fresh air shouldn't include getting Lyme disease. Learn about a clinical study for a Lyme disease vaccine.



**Seeking Active Adults And  
Children Over 5 Years Old  
For A Lyme Disease  
Vaccine Clinical Study**



///  
///  
///  
///  
///




KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California



**Livongo**  
Sponsored ·

Livongo empowers you to manage your health, offering personalized support for blood pressure. Eligibility requirements apply. Check if you're eligible.



READY.LIVONGO.COM

**Heart Health Made Easier**

Livongo empowers people with chronic conditions to live better and healthi...

[Learn more](#)



///

///

///

KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

**NUE Life Health**  
Sponsored · 

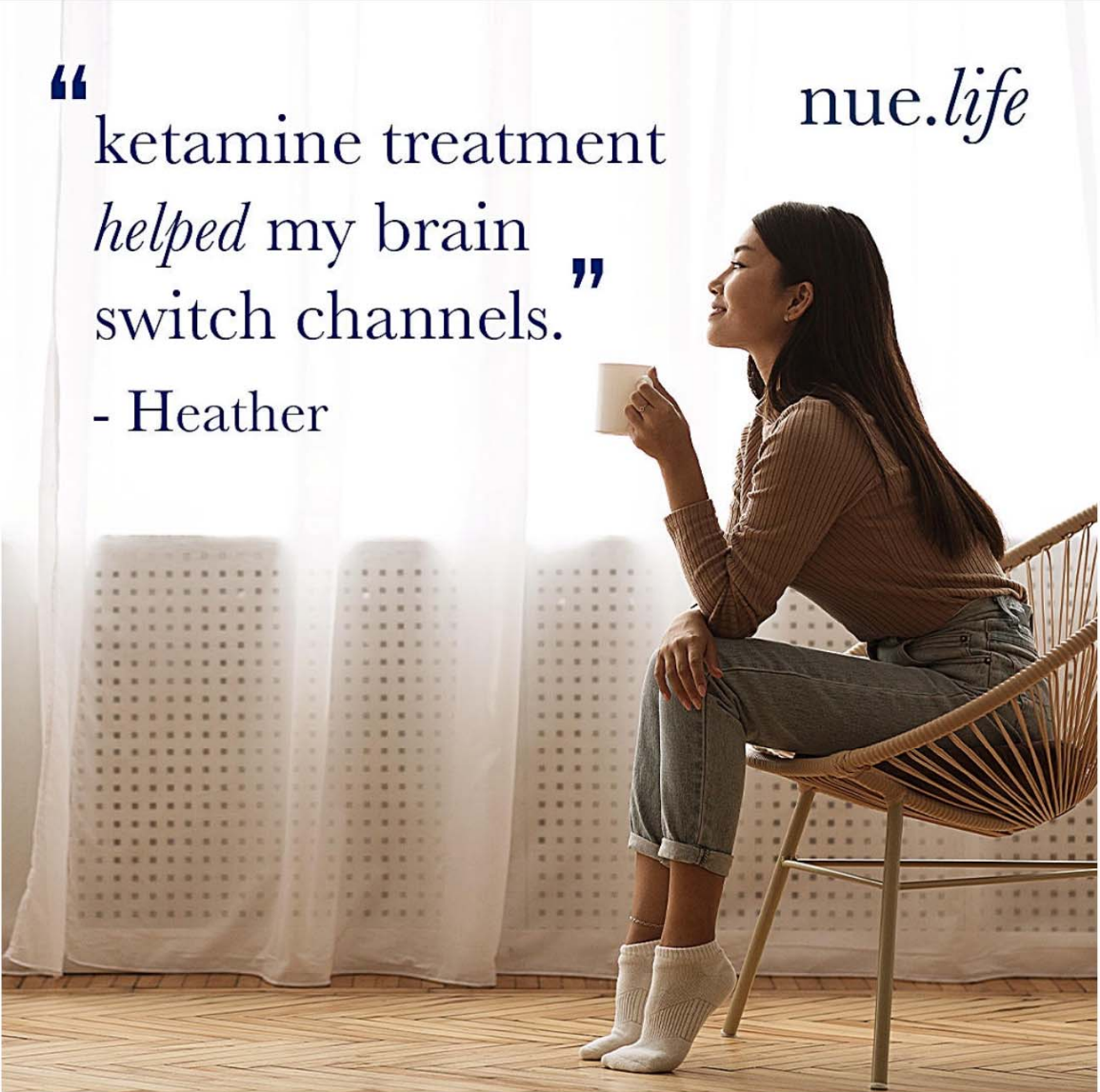
Experience a safe and fast-acting antidepressant in the comfort of your home.

“

ketamine treatment  
*helped* my brain  
switch channels.”

”

- Heather



NUE.LIFE

Discover A More Functional You

Learn more

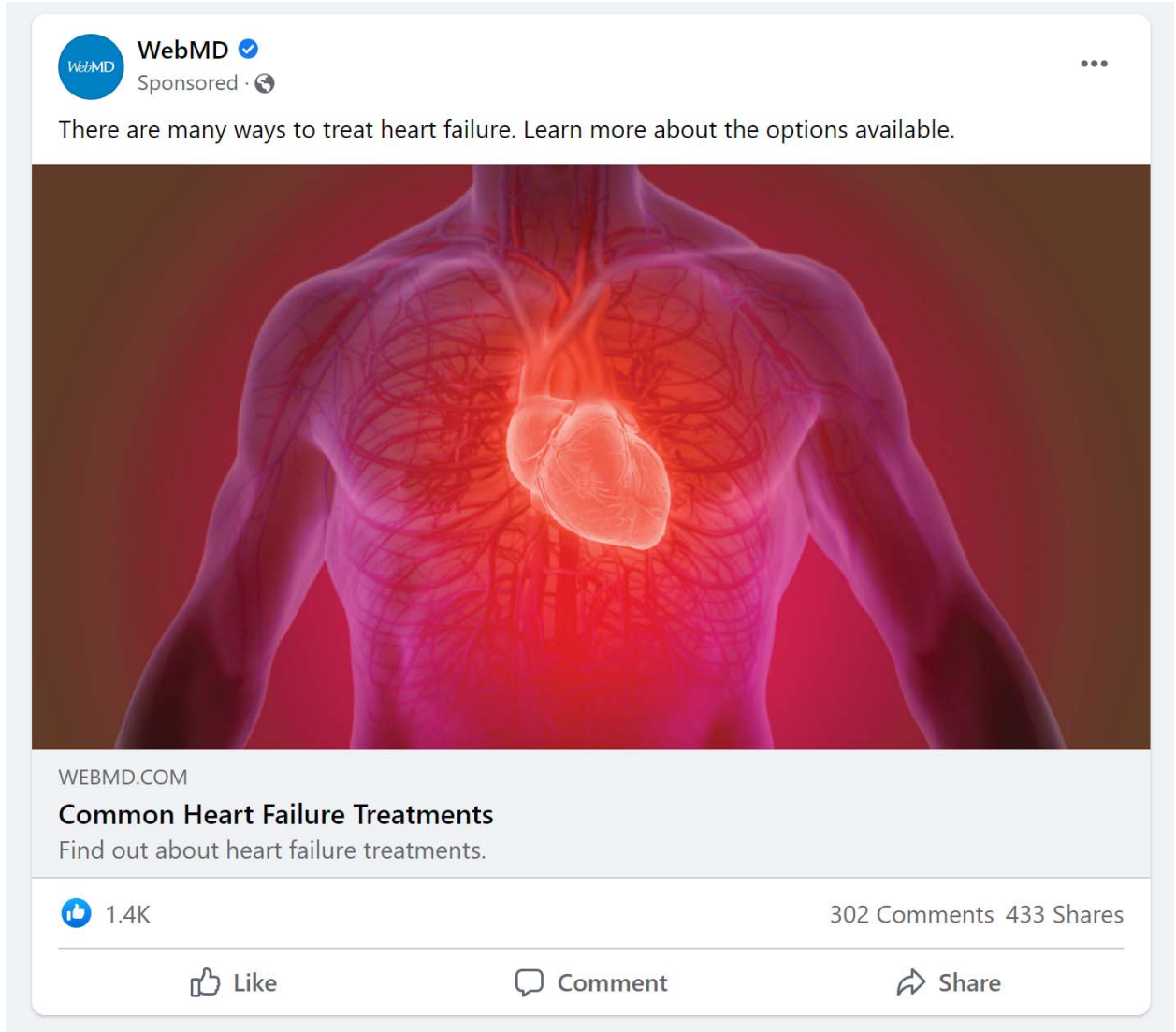
25 ///

26 ///

27 ///

28 ///

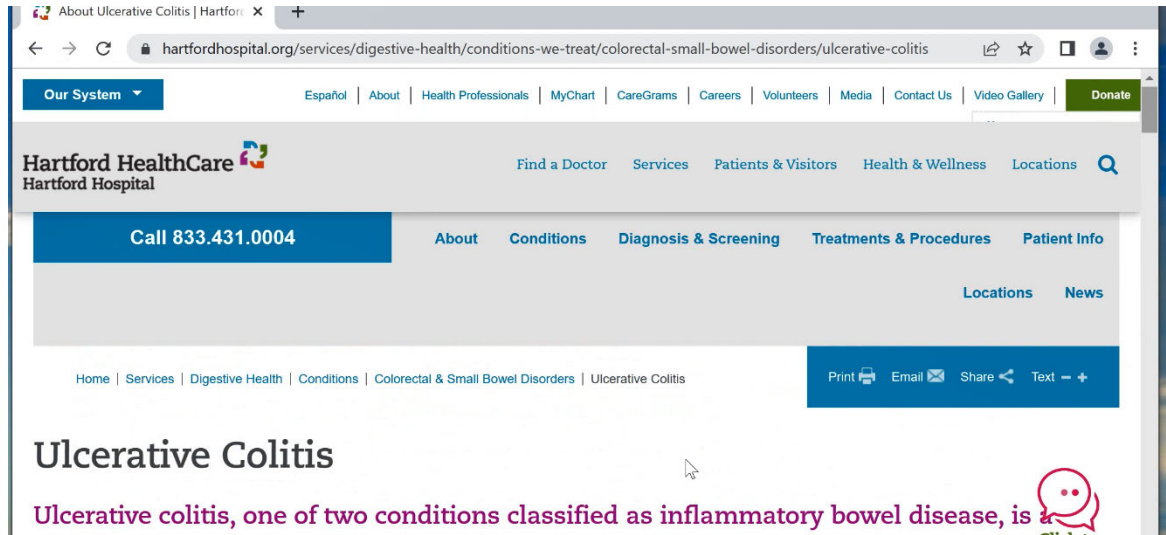
KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California



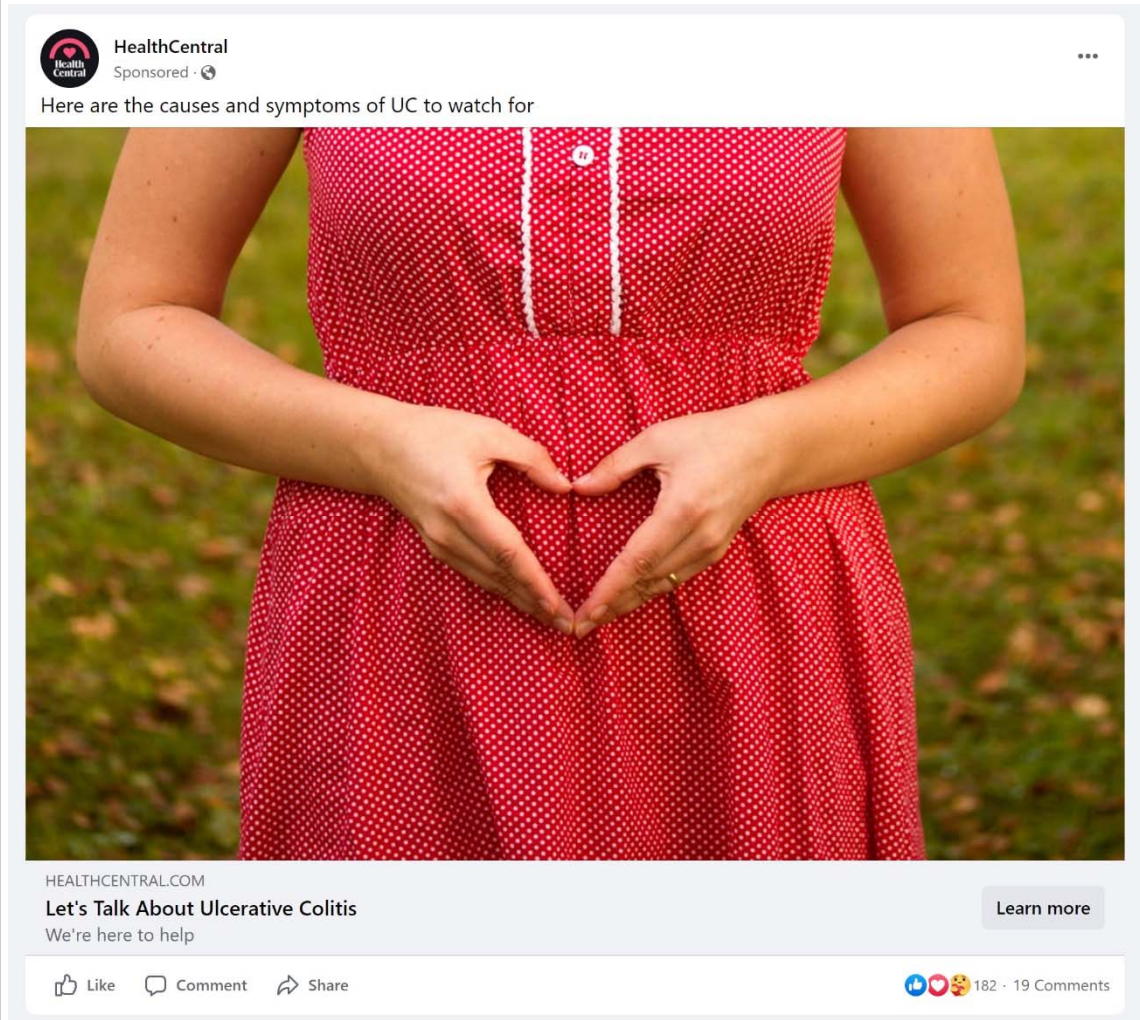
189. While visiting the Hartford HealthCare web site, I searched for information on ulcerative colitis and visited this Web page on the condition:



KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California



190. Within two hours of visiting this Web page on ulcerative colitis, I was shown the following advertisement related to ulcerative colitis in my Facebook video feed:



191. Meta provides basic information about how ads get targeted to users. For example:

**PADCEV® (enfortumab vedotin-ejfv)**  
Sponsored · ⚙️

Please see full Prescribing Information/Patient Information for more information.

**What is the most important information I should know about PADCEV?**

**PADCEV may cause serious side effects, including skin reactions.** Severe skin reactions have happened with PADCEV; in some cases severe skin reactions have caused death. Most severe skin reactions occurred during the first cycle (28 days) of treatment but may happen later. Your healthcare provider will monitor you during treatment and may stop treatment if you get skin reactions. Tell your healthcare provider right away if you develop any of these signs of a skin reaction:

- target lesions (skin reactions that look like rings)
- rash or itching that continues to get worse
- blistering or peeling of the skin
- painful sores in the mouth or nose or genital area
- fever or flu-like symptoms
- swollen lymph nodes

See “What are the possible side effects of PADCEV?” for more information about side effects.

**WHAT IS PADCEV®?**

PADCEV is a prescription medicine used to treat adults with bladder cancer and cancers of the urinary tract (renal pelvis, ureter or urethra) that has spread or cannot be removed by surgery. PADCEV may be used if you:

- have received an immunotherapy medicine **and** chemotherapy that contains platinum, **or**
- you are not able to receive a chemotherapy that contains the medicine cisplatin and you have received one or more prior therapies.

It is not known if PADCEV is safe and effective in children.

⌵ Hide ad  
Never see this ad again.

⚠️ Report ad  
Tell us about a problem with this ad.

📌 Save video  
Add this to your saved items.

🔗 Copy link

🔔 Turn on notifications for this post



ℹ️ Why am I seeing this ad?

⏸ 0:32 / 2:30

## Why you're seeing this ad

🔒 Only you can see this



PADCEV® (enfortumab vedotin-ejfv) wants to reach people like you, who may have:

-  Set their age to 55 and older >
-  A primary location in the United States >

### What else influences your ads

Your personalized ads may be based on other advertiser choices, your profile and activities—like websites you visit and ads you interact with—as well as other information not listed here. [Learn more about how ads work](#)

### What you can do

-  **Hide all ads from this advertiser** Hide  
You won't see PADCEV® (enfortumab vedotin-ejfv) 's ads
-  **Make changes to your ad preferences** >  
Adjust settings to personalize your ads

Was this explanation useful?

Yes

No

Source: <https://www.facebook.com>

To show you more relevant ads, we receive and use data that advertisers and other partners provide to us about your activity on their websites and apps, as well as some of your offline interactions, such as purchases. For example, we may show you an ad for a shirt based on your visit to a clothing website.

Source: [https://www.facebook.com/help/568137493302217/?helpref=related\\_articles](https://www.facebook.com/help/568137493302217/?helpref=related_articles)

**Hospital Web sites who have recently removed the Meta Pixel**

192. On July 29, 2022, the plaintiffs submitted to Meta a “PLAINTIFFS’ REQUESTS FOR PRODUCTION TO DEFENDANT META PLATFORMS, INC., SET ONE”. Exhibit A of this request listed 664 hospital Web sites which the plaintiffs believe employ the Facebook/Meta Pixel.

193. In the course of my testing for this declaration, I found in mid-August 2022 that the Meta Pixel had been removed from a number of Hospital Web sites listed in Appendix A.

194. For example, in the first 20 Web sites which are listed in Appendix A, the following five sites appear to no longer use the Meta Pixel on August 18, 2022:

- a. alaskaregional.com
- b. arnothealth.org
- c. ascension.org
- d. aultman.org
- e. barnesjewish.org

195. The Fiddler capture file First-20-2022-08-18.saz, contains the results of visiting each of the first 20 Web sites of the Appendix A on August 18, 2022 with the Windows Chrome Browser.

196. In addition, I found that Meta/Facebook Pixel was removed from the Wellstar Web site ([www.wellstar.org](http://www.wellstar.org)), which appears in Appendix A, somewhere between June 9, 2022 and July 5, 2022 based on saved versions of the Wellstar home page held by the archive.org Web site:

```
<!-- Facebook Pixel Code -->
<script>
!function(f,b,e,v,n,t,s)
{if(f.fbq)return;n=f.fbq=function(){n.callMethod?
n.callMethod.apply(n,arguments):n.queue.push(arguments)};
if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
n.queue=[];t=b.createElement(e);t.async=!0;
t.src=v;s=b.getElementsByTagName(e)[0];
s.parentNode.insertBefore(t,s)}(window, document,'script',
'https://web.archive.org/web/20220609182504/https://connect.facebook.net/en_US/fbevents.js')
;
fbq('init', '1617536358466149');
fbq('track', 'PageView');
</script>
```



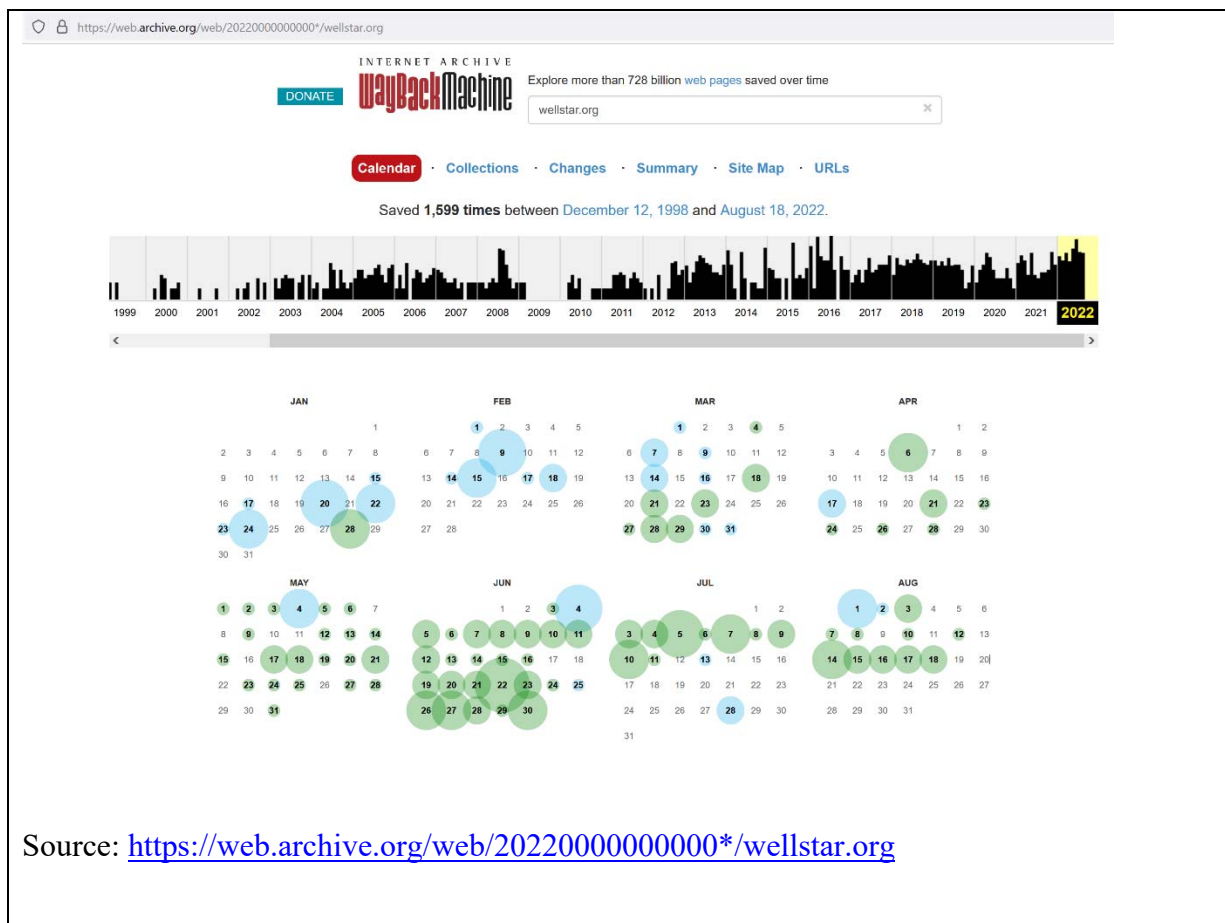
<noscript><img height="1" width="1" style="display:none"  
 src=[https://web.archive.org/web/20220609182504im\\_/https://www.facebook.com/tr?id=1617536358466149&ev=PageView&noscript=1/](https://web.archive.org/web/20220609182504im_/https://www.facebook.com/tr?id=1617536358466149&ev=PageView&noscript=1/)></noscript>  
 <!-- End Facebook Pixel Code -->

Source: HTML source of  
<https://web.archive.org/web/20220609182504/https://www.wellstar.org/>

No Facebook Pixel Code

Source: HTML source of  
<https://web.archive.org/web/20220705181803/https://www.wellstar.org/>

197. The following screen shot from archive.org shows saved versions of Web pages at the Wellstar Web site in 2022:



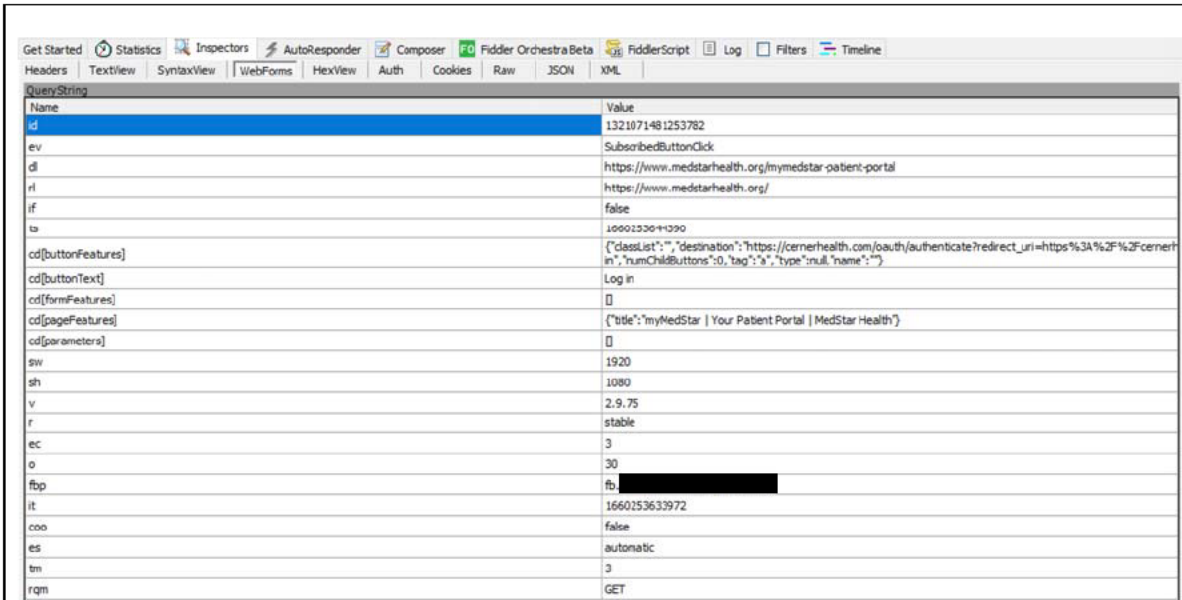
198. My understanding is that the complaint against Meta was filed on June 17, 2022.

## Summary

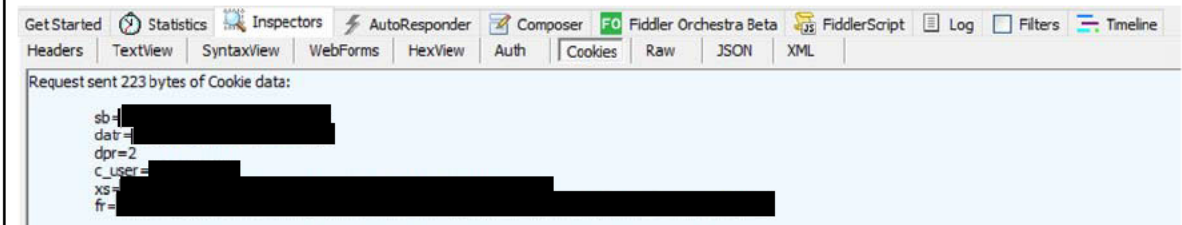
199. Meta acquires patient Protected Health Information (PHI) through the use of the Meta Pixel on the websites of HIPAA-covered entities, including but not limited to:

- a. MedStar Health – medstarhealth.org
- b. Rush University System for Health - rush.edu
- c. Hartford HealthCare - hartfordhospital.org
- d. Summa Health System - www.summahealth.org
- e. University Hospitals - www.uhhospitals.org

200. Meta acquires the patient status of individuals logging into the “patient portals” of their providers through click data, including the Meta Pixel “SubscribedButtonClick” as illustrated by the following HTTP GET request parameters for a Meta Pixel used on the MedStar Health patient portal home page:



Name	Value
id	1321071481253782
ev	SubscribedButtonClick
dl	https://www.medstarhealth.org/mymedstar-patient-portal
rl	https://www.medstarhealth.org/
if	false
ts	10001230911090
cd[buttonFeatures]	{"classList": [], "destination": "https://cernerhealth.com/oauth/authenticate?redirect_uri=https%3A%2F%2Fcernerin%2F", "numChildButtons": 0, "tag": "a", "type": "null", "name": ""}
cd[buttonText]	Log in
cd[formFeatures]	{}
cd[pageFeatures]	{"title": "myMedStar   Your Patient Portal   MedStar Health"}
cd[parameters]	{}
sw	1920
sh	1080
v	2.9.75
f	stable
ec	3
o	30
fb	fb [REDACTED]
it	1660253633972
coo	false
es	automatic
tm	3
rqn	GET

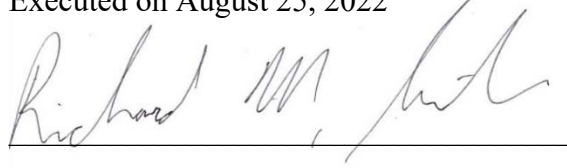


Cookie Name	Value
sb	[REDACTED]
datr	[REDACTED]
dpr	2
c_user	[REDACTED]
xs	[REDACTED]
fr	[REDACTED]



1           201. The patient PHI that Meta acquires through the Meta Pixel is used for marketing  
2 purposes, including targeted advertising.

3 Executed on August 25, 2022

4   
5

6 Richard M. Smith  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

KIESEL LAW LLP  
Attorneys at Law  
Beverly Hills, California