

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

7 Jason 'Jay' Barnes (to be admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
8 An Truong (to be admitted *pro hac vice*)
atruong@simmonsfirm.com
9 Eric Johnson (to be admitted *pro hac vice*)
ejohnson@simmonsfirm.com
10 **SIMMONS HANLY CONROY LLC**
11 112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: (212) 784-6400
12 Fax: (212) 213-5949

Stephen M. Gorny [to be 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 [to be admitted *Pro Hac Vice*]
agunn@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

13
14 *Attorneys for Plaintiffs*
15

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

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

20 Plaintiffs,

21 v.

22 META PLATFORMS, INC.,

23 Defendant.
24
25
26
27
28

Case No. 3:22-cv-3580

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

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

I. INTRODUCTION..... 1

II. JURISDICTION AND VENUE..... 4

III. PARTIES TO THE LITIGATION..... 5

IV. FACTS COMMON TO ALL COUNTS..... 5

 A. HEALTH PRIVACY LAWS IN THE UNITED STATES 5

 B. FACEBOOK’S CONTRACTUAL PROMISES 8

 C. HOW THE PIXEL WORKS..... 10

 D. FACEBOOK PUBLICLY ACKNOWLEDGES THAT HEALTH-BASED
ADVERTISING IS INAPPROPRIATE 16

 E. FACEBOOK CHANGED ITS CONTRACTUAL PRIVACY PROMISES IN
2018..... 17

V. CLASS ACTION ALLEGATIONS..... 18

VI. TOLLING..... 19

VII. CAUSES OF ACTION 20

 FIRST CAUSE OF ACTION - BREACH OF CONTRACT 20

 SECOND CAUSE OF ACTION - GOOD FAITH AND FAIR DEALING 22

 THIRD CAUSE OF ACTION - INTRUSION UPON SECLUSION—
CONSTITUTIONAL INVASION OF PRIVACY 23

 FOURTH CAUSE OF ACTION - VIOLATION OF THE ELECTRONIC
COMMUNICATIONS PRIVACY ACT 25

 FIFTH CAUSE OF ACTION - THE CALIFORNIA INVASION OF PRIVACY ACT ... 27

 SIXTH CAUSE OF ACTION - NEGLIGENT MISREPRESENTATION..... 28

 SEVENTH CAUSE OF ACTION - VIOLATION OF CALIFORNIA’S UNFAIR
COMPETITION LAW 29

VIII. PRAYER FOR RELIEF 31

IX. DEMAND FOR JURY TRIAL..... 33

1 Plaintiff John Doe, on behalf of himself and all others similarly situated, alleges as follows
2 upon personal knowledge as to his own conduct and on information and belief as to all other matters
3 based on an investigation by counsel, such that each allegation has evidentiary support or is likely
4 to have evidentiary support upon further investigation and discovery:

5 **I. INTRODUCTION**

6 1. Plaintiffs bring this action on behalf of themselves and millions of other Americans
7 whose medical privacy has been violated by Facebook’s Pixel tracking tool. As explained herein,
8 Facebook knows (or should have known) that its Pixel tracking tool is being improperly used on
9 hospital websites resulting in the wrongful, contemporaneous, re-direction to Facebook of patient
10 communications to register as a patient, sign-in or out of a supposedly “secure” patient portal,
11 request or set appointments, or call their provider via their computing device. This unlawful
12 collection of data is done without the knowledge or authorization of the patient, like Plaintiffs, in
13 violation of federal and state laws as well as Facebook’s own contract with its users.

14 2. When a patient communicates with a health care provider’s website where the
15 Facebook Pixel is present on the patient portal login page, the Facebook Pixel source code causes
16 the exact content of the patient’s communication with their health care provider to be re-directed
17 to Facebook in a fashion that identifies them as a patient.

18 3. For example, Plaintiff John Doe is a patient of the Medstar Health System in
19 Baltimore, Maryland. In the course of receiving medical care at MedStar, Plaintiff Doe has used
20 the “MyMedStar” patient portal to review his lab results, make appointments, and communicate
21 with his providers.

22 4. Unbeknownst to Plaintiff John Doe, and millions of other patients around the
23 country, when he signed-in to the patient portal, the Facebook Pixel secretly deployed on the
24 webpage sent the fact that he has clicked to sign-in to the patient portal to Facebook.

25 5. The data that the Facebook Pixel causes to be re-directed from the patient’s
26 computing device to Facebook includes:

- 27 a. The patient was communicating with Medstar via its
28 www.MedStarHealth.org property;

- b. The patient engaged in an ‘ev’ or event called a SubscribedButtonClick;
- c. The content of the button the patient clicked was “Login to myMedstar”
- d. The page from which the button the patient clicked was Patient Portal – *i.e.* Home;
- e. The patient had previously been at a Medstar page about breast health;
- f. The patient’s Internet Protocol address;
- g. Identifiers that Facebook uses to identify the patient and his/her device, including cookies named c-user, datr, fr, and fbp (*i.e.* Facebook Pixel); and
- h. Browser attribute information sufficient to fingerprint the patient’s 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=to myMedstar", "numChildButtons":0, "tag":"a", "name":""}
cd[buttonText]	Login to myMedstar
cd[formFeature]	[]
cd[pageFeature]	{'title':"Patient Portal - Home"}
cd[parameters]	[]
coo	false
dl	https://www.mymedstar.org/?ReturnUrl=%2Fdefault.aspx&opt_id=[REDACTED]&ga=[REDACTED]
ec	2
es	automatic
ev	SubscribedButtonClick
fbp	fb.1.1 [REDACTED] 23
id	[REDACTED]
if	false
it	[REDACTED]
o	30
r	stable
rl	https://www.medstarhealth.org/mhs/our-services/womens-health/conditions/breast-health/breast-conditions/
rqm	GET
sh	1080
sw	1920

6. As explained in further detail below, patient-status is protected by HIPAA, which requires a valid HIPAA-compliant authorization before it is collected by Facebook.

7. Neither Facebook nor any of the hospitals that deployed the Facebook Pixel on their web properties (“Facebook Partner Medical Providers”) procured HIPAA authorizations for the disclosure of patient status and health information to Facebook.

8. Facebook’s collection of patient status and the content of patient communications with their medical providers, including when they register, log-in and logout of patient portals and

1 to set up appointments, in the absence of a HIPAA authorization violates Facebook’s privacy
2 promises to users.

3 9. Facebook promises users, that “publishers can send us information through Meta
4 Business Tools [such as] the Meta Pixel” but Facebook “require[s] each of these partners to have
5 lawful rights to collect, use, and share your data before providing any data to us.”

6 10. However, Facebook knowingly receives patient data—including patient portal
7 usage information— from hundreds medical providers in the United States that have deployed the
8 Facebook Pixel on their web properties.

9 11. To date, through experts, Plaintiffs have identified at least 664 hospital systems or
10 medical provider web properties where Facebook has received patient data via the Facebook Pixel.

11 12. Despite knowingly receiving health-related information from medical providers,
12 Facebook has not taken any action to enforce or validate its requirement that medical providers
13 obtain adequate consent from patients before providing patient data to Facebook.

14 13. Facebook monetizes the information it receives through the Facebook Pixel
15 deployed on medical providers’ web properties by using it to generate highly-profitable targeted
16 advertising on- and off-Facebook.

17 14. The targeted advertising Facebook offers for sale includes the ability to target
18 patients based on specific actions that a patient has taken on the medical providers’ websites.

19 15. Facebook also offers the ability to engage in remarketing based on positive targeting
20 – that is, serving specific ad campaigns to patients based on the specific actions those patients took
21 on the medical providers’ website. For example, Facebook could target ads to a patient who had
22 (1) used the patient portal and (2) viewed a page about a specific condition, such as cancer.

23 16. Facebook also offers medical providers the ability to engage in remarketing based
24 on negative targeting – that is, ensuring that ads are not shown to users who have taken specific
25 action. This could mean that Facebook would exclude existing patients from a medical provider’s
26 advertising campaign in order to establish new patients.

27 17. Facebook employs thousands of account managers or representatives to help
28 partners, including medical providers, use the Facebook Pixel and other tools.

1 18. Through its account managers and representatives, Facebook is aware that it is
2 receiving patient data from hundreds of different medical providers in the United States without
3 patient knowledge, consent, or valid HIPAA authorizations.

4 19. Facebook also utilizes “The Facebook Crawler” that scans pages of partner apps and
5 websites and through which Facebook gathers information about the app or website, including its
6 title and description.

7 20. Through the Facebook Crawler, Facebook is aware that it is receiving patient data.

8 21. Facebook has also been served subpoenas in other actions regarding disclosure of
9 patient information through the Facebook Pixel.

10 22. Facebook is also aware of every web property where the Facebook Pixel is deployed
11 and fully capable of conducting the same types of expert analysis that Plaintiffs conducted to
12 identify at least 664 hospitals or medical provider properties where the Facebook Pixel is present.

13 23. Facebook’s actions described herein give rise to causes of action for: (1) breach of
14 contract; (2) breach of the duty of good faith and fair dealing; (3) intrusion upon seclusion /
15 violation of Article I, section 1 of the California Constitution; (4) federal and state electronic
16 communications privacy and wiretap claims; (5) the California Invasion of Privacy Act, Cal. Penal
17 Code §§ 631 and 632; (6) Negligent Misrepresentation; and (7) Violation of California’s Unfair
18 Competition Law.

19 **II. JURISDICTION AND VENUE**

20 24. This Court has personal jurisdiction over the Defendant because it has sufficient
21 minimum contacts with this District in that it operates and markets their services throughout the
22 country and in this District. Additionally, Defendant is headquartered in this District.

23 25. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331 because this
24 action arises under 18 U.S.C. §2510, et. seq., (the Electronic Communications Privacy Act). This
25 Court further has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) (the Class Action
26 Fairness Act) because the amount in controversy exceeds \$5,000,000, exclusive of interest and
27 costs, and a member of the Class is a citizen of a State different from any Defendant.

28 ///

1 26. This Court has supplemental jurisdiction over the remaining state law claims
2 pursuant to 28 U.S.C. §1367 because the state law claims form part of the same case or controversy
3 under Article III of the United States Constitution.

4 27. Venue is proper in this district because a substantial part of the events or omissions
5 giving rise to the claim occurred in this judicial district and because Facebook’s Terms of Use
6 governing its relationship with its users and developers adopt California law and choose California
7 as the venue for disputes.

8 **III. PARTIES TO THE LITIGATION**

9 28. Plaintiff John Doe is a Maryland resident, Facebook user, and a patient of MedStar
10 Health, Inc. (“MedStar”) who used MedStar’s myMedStar patient portal, currently located at
11 <https://www.medstarhealth.org/mymedstar-patient-portal>, to view medical records, lab results, and
12 otherwise communicate with his provider. Plaintiff’s use of the myMedStar patient portal included
13 the time during which the Facebook Pixel was secretly deployed on the portal login page.

14 29. Defendant Meta Platforms, Inc. (referred to herein by its previous name of
15 “Facebook”) is a publicly traded Delaware corporation headquartered in Menlo Park, California,
16 and does business throughout the United States and the world, deriving substantial revenue from
17 interstate commerce.

18 **IV. FACTS COMMON TO ALL COUNTS**

19 **A. HEALTH PRIVACY LAWS IN THE UNITED STATES**

20 30. Patient health care information in the United States is protected by federal law under
21 the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing
22 regulations promulgated by the United States Department of Health and Human Services (“HHS”).

23 31. The HIPAA Privacy Rule establishes “national standards to protect individuals’
24 medical records and other individually identifiable health information (collectively defined as
25 “protected health information”) and applies to health plans, health care clearinghouses, and those
26 health care providers that conduct certain health care transactions electronically. The Rule requires
27 appropriate safeguards to protect the privacy of protected health information and sets limits and
28 conditions on the uses and disclosures that may be made of such information without an

1 individual's authorization. The Rule also gives individuals rights over their protected health
2 information, including rights to examine and obtain a copy of their health records, to direct a
3 covered entity to transmit to a third party an electronic copy of their protected health information
4 in an electronic health record, and to request corrections. The Privacy Rule is located at 45 CFR
5 Part 160 and Subparts A and E of Part 164." [https://www.hhs.gov/hipaa/for-](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html)
6 [professionals/privacy/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html)

7 32. Under 45 C.F.R. § 164.502, a health care provider or business associate of a health
8 care provider "may not use or disclose 'protected health information' except as permitted or
9 required by" the HIPAA Privacy Rule.

10 33. Under 45 C.F.R. 160.103, the Privacy Rule defines "protected health information"
11 or PHI as "individually identifiable health information" that is "transmitted by electronic media;
12 maintained in electronic media; or transmitted or maintained in any other form or medium."

13 34. Under 45 C.F.R. § 160.103, the Privacy Rule defines "individually identifiable
14 health information" as "a subset of health information, including demographic information
15 collected from an individual" that is (1) "created or received by a health care provider;" (2)
16 "[r]elates to the past, present, or future physical or mental health or condition of an individual; the
17 provision of health care to an individual; or the past, present, or future payment for the provision
18 of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to
19 which there is a reasonable basis to believe the information can be used to identify the individual."

20 35. Under 45 C.F.R. § 164.514, the HIPAA de-identification rule states that "health
21 information is not individually identifiable only if" (1) an expert "determines that the risk is very
22 small that the information could be used, alone or in combination with other reasonably available
23 information, by an anticipated recipient to identify an individual who is a subject of the
24 information" and "documents the methods and results of the analysis that justify such
25 determination" or (2) "the following identifiers of the individual or of relatives, employers, or
26 household members of the individual are removed: Names ... Medical record numbers; ... Account
27 numbers ... Device identifiers and serial numbers; ... Web Universal Resource Locators (URLs);
28 Internet Protocol (IP) address numbers; ... and any other unique identifying number, characteristic,

1 or code.” In addition, the covered entity must not “have actual knowledge that the information
2 could be used alone or in combination with other information to identify an individual who is a
3 subject of the information.”

4 36. Under 42 U.S.C. § 1320d-6, any “person [individual ... or a corporation] who
5 knowingly and in violation of this part—(1) uses or causes to be used a unique health identifiers;
6 [or] (2) obtains individually identifiable health information relating to an individual ... shall be
7 punished” by fine or, in certain circumstances, imprisonment, with increased penalties for “intent
8 to sell, transfer, or use individually identifiable health information for commercial advantage[.]”
9 The statute further provides that a “person ... shall be considered to have obtained or disclosed
10 individually identifiable health information ... if the information is maintained by a covered entity
11 ... and the individual obtained or disclosed such information without authorization.”

12 37. Patient status alone is protected by HIPAA.

13 38. Guidance from HHS instructs health care providers that patient status is protected
14 by HIPAA. In Guidance Regarding Methods for De-identification of Protected Health Information
15 in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, HHS
16 sets out:

17 Identifying information alone, such as personal names, residential addresses,
18 or phone numbers, would not necessarily be designated as PHI. For instance,
19 if such information was reported as part of a publicly accessible data source,
20 such as a phone book, then this information would not be PHI because it is
21 not related to health data. ... *If such information was listed with health
22 condition, health care provision or payment data, such as an indication that
23 the individual was treated at a certain clinic, then this information would be
24 PHI.*¹

25 39. In its guidance for Marketing, HHS further instructs:

26 The HIPAA Privacy Rule gives individuals important controls over whether
27 and how their protected health information is used and disclosed for
28 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

¹ https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf at 5 (emphasis added).

1 *authorization from each person on the list.*²

2 40. HHS has previously instructed that HIPAA covers patient-status alone:

3 a. “The sale of a patient list to a marketing firm” is not permitted under HIPAA.

4 65 Fed. Reg. 82717 (Dec. 28, 2000);

5 b. “A covered entity must have the individual’s prior written authorization to
6 use or disclose protected health information for marketing communications,”

7 which would include disclosure of mere patient status through a patient list.

8 67 Fed. Reg. 53186 (Aug. 14, 2002);

9 c. It would be a HIPAA violation “if a covered entity impermissibly disclosed
10 a list of patient names, addresses, and hospital identification numbers.” 78

11 Fed. Reg. 5642 (Jan. 25, 2013); and

12 d. The only exception permitting a hospital to identify patient status without
13 express written authorization is to “maintain a directory of individuals in its

14 facility” that includes name, location, general condition, and religious
15 affiliation when used or disclosed to “members of the clergy” or “other

16 persons who ask for the individual by name.” 45 C.F.R. § 164.510(1). Even
17 then, patients must be provided an opportunity to object to the disclosure of

18 the fact that they are a patient. 45 C.F.R. § 164.510(2).

19 41. There is no HIPAA-exception for the Internet or online patient portals.

20 **B. FACEBOOK’S CONTRACTUAL PROMISES**

21 42. Every Facebook user is legally deemed to have agreed to the Terms, Data Policy,

22 and Cookie Policy via a checkbox on the sign-up page; and the Terms, Data Policy, and Cookie
23 Policy are binding upon Facebook and its users.

24 ///

25 ///

26
27 _____
28 ²<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/marketing.pdf> at 1-2 (emphasis added).

1 43. The Facebook Data Policy expressly provides that Facebook “requires” businesses
2 that use the Facebook Pixel “to have lawful rights to collect, use, and share your data before
3 providing any data to [Facebook].”

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](#).

19
20 44. But Facebook does not “require” medical providers to have lawful rights to share
21 patient data associated with their respective patient portals and appointment software before
22 sending it to Facebook.

23 45. Instead, Facebook merely includes a provision in its form contract which creates an
24 unenforced “honor system” for publishers, stating that, by using the Facebook Business Tools, the
25 publisher “represent[s] and warrant[s] that [it has] provided robust and sufficient prominent notice
26 to users regarding the Business Tool Data collection, sharing, and usage.”

27 ///

28 ///

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

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](#).)

46. In reality, Facebook does not actually verify publishers have obtained adequate consent per the contract.³

47. Instead, the Facebook Pixel is blindly made available to any willing publisher regardless of their privacy policies, consent processes, or the nature of their business.

48. Facebook's contract with medical providers for use of the Facebook Pixel does not mention HIPAA at all.

49. Facebook does not take any action to discourage medical providers from using the Facebook Pixel.

50. Facebook actively encourages medical providers to use the Facebook Pixel for their marketing campaigns.

C. HOW THE PIXEL WORKS

51. Facebook operates the world's largest social media company.

52. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers including IP addresses, cookies, and device identifiers.

³ In contrast, Facebook requires publishers in the European Union to provide "all necessary consents" in a "verifiable manner."

1 53. Facebook also tracks non-users across the web through its widespread Internet
2 marketing products and source code.

3 54. Facebook’s revenue is derived almost entirely from selling targeted advertising to
4 Facebook users on Facebook.com and to all Internet users on non-Facebook sites that integrate
5 Facebook marketing source code on their websites.

6 55. Facebook Business is the division that provides advertising services to developers.
7 Facebook Business and the advertising tools it provides to developers are focused on trade and
8 commerce.

9 56. The Facebook Pixel, a product for Facebook Business, is a “piece of code” that lets
10 developers “measure, optimize and build audiences for ... ad campaigns.”⁴

11 57. The Facebook Pixel is an invisible 1x1 web bug that Facebook makes available to
12 web-developers to help track ad-driven activity from Facebook and others on their website.

13 58. Key features of the Facebook Pixel include its ability to help developers:

- 14 a. “Measure cross-device conversions” and “understand how your cross-device
15 ads help influence conversion”;
- 16 b. “Optimize delivery to people likely to take action” and “ensure your ads are
17 shown to the people most likely to take action”; and
- 18 c. “Create custom audience from website visitors” and create “dynamic ads [to]
19 help you automatically show website visitors the products they viewed on
20 your website – or related ones.”

21 59. Facebook describes the Facebook Pixel as “a snippet of Javascript code” that “relies
22 on Facebook cookies, which enable [Facebook] to match ... website visitors to their respective
23 Facebook User accounts.”

24 ///

25 ///

26 ///

27

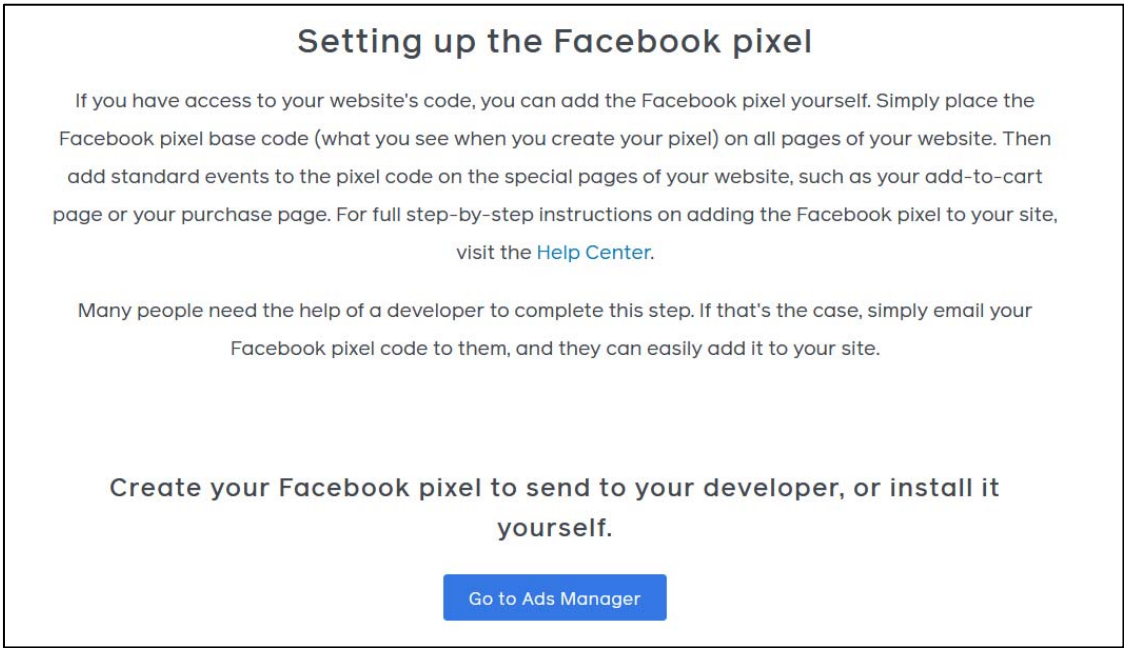
28

⁴ <https://www.facebook.com/business/learn/facebook-ads-pixel>

1 60. Facebook further explains “How the Facebook Pixel Works”⁵



7 61. Facebook provides simple instructions for developers to set up the Facebook Pixel:



19 62. Facebook creates the Facebook code for each developer who installs it.

20 ///
21 ///
22 ///
23 ///
24 ///
25 ///
26 ///

28 ⁵ <https://www.facebook.com/business/learn/facebook-ads-pixel>

1 63. Facebook recommends that the Pixel code be placed early in the source code for any
2 given webpage or website to ensure that the user will be tracked:

<p>3 Installing The Pixel</p> <p>4</p> <p>5 To install the pixel, we highly recommend that you add its base code between the opening and closing <code><head></code> 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.</p> <p>6</p> <p>7 Placing the code within your <code><head></code> 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.</p> <p>8</p>

9

10 64. By executing the code sooner, Facebook has designed the Pixel such that Facebook
11 receives the information about patient actions on the medical provider's properties
12 contemporaneous with their making.

13 65. As soon as a patient take any action on a webpage which includes the Facebook
14 Pixel—such as clicking a button to register, login, or logout of a patient portal or to create an
15 appointment—Facebook's source code commands the patient's computing device to re-direct the
16 content of the patient's communication to Facebook while the exchange of the communication
17 between the patient and the medical provider is still occurring.

18 66. By design, Facebook receives the content of a patient's patient portal sign-in
19 communication immediately *after* the patient clicks the log-in button and *before* the medical
20 provider receives it.

21 67. In *all* cases, the content of the patient's portal and appointment communications are
22 re-directed to Facebook while the communications are still occurring.

23 68. The cookies that Facebook identifies patients with include, but are not necessarily
24 limited to, cookies named: `c_user`, `datr`, `fr`, and `_fbp`.

25 69. The `c_user` cookie is a means of identification for Facebook users. The `c_user` cookie
26 value is the Facebook equivalent of a user identification number. Each Facebook user account has
27 one – and only one – unique `c_user` cookie. Facebook uses the `c_user` cookie to record user activities
28 and communications.

1 70. A skilled computer user can obtain the `c_user` cookie value for any Facebook user
2 by (1) going to the user’s Facebook page, (2) right-clicking on their mouse, (3) selecting ‘View page
3 source,’ (4) executing a control-F function for “fb://profile,” and (5) copying the number value that
4 appears after “fb://profile” in the page source code of the target Facebook user’s page.

5 71. It is even easier to find the Facebook account associated with a `c_user` cookie: one
6 simply needs to log-in to Facebook, and then type `www.facebook.com/#`, with # representing the
7 `c_user` cookie identifier. For example, the `c_user` cookie value for Mark Zuckerberg is 4. Logging
8 in to Facebook and typing `www.facebook.com/4` in the web browser retrieves Mark Zuckerberg’s
9 Facebook page: `www.facebook.com/zuck`.

10 72. The Facebook `datr` cookie identifies the patient’s specific web browser from which
11 the patient is sending the communication. It is an identifier that is unique to the patient’s specific
12 web browser and is therefore a means of identification for Facebook users.

13 73. Facebook keeps a record of every `datr` cookie identifier associated with each of its
14 users, and a Facebook user can obtain a redacted list of all `datr` cookies associated with his or her
15 Facebook account from Facebook.

16 74. Any Facebook user can view the specific `datr` cookie identifiers that Facebook has
17 associated with their account by using the Facebook Download Your Information tool.

18 75. The Facebook `fr` cookie is an encrypted combination of the `c_user` and `datr` cookies.⁶


19 76. The Facebook `_fbp` cookie is a Facebook identifier that is set by Facebook source
20 code and associated with Defendant’s use of the Facebook Pixel. The `_fbp` cookie is a Facebook
21 cookie that masquerades as a first-party cookie to evade third party cookie blockers and share data
22 more directly between a medical provider and Facebook.

23 77. The medical provider or its developer then simply copy-paste the Facebook Pixel
24 code that Facebook creates and providers into the medical provider’s web-property.

25 ///

26 _____
27 ⁶ See Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian
28 Privacy Commission, Mar. 27, 2015, available at
https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

1 78. Facebook expressly admits that the Pixel “log[s] when someone takes an action” such
2 as “adding an item to their shopping cart or making a purchase.”



3
4
5
6
7
8
9

10 Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website.
11 Examples of actions include adding an item to their shopping cart or making a purchase. The Meta
12 Pixel receives these actions, or events, which you can view on your Meta Pixel page in [Events](#)
13 [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.

- 14 79. For medical providers, the actions that the Facebook Pixel logs include:
- 15 a. When a patient clicks to register for the patient portal;
 - 16 b. When a patient clicks to log-in to the patient portal;
 - 17 c. When a patient clicks to logout of the patient portal;
 - 18 d. When a patient sets up an appointment;
 - 19 e. When a patient clicks a button to call the provider; and
 - 20 f. The specific communications a patient exchanges at the provider’s property,
21 including those relating to specific providers, conditions, and treatments and
22 the timing of such actions, including whether they are made while a patient
23 is still logged-in to a patient portal or around the same time that the patient
24 has scheduled an appointment, called the medical provider, or logged in or
25 out of the patient portal.

26 ///
27 ///
28 ///

1 **D. FACEBOOK PUBLICLY ACKNOWLEDGES THAT HEALTH-BASED**
2 **ADVERTISING IS INAPPROPRIATE**

3 80. Facebook has publicly acknowledged that targeted advertising based on health
4 information is not appropriate.

5 81. On November 9, 2021, Facebook announced that it was removing the ability to target
6 users on “topics people may perceive as sensitive, such as options referencing causes, organizations,
7 or public figures that relate to health[.]”⁷

8 82. Facebook’s announcement was a public relations success:

9 a. Reuters published a story headlined “Facebook plans to remove thousands of
10 sensitive ad-targeting options” and lead the story with a sentence about
11 Facebook’s “plans to remove detailed ad-targeting options that refer to
12 ‘sensitive’ topics, such as ads based on interactions with content around ...
13 health[.]”⁸

14 b. The New York Times published a similar story with a similar headline, “Meta
15 plans to remove thousands of sensitive ad-targeting categories: Ad buyers
16 will no long be able to use topics such as health ... to target people[.]”⁹

17 c. Many more, similar, articles were published, giving Facebook’s users the
18 misimpression that Facebook would not allow targeting based on health

19 83. But Facebook did not change the most insidious types of targeting based on health:
20 those marketing campaigns from medical providers that disclose patient identities and their
21 individually identifiable health information to Facebook for the purpose of targeted marketing based
22 on their communications with their medical providers.

23 ///

24
25 ⁷ <https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls>

26 ⁸ <https://www.reuters.com/technology/facebook-removes-target-options-advertisers-some-topics-2021-11-09/>

27 ⁹ <https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html>

1 84. Facebook clarified that the change was limited to “people’s interactions with
2 content” on the Facebook “platform.”

3 85. Facebook then informed advertisers that they could still use “website custom
4 audiences and lookalike” to “help reach people who have already engaged with a business or group’s
5 website or products.” In the case of medical providers, the “people who have already engaged” are
6 patients.

7 **E. FACEBOOK CHANGED ITS CONTRACTUAL PRIVACY PROMISES IN**
8 **2018**

9 86. Prior to April 2018, Facebook’s contract did not “require” partners to have the
10 lawful rights to share user data before doing so.

11 87. Upon information and belief, Facebook changed its contract with users on or about
12 April 19, 2018, which added a clause stating: “We require each of these partners to have lawful
13 rights to collect, use and share your data before providing any data to us.”

14 88. The following is a side-by-side comparison of the pre- and post-April 2018 contract
15 provisions:

Before April 19, 2018	After April 19, 2018
<p>Information from websites and apps that use our Services. We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.</p> <p>Information from third-party partners. We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.</p>	<p>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.</p> <p>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.</p> <p>To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.</p>

26 ///

27 ///

1 **V. CLASS ACTION ALLEGATIONS**

2 89. Plaintiffs file this as a class action on behalf of themselves and the following class:

3 All Facebook users who are current or former patients of medical providers in the
4 United States with web properties through which Facebook acquired patient
5 communications relating to medical provider patient portals, appointments, phone
6 calls, and communications associated with patient portal users, for which neither
7 the medical provider nor Facebook obtained a HIPAA, or any other valid, consent.

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

11 91. The members of the Class are so numerous that joinder is impracticable.

12 92. Common questions of law and fact are apt to drive resolution of the case, exist as to
13 all members of the Class and predominate over any questions affecting solely individual members
14 of the Class including, but not limited to, the following:

- 15 a. Whether the Facebook Pixel is designed to send individually identifiable
16 information to Facebook;
- 17 b. Whether the Facebook Terms and Privacy Notice are valid contracts;
- 18 c. Whether Facebook failed to require medical providers to have lawful rights
19 to share patient data with Facebook before deploying the Facebook Pixel;
- 20 d. Whether Facebook acquired the content of patient communications;
- 21 e. Whether the patient class provided Facebook with authorization to acquire
22 their communications with their medical providers, including through the
23 patient portal, appointment forms, and phone calls;
- 24 f. Whether the Facebook Pixel's presence and use on medical provider
25 websites where it discloses actions that patients take relating to patient
26 portals, appointments, and phone calls to their medical providers is highly
27 offensive;
- 28 g. Whether Facebook's acquisition of the content of communications between
patients and their medical providers occurred contemporaneous to their
making;

- 1 h. Whether Facebook breached its contract with users;
- 2 i. Whether the information at issue has economic value; and
- 3 j. Whether Facebook unjustly profited from its collection of patient portal,
- 4 appointment, and phone call information.

5 93. The named Plaintiff’s claims are typical of the claims of other Class members, as
 6 all members of the Class were similarly affected by Facebook’s wrongful conduct in violation of
 7 federal and California law, as complained of herein.

8 94. The named Plaintiff will fairly and adequately protect the interests of the members
 9 of the Class and has retained counsel that is competent and experienced in class action litigation.
 10 The named Plaintiff has no interests that conflict with, or are otherwise antagonistic to, the interests
 11 of, other Class members.

12 95. A class action is superior to all other available methods for the fair and efficient
 13 adjudication of this controversy since joinder of all members is impracticable. Further, as the
 14 damages that individual Class members have suffered may be relatively small, the expense and
 15 burden of individual litigation make it impossible for members of the Class to individually redress
 16 the wrongs done to them. There will be no difficulty in management of this action as a class action.

17 **VI. TOLLING**

18 96. Any applicable statute of limitations has been tolled by Defendant’s knowing and
 19 active concealment of the misrepresentations and omissions alleged herein. Through no fault or
 20 lack of diligence, Plaintiff and members of the Class were deceived and could not reasonably
 21 discover Defendant’s deception and unlawful conduct.

22 97. Plaintiff and members of the Class did not discover and did not know of any facts
 23 that would have caused a reasonable person to suspect that Defendant was acting unlawfully and
 24 in the manner alleged herein. As alleged herein, the representations made by Facebook were
 25 material to Plaintiff and members of the Class at all relevant times. Within the time period of any
 26 applicable statutes of limitations, Plaintiff and members of the Class could not have discovered
 27 through the exercise of reasonable diligence the alleged wrongful conduct.

28 ///

1 98. At all times, Defendant is and was under a continuous duty to disclose to Plaintiff
2 and members of the Class the true nature of the disclosures being made and the lack of an actual
3 “requirement” before the data was shared with it.

4 99. Defendant knowingly, actively, affirmatively and/or negligently concealed the facts
5 alleged herein. Plaintiff and members of the Class reasonably relied on Defendant’s concealment.

6 100. For these reasons, all applicable statutes of limitation have been tolled based on the
7 discovery rule and Defendant’s concealment, and Defendant is estopped from relying on any
8 statutes of limitations in defense of this action.

9 **VII. CAUSES OF ACTION**

10 **FIRST CAUSE OF ACTION**

11 **BREACH OF CONTRACT**

12 101. Plaintiffs hereby incorporate all prior paragraphs as if fully stated herein.

13 102. Facebook requires users to click a box indicating that, “By clicking Sign Up, you
14 agree to our Terms, Data Policy and Cookies Policy.”

15 103. “Click-wrap agreements” such as those at issue herein are valid and binding
16 contracts.

17 104. The Facebook Terms are binding on Facebook and its users.

18 105. The Facebook Data Policy is binding on Facebook and its users.

19 106. The Facebook Cookies Policy is binding on Facebook and its users.

20 107. The Facebook Data Policy promises users that Facebook “requires each of
21 [Facebook’s] partners to have lawful rights to collect, use and share your data before providing any
22 data to [Facebook].”

23 108. Facebook breached this contractual promise, as described in detail above, by not
24 requiring its partners that are medical providers to obtain patient consent before sharing patient
25 status and other data relating to online patient portal registration, logins, and logouts as well as
26 appointment information with Facebook through the Facebook Pixel and through other means.

27 109. In addition to the express contract provision set forth above, an implied contract
28 existed between Facebook and its users that Facebook would not conspire with others to violate

1 Plaintiffs' legal rights to privacy in their individually identifiable health information.

2 110. Plaintiffs are Facebook account holders who used patient portals and/or
3 appointment-related functionality of their medical providers' respective web-properties through
4 which Facebook obtained their individually identifiable health information.

5 111. Plaintiff Doe used the MyMedStar patient portal by signing in and out of the portal
6 to access medical records, lab results, and otherwise to communicate with his provider.

7 112. The patient health information that Facebook obtained in breach of the contract
8 included:

- 9 a. Patient identifiers including, but not limited to, email addresses, IP
10 addresses, persistent cookie identifiers, device identifiers, and browser
11 fingerprint information;
- 12 b. the data and time of patient registrations for their medical providers' patient
13 portals;
- 14 c. log-in and logout times for their medical providers' patient portals;
- 15 d. the contents of communications that patients exchange inside their medical
16 providers' patient portals immediately before logging out of those portals;
- 17 e. the contents of communications relating to appointments that patients made
18 with their medical providers; and
- 19 f. the user's status as a patient of their medical provider.

20 113. Facebook's breach caused Plaintiff and Class members the following damages:

- 21 a. Nominal damages for breach of contract;
- 22 b. General damages for invasion of their privacy rights in an amount to be
23 determined by a jury without reference to specific pecuniary harm;
- 24 c. Sensitive and confidential information including patient status and
25 appointments that Plaintiff and Class members intended to remain private
26 are no longer private;
- 27 d. Facebook eroded the essential confidential nature of the patient-provider
28 relationship;

- 1 e. Facebook took something of value from Plaintiff and Class members and
2 derived benefits therefrom without Plaintiff's and Class members'
3 knowledge or informed consent and without sharing the benefit of such
4 value;
- 5 f. Benefit of the bargain damages in that Facebook's contract stated that
6 payment for the service would consist of a more limited set of collection of
7 personal information than that which Facebook actually charged.

8 **SECOND CAUSE OF ACTION**

9 **GOOD FAITH AND FAIR DEALING**

10 114. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

11 115. A valid contract exists between Plaintiffs and Facebook.

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

13 117. Facebook prevented Plaintiff and Class members from receiving the full benefit of
14 the contract by intercepting the content of protected individually identifiable health information
15 exchanged with medical providers.

16 118. By doing so, Facebook abused its power to define terms of the contract, specifically
17 the meaning of the term "require" in Facebook's promise that it would "require" partners to have
18 lawful rights to share users' data with Facebook before doing so and then taking no action (and
19 actually encouraging) medical providers to share protected health information without valid patient
20 authorization.

21 119. By doing so, Facebook did not act fairly and in good faith.

22 120. Facebook's breach caused Plaintiff and Class members the following damages:

- 23 a. Nominal damages for breach of contract;
- 24 b. General damages for invasion of their privacy rights in an amount to be
25 determined by a jury without reference to specific pecuniary harm;
- 26 c. Sensitive and confidential information including patient status and
27 appointments that Plaintiff and Class members intended to remain private
28 are no longer private;

- 1 d. Facebook eroded the essential confidential nature of the patient-provider
- 2 relationship;
- 3 e. Facebook took something of value from Plaintiff and Class members and
- 4 derived benefits therefrom without Plaintiff’s and Class members’
- 5 knowledge or informed consent and without sharing the benefit of such
- 6 value; and
- 7 f. Benefit of the bargain damages in that Facebook’s contract stated that
- 8 payment for the service would consist of a more limited set of collection of
- 9 personal information than that which Facebook actually charged.

THIRD CAUSE OF ACTION

INTRUSION UPON SECLUSION—CONSTITUTIONAL INVASION OF PRIVACY

- 12 121. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.
- 13 122. 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.

17 Cal. Const. art. I, § 1 (emphasis added).

18 123. Plaintiffs had no knowledge and did not consent or authorize Facebook to obtain the
19 content of their communications with their medical providers as described herein.

20 124. Plaintiffs enjoyed objectively reasonable expectations of privacy surrounding
21 communications with their medical providers relating to the respective patient portals and
22 appointments based on:

- 23 a. The medical providers status as their health care providers and the
- 24 reasonable expectations of privacy that attach to such relationships;
- 25 b. HIPAA;
- 26 c. the Electronic Communications Privacy Act; and
- 27 d. Facebook’s promise that it would “require” partners to have lawful
- 28 permission to share their data before Facebook would collect it.

- 1 125. Plaintiffs' claims are based on the following private facts:
- 2 a. that Plaintiffs are patients of the various medical providers;
- 3 b. The specific dates and times Plaintiffs clicked to log-in or log-out of the
- 4 various medical providers' patient portals;
- 5 c. The specific and detailed communications exchanged while logged-in to a
- 6 patient portal; and
- 7 d. The specific dates and times where Plaintiffs requested appointments and
- 8 from which doctor's or practice group pages such appointments were
- 9 requested.

10 126. Facebook's conduct was intentional and intruded on Plaintiff's and Class members'

11 medical communications which constitute private conversations, matters, and data.

12 127. Facebook's conduct in acquiring patient portal and appointment communications

13 would be highly offensive to a reasonable person because:

- 14 a. Facebook conspired with Plaintiffs' medical providers to violate a cardinal
- 15 rule of the provider-patient relationship;
- 16 b. Facebook's conduct violated federal law designed to protect patient privacy;
- 17 c. Facebook's conduct violated the ECPA; and
- 18 d. Facebook's conduct violated the express promises it made to users.

19 128. Facebook's breach caused Plaintiff and Class members the following damages:

20 a. Nominal damages for breach of contract;

21 b. General damages for invasion of their privacy rights in an amount to be

22 determined by a jury without reference to specific pecuniary harm;

23 c. Sensitive and confidential information including patient status and

24 appointments that Plaintiff and Class members intended to remain private

25 are no longer private;

26 d. Facebook eroded the essential confidential nature of the patient-provider

27 relationship;

28 ///

- 1 e. Facebook took something of value from Plaintiff and Class members and
- 2 derived benefits therefrom without Plaintiff’s and Class members’
- 3 knowledge or informed consent and without sharing the benefit of such
- 4 value; and
- 5 f. Benefit of the bargain damages in that Facebook’s contract stated that
- 6 payment for the service would consist of a more limited set of collection of
- 7 personal information than that which Facebook actually charged.

FOURTH CAUSE OF ACTION

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

- 10 129. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.
- 11 130. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional
- 12 interception of the contents of any electronic communication. 18 U.S.C. § 2511.
- 13 131. The ECPA protects both the sending and receipt of communications.
- 14 132. 18 U.S.C. § 2520(a) provides a private right of action to any person whose electronic
- 15 communications are intercepted.
- 16 133. Facebook intentionally intercepted the electronic communications that Plaintiffs
- 17 exchanged with their respective medical providers on the providers properties where the Facebook
- 18 Pixel was present.
- 19 134. The transmissions of data between Plaintiffs and their medical providers qualify as
- 20 communications under the ECPA’s definition in 18 U.S.C. § 2510(12).
- 21 135. Facebook acquired patient communications with their medical providers as alleged
- 22 herein contemporaneous with their making.
- 23 136. The intercepted communications include:
- 24 a. the content of patient registrations for various patient portals, including
- 25 clicks on buttons to “Register” or “Signup” for said portals;
- 26 b. the content patient log-in and logout of the various patient portals, including
- 27 clicks to “Sign-in,” “Log-in,” “Sign-out,” or “Log-out.”

28 ///

1 c. the contents of communications that patients exchange inside various patient
2 portals immediately before logging out of those portals; and

3 d. the contents of communications relating to appointments with medical
4 providers.

5 137. The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

6 a. The cookies Facebook used to track patients’ communications;

7 b. The patients’ browsers;

8 c. The patients’ computing devices;

9 d. Facebook’s web-servers;

10 e. The web-servers of the properties of the medical providers where the
11 Facebook Pixel was present; and

12 f. The Facebook Pixel source code deployed by Facebook to effectuate its
13 acquisition of patient communications.

14 138. Facebook is not a party to patient communications with their medical providers.

15 139. Facebook received the content of patient communications through the surreptitious
16 redirection of them from the patients’ computing devices to Facebook.

17 140. Patients did not consent to Facebook’s acquisition of their patient portal,
18 appointment, and phone call communications with their medical providers.

19 141. Facebook did not obtain legal authorization to obtain patient communications with
20 their medical providers relating to patient portals, appointments, and phone calls.

21 142. Facebook did not require any medical provider to obtain the lawful rights to share
22 the content of patient communications relating to patient portals, appointments, and phone calls.

23 143. Any purported consent that Facebook received from medical providers to obtain
24 patient communications content was not valid.

25 144. In acquiring the content of patient communications relating to patient portals,
26 appointments, and phone calls, Facebook had a purpose that was tortious, criminal, and designed
27 to violate state constitution provisions including:

28 ///

- 1 a. A knowing intrusion into a private, place, conversation, or matter that would
- 2 be highly offensive to a reasonable person;
- 3 b. A violation of 42 U.S.C. § 1320d-6, which is a criminal offense punishable
- 4 by fine or imprisonment;
- 5 c. Violation of state unfair business practice statutes;
- 6 d. Violation of HIPAA; and
- 7 e. Violation of Article I, section 1 of the California Constitution.

8 145. Facebook knew that such conduct would be highly offensive, as evidence by its
 9 announcement in DATE, that it would no longer allow advertising targeted based on health, yet
 10 continued to use the Facebook Pixel on medical provider properties for that purpose.

11 **FIFTH CAUSE OF ACTION**

12 **THE CALIFORNIA INVASION OF PRIVACY ACT**

13 **(Cal. Penal Code §§ 631 and 632)**

14 146. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

15 147. The California Invasion of Privacy Act (CIPA) is codified at Cal. Penal Code §§
 16 630-638. The Act begins with its statement of purpose: “The legislature hereby declares that
 17 advances in science and technology have led to the development of new devices and techniques for
 18 the purpose of eavesdropping upon private communications and that the invasion of privacy
 19 resulting from the continual and increasing use of such devices and techniques has created a serious
 20 threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized
 21 society.” Cal. Penal Code § 630.

22 148. Cal. Penal Code § 631(a) provides, in pertinent part: “Any person who, by means of
 23 any machine, instrument, or contrivance, or in any other manner willfully and without the
 24 consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to
 25 read, or to learn the contents or meaning of any message, report, or communication while the same
 26 is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place
 27 within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to
 28 communicate in any way, any information so obtained, or who aids, agrees with, employs, or

1 conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts
2 or things mentioned above in this section, is punishable by a fine not exceeding two thousand five
3 hundred dollars.”

4 149. Cal. Penal Code § 632 provides, in pertinent part, that it is unlawful for any person
5 to “intentionally and without the consent of all parties to a confidential communication,” to “use[]
6 [a] recording device to ... record the confidential communication.” As used in the statute, a
7 “confidential communication” is “any communication carried on in circumstances as may
8 reasonably indicate that any part to the communication desired it to be confined to the parties
9 thereto[.]”

10 150. Facebook is a “person” within the meaning of CIPA §§ 631 and 632.

11 151. Facebook did not have the consent of all parties to learn the contents of or record
12 the confidential communications at issue.

13 152. Facebook is headquartered in California, designed and contrived and effectuated its
14 scheme to track patient communication at issue here from California, and has adopted California
15 substantive law to govern its relationship with users.

16 153. At all relevant times, Facebook’s conduct alleged herein was without the
17 authorization and consent of the Plaintiff and Class members.

18 154. Facebook’s actions were designed to learn or attempt to learn the meaning of the
19 patient portal and appointment communications patients exchanged with their medical providers.

20 155. Facebook’s learning of or attempt to learn the contents of patient communications
21 occurred while they were in transit or in the process of being sent or received.

22 **SIXTH CAUSE OF ACTION**

23 **NEGLIGENT MISREPRESENTATION**

24 156. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

25 157. Facebook represented to Plaintiff and the members of the Class that a fact was true,
26 namely, that before receiving the confidential information at issue, Facebook “requires” business
27 “to have lawful rights to collect, use, and share [Plaintiffs’ and Class members’] data before
28 providing any data” to Facebook.

1 158. Facebook’s representation was not true.

2 159. Although Facebook may have honestly believed that the representation was true,
3 Facebook had no reasonable grounds for believing the representation was true when it was made.

4 160. Facebook intended that Plaintiff and the members of the Class rely on the
5 representation.

6 161. Plaintiff and the members of the Class reasonably relied on Facebook’s
7 representation.

8 162. Plaintiff and the Class were harmed as set forth above.

9 163. Plaintiff and Class members’ reliance on Facebook’s representation was a
10 substantial factor in causing the harm.

11 **SEVENTH CAUSE OF ACTION**

12 **VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW**

13 **(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)**

14 164. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

15 165. California Business and Professions Code section 17200 (“UCL”) prohibits any
16 “unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading
17 advertising”

18 166. Facebook has engaged in unlawful, fraudulent, and unfair business acts and
19 practices in violation of the UCL.

20 167. Defendant has engaged in unlawful acts or practices under section 17200 by its
21 violations of the California Constitution’s right to privacy, ECPA and California Penal Code
22 sections 631 and 632, through the acts and practices set forth in this Complaint.

23 168. Defendant has engaged in fraudulent business acts or practices under section 17200
24 because its misrepresentations and omissions regarding its requirement that businesses have lawful
25 rights to collect, use, and share Plaintiff’s and Class members’ data before providing any data to
26 Defendant, and Defendant’s receipt of the confidential information at issue, were intended to, were
27 likely to, and did deceive reasonable consumers such as Plaintiff and the Class. The information
28 Defendant misrepresented and concealed would be, and is, material to reasonable consumers

1 because Defendant does not require businesses to have lawful rights to collect, use, and share
2 Plaintiff's and Class members' data before providing any data to Defendant and Defendant receives
3 the confidential information at issue nonetheless.

4 169. Defendant has engaged in unfair acts and practices under section 17200 based on
5 the acts and practices alleged herein, namely, that Defendant claims that it requires businesses to
6 "have lawful rights to collect, use, and share [Plaintiff's and Class members'] data before providing
7 any data" to Defendant, but in reality knows (or should have known) that its Pixel tracking tool is
8 being improperly used on hospital websites resulting in the wrongful, contemporaneous, re-
9 direction to Facebook of patient communications without the knowledge or authorization of
10 Plaintiffs.

11 170. Defendant's actions offend public policy.

12 171. Defendant's conduct, misrepresentations and omissions have also impaired
13 competition within the health care market in that those actions have prevented Plaintiff and the
14 Class from making fully informed decisions about whether to communicate online with their
15 healthcare providers and to use their healthcare providers' website in the first instance.

16 172. Plaintiff and the Class have suffered an injury in fact, including the loss of money
17 and/or property, as a result of Defendant's unfair, unlawful and/or deceptive practices, to wit, the
18 disclosure of their personally identifiable data which has value as is demonstrated by the use and
19 sale of it by Defendant. While only an identifiable "trifle" of injury is needed to be shown, as set
20 forth above Plaintiffs, patients, and the public at large value their private health information at more
21 than a trifle. And, sale of this confidential and valuable information to has now diminished the
22 value of such information to Plaintiff and the Class.

23 173. Defendant's actions caused damage to and loss of Plaintiff's and other patients'
24 property right to control the dissemination and use of their personally identifiable patient data and
25 communications.

26 174. Defendant's actions caused damage to and loss of Plaintiff's and other patients'
27 property rights to control the dissemination and use of the personally identifiable communications.

28 175. Defendant's representation that it requires businesses to "have lawful rights to

1 collect, use, and share [Plaintiff’s and Class members’] data before providing any data” to
2 Defendant was untrue. Again, had Plaintiff and Class members known these facts, they would not
3 have used their health care provider’s website.

4 176. The wrongful conduct alleged herein occurred, and continues to occur, in the
5 conduct of Defendant’s business. Defendant’s wrongful conduct is part of a pattern or generalized
6 course of conduct that is still perpetuated and repeated, in the State of California.

7 177. Plaintiff and the Class request that this Court enjoin Defendant from continuing its
8 unfair, unlawful, and/or deceptive practices and to restore to Plaintiff and the Class, in the form of
9 restitution, any money Defendant acquired through its unfair competition.

10 **VIII. PRAYER FOR RELIEF**

11 WHEREFORE, Plaintiffs respectfully request that this Court:

12 1. Certify the proposed Class, designating Plaintiff John Doe as the named
13 representative of the Class, and designating the undersigned as Class Counsel;

14 2. Award compensatory damages, including statutory damages where available, to
15 Plaintiff and the Class against Defendant for all damages sustained as a result of Defendant’s
16 wrongdoing, in an amount to be proven at trial, including interest thereon;

17 3. Award punitive damages on the causes of action that allow for them and in an amount
18 that will deter Defendant and others from like conduct;

19 4. Award attorneys’ fees and costs, as allowed by law including, but not limited to,
20 California Code of Civil Procedure section 1021.5;

21 5. Award pre-judgment and post-judgment interest, as provided by law; and,

22 6. For such other, further, and different relief as the Court deems proper under the
23 circumstances.

24 DATED: June 17, 2022

KIESEL LAW LLP

26 By: /s/ Jeffrey A. Koncius
27 Paul R. Kiesel
28 Jeffrey A. Koncius
Nicole Ramirez

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

SIMMONS HANLY CONROY LLC
Jason ‘Jay’ Barnes (to be admitted *pro hac vice*)
An Truong (to be admitted *pro hac vice*)
Eric Johnson (to be admitted *pro hac vice*)

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

THE SIMON LAW FIRM, P.C.
Amy Gunn (to be admitted *pro hac vice*)

Attorneys for Plaintiffs

1 **IX. DEMAND FOR JURY TRIAL**

2 Plaintiff, on behalf of himself and the Class, demands a trial by jury of any and all issues in
3 this action so triable of right.

4 DATED: June 17, 2022

KIESEL LAW LLP

6 By: /s/ Jeffrey A. Koncius
7 Paul R. Kiesel
8 Jeffrey A. Koncius
9 Nicole Ramirez

10 **SIMMONS HANLY CONROY LLC**
11 Jason ‘Jay’ Barnes (to be admitted *pro hac vice*)
12 An Truong (to be admitted *pro hac vice*)
13 Eric Johnson (to be admitted *pro hac vice*)

14 **GORNY DANDURAND, LC**
15 Stephen M. Gorny (to be admitted *pro hac vice*)

16 **THE SIMON LAW FIRM, P.C.**
17 Amy Gunn (to be admitted *pro hac vice*)

18 Attorneys for Plaintiffs
19
20
21
22
23
24
25
26
27
28