MICHAEL F. RAM (SBN 104805)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@ForThePeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN J. MCGEE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com

Attorneys for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

JANE DOE, on behalf of herself and all others similarly situated,

Plaintiff,

v.

META PLATFORMS, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

CLASS ACTION FOR
(1) BREACH OF CONTRACT;
(2) GOOD FAITH & FAIR DEALING;
(3) INTRUSION UPON SECLUSION;
(4) VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT;
(5) VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT;
(6) NEGLIGENT MISREPRESENTATION;
(7) VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

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

INTRODUCTION

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

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

3. For example, Plaintiff Jane Doe is a patient of Novant Health headquartered in Winston-Salem, North Carolina ("Novant"). In the course of receiving medical care at Novant, Plaintiff Doe has used the patient portal to schedule appointments, access lab results, and review health information.

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

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

a. The patient was communicating with Novant;

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

c. The content of the button the patient clicked was a login prompt

d. The patient's Internet Protocol address;

e. 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

f. Browser attribute information sufficient to fingerprint the patient's device.

6. Likewise, Novant disclosed identical fields of information when Plaintiff Jane Doe used the patient portal.

7. 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.

8. 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.

9. 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 to set up appointments, in the absence of a HIPAA authorization violates Facebook's privacy promises to users.

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

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

12. To date, through public filings in related cases, there have been at least 664 hospital systems or medical provider web properties identified where Facebook has received patient data via the Facebook Pixel.

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

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

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

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

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

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

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

20. Facebook also utilizes "The Facebook Crawler" that scans pages of partner apps and websites and through which Facebook gathers information about the app or website, including its title and description.

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

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

23. Facebook is also aware of every web property where the Facebook Pixel is deployed and fully capable of conducting the same types of expert analysis reflected in other complaints to identify at least 664 hospitals or medical provider properties where the Facebook Pixel is present.

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

JURISDICTION AND VENUE

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

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

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

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

PARTIES TO THE LITIGATION

29. Plaintiff Jane Doe is a North Carolina resident, Facebook user, and a patient of Novant who used Novant's patient portal to schedule appointments, access lab results, and review health information, among other things. Plaintiff's use of the Novant patient portal included the time during which the Facebook Pixel was secretly deployed on the portal login page.

30. On or about August 12, 2022, Jane Doe received a letter from Novant informing her

that in May 2020, a tracking pixel was placed on Novant's website to assist with advertising efforts during the COVID pandemic. Following an investigation, Novant determined that the Facebook Pixel was capable of collecting sensitive information and/or PHI, including: demographic information such as email address, phone number, computer IP address, and contact information entered into forms; and information such as appointment type and data, physician selected, button/menu selections, and/or content typed into free text boxes. Novant disabled and removed that Facebook Pixel from its website.

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

FACTS COMMON TO ALL COUNTS

A. HEALTH PRIVACY LAWS IN THE UNITED STATES

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

33. The HIPAA Privacy Rule establishes "national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires 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 such information without an individual's authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections. The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164."

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

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

36. Under 45 C.F.R. § 160.103, the Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (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) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

37. Under 45 C.F.R. § 164.514, the HIPAA de-identification rule states that "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: Names … Medical record numbers; … Account numbers … Device identifiers and serial numbers; … Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; … and any other unique identifying number, characteristic, or code." In addition, 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."

38. Under 42 U.S.C. § 1320d-6, any "person [individual … or a corporation] who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifiers; [or] (2) obtains individually identifiable health information relating to an individual … shall be

punished" by fine or, in certain circumstances, imprisonment, with increased penalties for "intent to sell, transfer, or use individually identifiable health information for commercial advantage[.]" The statute further provides 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."

39. Patient status alone is protected by HIPAA.

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

> 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.[1]

41. In its guidance for Marketing, HHS further instructs:

> 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*.[2]

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

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

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

[2]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf at 1-2 (emphasis added).

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which would include 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

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).

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

B. FACEBOOK'S CONTRACTUAL PROMISES

44. Every Facebook user is legally deemed to have agreed to the Terms, Data Policy, and Cookie Policy via a checkbox on the sign-up page; and the Terms, Data Policy, and Cookie Policy are binding upon Facebook and its users.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

45. The Facebook Data Policy expressly provides that Facebook "requires" businesses that use the Facebook Pixel "to have lawful rights to collect, use, and share your data before 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.

46. But Facebook does not "require" medical providers to have lawful rights to share patient data associated with their respective patient portals and appointment software before sending it to Facebook.

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

> 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.)

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

49. 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.

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

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

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

C. HOW THE PIXEL WORKS

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

54. 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."

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

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

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

58. The Facebook Pixel, a product for Facebook Business, is a "piece of code" that lets developers "measure, optimize and build audiences for . . . ad campaigns."[4]

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

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

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

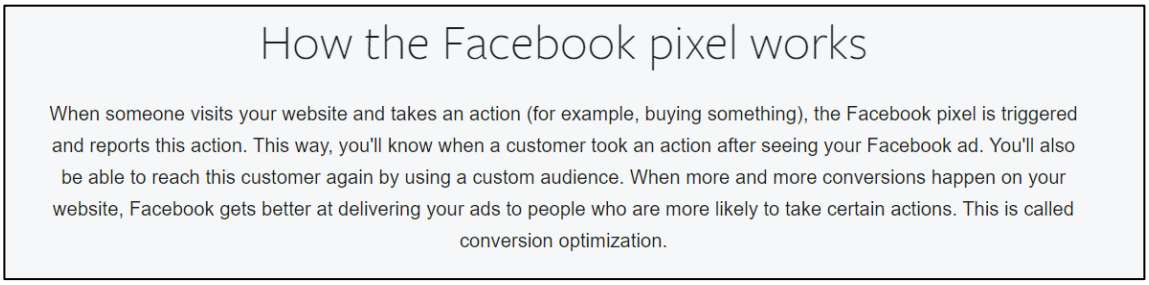
b. "Optimize delivery to people likely to take action" and "ensure your ads are shown to the people most likely to take action"; and

c. "Create custom audience from website visitors" and create "dynamic ads [to] help you automatically show website visitors the products they viewed on your website – or related ones."

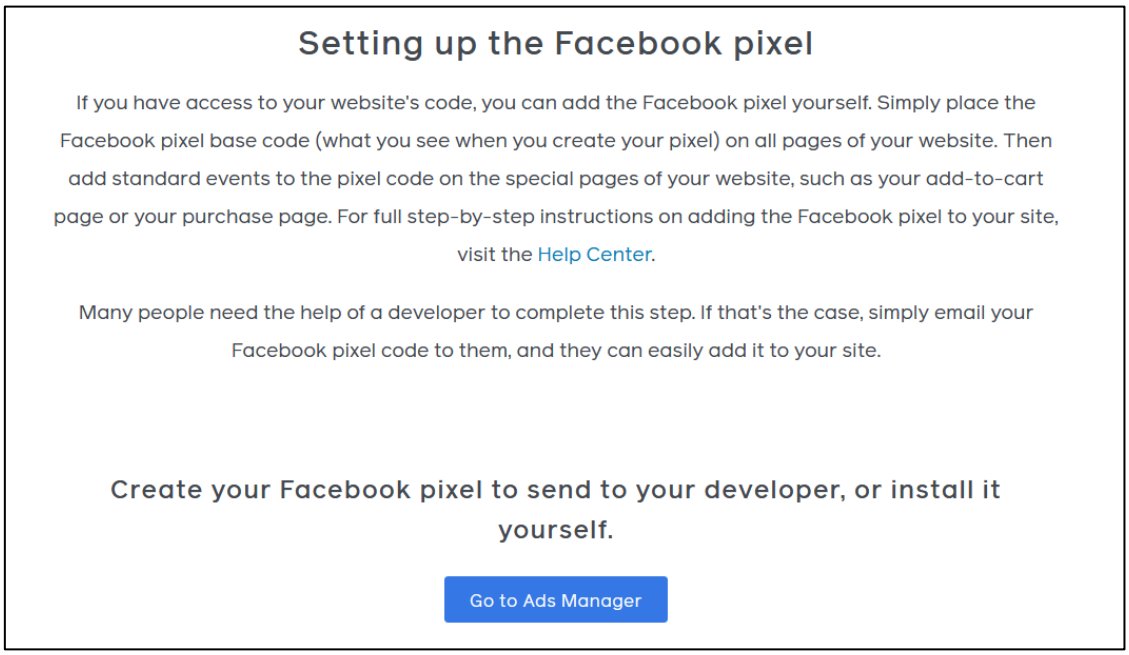
61. Facebook describes the Facebook Pixel as "a snippet of Javascript code" that "relies on Facebook cookies, which enable [Facebook] to match … website visitors to their respective Facebook User accounts."

62. Facebook further explains "How the Facebook Pixel Works"[5]

[4] https://www.facebook.com/business/learn/facebook-ads-pixel
[5] https://www.facebook.com/business/learn/facebook-ads-pixel

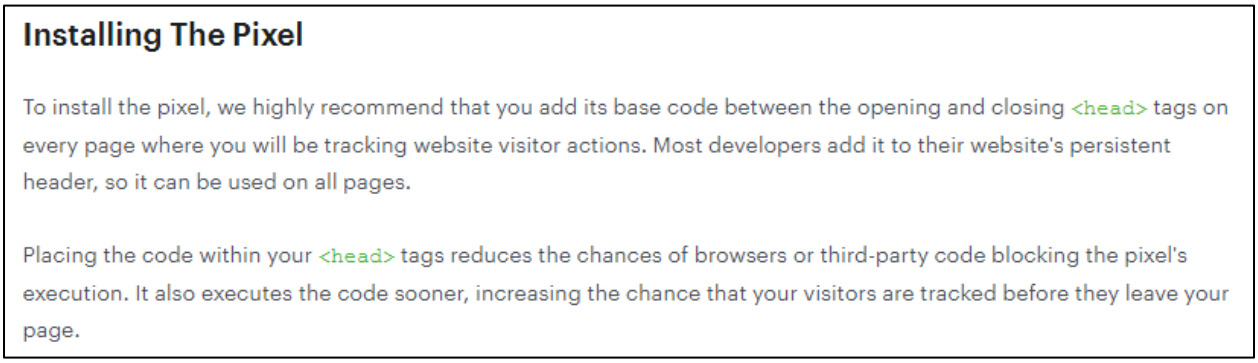


63. Facebook provides simple instructions for developers to set up the Facebook Pixel:



64. Facebook creates the Facebook code for each developer who installs it.

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



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

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

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

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

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

71. The c_user cookie is a means of identification for 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. Facebook uses the c_user cookie to record user activities and communications.

72. A skilled 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 on their mouse, (3) selecting 'View page source,' (4) executing a find (CTRL-F) function for "fb://profile," and (5) copying the number value that appears after "fb://profile" in the page source code of the target Facebook user's page.

73. It is even easier to find the Facebook account associated with a c_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c_user cookie identifier. 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 retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

74. The Facebook datr cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users.

75. Facebook 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 Facebook.

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

77. The Facebook fr cookie is an encrypted combination of the c_user and datr cookies.[6]

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

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

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

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.

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

81. For medical providers, the actions that the Facebook Pixel logs include:

a. When a patient clicks to register for the patient portal;

b. When a patient clicks to log-in to the patient portal;

c. When a patient clicks to logout of the patient portal;

d. When a patient sets up an appointment;

e. When a patient clicks a button to call the provider; and

f. The specific communications a patient exchanges at the provider's property, including those relating to specific providers, conditions, and treatments and the timing of such actions, 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.

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

82. Facebook has publicly acknowledged that targeted advertising based on health information is not appropriate.

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

84. Facebook's announcement was a public relations success:

a. Reuters published a story headlined "Facebook plans to remove thousands of sensitive ad-targeting options" and lead the story with a sentence about Facebook's "plans to remove detailed ad-targeting options that refer to 'sensitive' topics, such as ads based on interactions with content around … health[.]"[8]

[7] https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls

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

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 long be able to use topics such as health … to target people[.]"[9]

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

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

86. Facebook clarified that the change was limited to "people's interactions with content" on the Facebook "platform."

87. Facebook then informed advertisers that 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." In the case of medical providers, the "people who have already engaged" are patients.

E. FACEBOOK CHANGED ITS CONTRACTUAL PRIVACY PROMISES IN 2018

88. Prior to April 2018, Facebook's contract did not "require" partners to have the lawful rights to share user data before doing so.

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

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

[9] https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html

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

CLASS ACTION ALLEGATIONS

91. Plaintiff files this as a class action on behalf of herself and the following class:

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

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

93. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

94. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3), and (c)(4).

95. **Numerosity:** Previous publicly-filed documents confirm the Facebook Pixel has been implemented on at least 664 healthcare provider websites with millions of patients. Accordingly, the members of the Class are so numerous that joinder is impracticable. Class members may be identified from Defendant's records.

96. **Predominant Common Questions:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether the Facebook Pixel is designed to send individually identifiable information to Facebook;

b. Whether the Facebook Terms and Privacy Notice are valid contracts;

c. Whether Facebook failed to require medical providers to have lawful rights to share patient data with Facebook before deploying the Facebook Pixel;

d. Whether Facebook acquired the content of patient communications;

e. Whether the patient class provided Facebook with authorization to acquire their communications with their medical providers, including through the patient portal, appointment forms, and phone calls;

f. Whether the Facebook Pixel's presence and use on medical provider websites where it discloses actions that patients take relating to patient portals, appointments, and phone calls to their medical providers is highly offensive;

g. Whether Facebook's acquisition of the content of communications between patients and their medical providers occurred contemporaneous to their making;

h. Whether Facebook breached its contract with users;

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

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

97. **Typicality:** Plaintiff's claims are typical of the claims of other Class members, as all members of the Class were similarly affected by Facebook's wrongful conduct in violation of federal and California law, as complained of herein.

98. **Adequacy of Representation:** Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel that is competent and experienced

in class action litigation, including nationwide class actions involving privacy violations. Plaintiff and her counsel have no interests that conflict with, or are otherwise antagonistic to, the interests of other Class members. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so.

99. **Superiority:** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single, able court. Furthermore, as the damages that individual Class members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

100. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

TOLLING

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

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

103. At all times, Defendant is and was under a continuous duty to disclose to Plaintiff and members of the Class the true nature of the disclosures being made and the lack of an actual

"requirement" before the data was shared with it.

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

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

CAUSES OF ACTION

COUNT I: BREACH OF CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

106. Plaintiff hereby incorporates paragraphs 1 through 105 as if fully stated herein.

107. Facebook requires users to click a box indicating that, "By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy."

108. "Click-wrap agreements" such as those at issue herein are valid and binding contracts.

109. The Facebook Terms are binding on Facebook and its users.

110. The Facebook Data Policy is binding on Facebook and its users.

111. The Facebook Cookies Policy is binding on Facebook and its users.

112. The Facebook Data Policy promises users that Facebook "requires each of [Facebook's] partners to have lawful rights to collect, use and share your data before providing any data to [Facebook]."

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

114. In addition to the express contract provision set forth above, an implied contract existed between Facebook and its users such that Facebook would not conspire with others to violate Plaintiff's legal rights to privacy in her individually identifiable health information.

115. Plaintiff is a Facebook account holder who used patient portals and/or appointment-related functionality of her medical providers' respective web-properties through which Facebook obtained her individually identifiable health information.

116. Plaintiff Jane Doe used the Novant patient portal by signing in and out of the portal to schedule appointments, access lab results, and review health information, among other things.

117. The patient health information that Facebook obtained in breach of the contract included:

a. Patient identifiers including, but not limited to, email addresses, IP addresses, persistent cookie identifiers, device identifiers, and browser fingerprint information;

b. the data and time of patient registrations for their medical providers' patient portals;

c. log-in and log-out times for their medical providers' patient portals;

d. the contents of communications that patients exchange inside their medical providers' patient portals immediately before logging out of those portals;

e. the contents of communications relating to appointments that patients made with their medical providers; and

f. the user's status as a patient of their medical provider.

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

a. Nominal damages for breach of contract;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information including patient status and appointments that Plaintiff and Class members intended to remain private are no longer private;

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

e. Facebook took something of value from Plaintiff and Class members and derived benefits therefrom without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefit of such value;

f. Benefit of the bargain damages in that Facebook's contract stated that payment for the service would consist of a more limited set of collection of personal information than that which Facebook actually charged.

COUNT II: GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Nationwide Class)

119. Plaintiff hereby incorporates paragraphs 1 through 105 as if fully stated herein.

120. A valid contract exists between Plaintiff and Facebook.

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

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

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

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

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

a. Nominal damages for breach of contract;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information including patient status and appointments that Plaintiff and Class members intended to remain private are no longer private;

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

e. Facebook took something of value from Plaintiff and Class members and derived benefits therefrom without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefit of such value; and

f. Benefit of the bargain damages in that Facebook's contract stated that payment for the service would consist of a more limited set of collection of personal information than that which Facebook actually charged.

COUNT III: INTRUSION UPON SECLUSION CONSTITUTIONAL INVASION OF PRIVACY

(On Behalf of Plaintiff and the Nationwide Class)

126. Plaintiff hereby incorporates paragraphs 1 through 105 as if fully stated herein.

127. 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).

128. Plaintiff had no knowledge and did not consent or authorize Facebook to obtain the content of her communications with her medical providers as described herein.

129. Plaintiff enjoyed objectively reasonable expectations of privacy surrounding communications with her medical providers relating to the respective patient portal and appointments based on:

a. The medical providers status as their health care providers and the reasonable expectations of privacy that attach to such relationships;

b. HIPAA;

c. the Electronic Communications Privacy Act; and

d. Facebook's promise that it would "require" partners to have lawful permission to share their data before Facebook would collect it.

130. Plaintiff's claims are based on the following private facts:

a. that Plaintiff is a patient of Novant;

b. The specific dates and times Plaintiff clicked to log-in or log-out of her medical providers' patient portals;

c. The specific and detailed communications exchanged while logged-in to a patient portal; and

d. The specific dates and times where Plaintiff requested appointments and from which doctor's or practice group pages such appointments were requested.

131. Facebook's conduct was intentional and intruded on Plaintiff's and Class members' medical communications which constitute private conversations, matters, and data.

132. Facebook's conduct in acquiring patient portal and appointment communications would be highly offensive to a reasonable person because:

a. Facebook conspired with Plaintiff's medical providers to violate a cardinal rule of the provider-patient relationship;

b. Facebook's conduct violated federal law designed to protect patient privacy;

c. Facebook's conduct violated the ECPA; and

d. Facebook's conduct violated the express promises it made to users.

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

a. Nominal damages for breach of contract;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information including patient status and appointments that Plaintiff and Class members intended to remain private are no longer private;

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

e. Facebook took something of value from Plaintiff and Class members and derived benefits therefrom without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefit of such value; and

f. Benefit of the bargain damages in that Facebook's contract stated that payment for the service would consist of a more limited set of collection of personal information than that which Facebook actually charged.

COUNT IV: VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

(On Behalf of Plaintiff and the Nationwide Class)

134. Plaintiff hereby incorporates paragraphs 1 through 105 as if fully stated herein.

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

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

137. 18 U.S.C. § 2520(a) provides a private right of action to any person whose electronic communications are intercepted.

138. Facebook intentionally intercepted the electronic communications that Plaintiff exchanged with her respective medical providers on the provider's property where the Facebook Pixel was present.

139. The transmissions of data between Plaintiff and her medical providers qualify as communications under the ECPA's definition in 18 U.S.C. § 2510(12).

140. Facebook acquired patient communications with Plaintiff's medical provider as alleged herein contemporaneous with their making.

141. The intercepted communications include:

a. the content of patient registrations for various patient portals, including clicks on buttons to "Register" or "Signup" for said portals;

b. the content patient log-in and logout of the various patient portals, including clicks to "Sign-in," "Log-in," "Sign-out," or "Log-out."

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

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

142. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Facebook used to track patients' communications;

b. The patients' browsers;

c. The patients' computing devices;

d. Facebook's web-servers;

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

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

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

144. Facebook received the content of patient communications through the surreptitious redirection of them from the patients' computing devices to Facebook.

145. Plaintiff did not consent to Facebook's acquisition of data in her patient portal, appointment, and phone call communications with their medical providers.

146. Facebook did not obtain legal authorization to obtain Plaintiff's communications with her medical providers relating to patient portals, appointments, and phone calls.

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

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

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

a. A knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person;

b. A violation of 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment;

c. Violation of state unfair business practice statutes;

d. Violation of HIPAA; and

e. Violation of Article I, section 1 of the California Constitution.

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

COUNT V: THE CALIFORNIA INVASION OF PRIVACY ACT
(Cal. Penal Code §§ 631 and 632)
(On Behalf of Plaintiff and the Nationwide Class)

151. Plaintiff hereby incorporates paragraphs 1 through 105 as if fully stated herein.

152. 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 for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

153. Cal. Penal Code § 631(a) provides, in pertinent part: "Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts

or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars."

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

155. Facebook is a "person" within the meaning of CIPA §§ 631 and 632.

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

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

158. At all relevant times, Facebook's conduct alleged herein was without the authorization and consent of the Plaintiff and Class members.

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

160. Facebook'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.

COUNT VI: NEGLIGENT MISREPRESENTATION
(On Behalf of Plaintiff and the Nationwide Class)

161. Plaintiff hereby incorporates paragraphs1 through 105 as if fully stated herein.

162. Facebook represented to Plaintiff and the members of the Class that a fact was true, namely, that before receiving the confidential information at issue, Facebook "requires" business "to have lawful rights to collect, use, and share [Plaintiff's and Class members'] data before providing any data" to Facebook.

163. Facebook's representation was not true.

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

165. Facebook intended that Plaintiff and the members of the Class rely on the representation.

166. Plaintiff and the members of the Class reasonably relied on Facebook's representation.

167. Plaintiff and the Class were harmed as set forth above.

COUNT VII: VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
(Cal. Bus. & Prof. Code §§ 17200, *et seq*.)
(On Behalf of Plaintiff and the Nationwide Class)

168. Plaintiff hereby incorporates paragraphs 1 through 105 as if fully stated herein.

169. 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 . . . ."

170. Facebook has engaged in unlawful and unfair business acts and practices in violation of the UCL.

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

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

173. Defendant's actions offend public policy.

174. Defendant's conduct, misrepresentations and omissions have also impaired competition within the health care market in that those actions have prevented Plaintiff and the

Class from making fully informed decisions about whether to communicate online with their healthcare providers and to use their healthcare providers' website in the first instance.

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

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

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

178. Defendant's representation that it requires businesses to "have lawful rights to collect, use, and share [Plaintiff's and Class members'] data before providing any data" to Defendant was untrue. Again, had Plaintiff and Class members known these facts, they would not have used their health care provider's website.

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

180. Plaintiff and the Class request that this Court enjoin Defendant from continuing its unfair, unlawful, and/or deceptive practices, including any use of the information collected to create, develop, or otherwise improve any of its processes, removal of that information from its systems, and to restore to Plaintiff and the Class, in the form of restitution, any money Defendant acquired through its unfair competition.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

1. Certify the proposed Class, designating Plaintiff Jane Doe as the representative of the Class, and designating the undersigned as Class Counsel;

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

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

4. Award attorneys' fees and costs, as allowed by law;

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

6. Enjoin Defendant from any use of the information collected to create, develop, or otherwise improve any of its processes, and remove that information from its systems; and,

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

Date: August 30, 2022

Respectfully Submitted,

Michael F. Ram

MICHAEL F. RAM (SBN 104805)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@ForThePeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN J. MCGEE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com

Attorneys for Plaintiff

DEMAND FOR JURY TRIAL

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

Date: August 30, 2022

Respectfully Submitted,

Michael F. Ram

MICHAEL F. RAM (SBN 104805)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@ForThePeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN J. MCGEE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com

Attorneys for Plaintiff