RACHELE R. BYRD (190634)
ALEX J. TRAMONTANO (276666)
FERDEZA ZEKIRI (335507)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599
byrd@whafh.com
tramontano@whafh.com
zekiri@whafh.com

M. ANDERSON BERRY (262879)
GREGORY HAROUTUNIAN (330263)
BRANDON P. JACK (325584)
CLAYEO C. ARNOLD A PROFESSIONAL CORPORATION
6200 Canoga Avenue, Suite 375
Woodland Hills, CA 91367
Tel: (747) 777-7748
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

JOHN J. NELSON (317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
jnelson@milberg.com

Attorneys for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA

JOHN DOE 1 and JOHN DOE 2, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

SCRIPPS HEALTH,

Defendant.

Case No. **'23CV2215 LL DEB**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1. Plaintiffs JOHN DOE 1, and JOHN DOE 2[1] ("PLAINTIFFS"), at all relevant times herein, have been patients of Scripps Health ("SCRIPPS" or "DEFENDANT") and bring this class action against Defendant in their individual capacity and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, their counsel's investigation, and upon information and belief as to all other matters, as follows:

2. Plaintiffs bring this case to address Defendant's unlawful practice of disclosing Plaintiffs' and Class Members' confidential, personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook") and Google, Inc. ("Google"), without consent, through the use of tracking software that is embedded in Defendant's website.

3. Defendant owns and controls scripps.org ("Defendant's Website" or the "Website"), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, and more.

4. Unbeknownst to patients, Defendant installed tracking technologies ("Tracking Tools") onto its Website. These Tracking Tools, such as pixels, web beacons, or cookies, track and collect communications with the Defendant via the Website and surreptitiously force the user's web browser to send those communications to undisclosed third parties, such as Facebook or Google.

5. Plaintiffs and Class Members used the Website to submit information related to their past, present, or future health conditions, including, for example, searching for particular medical specialists, such as neurologists, and searching for the specific services offered by particular medical specialists and physicians. Such

---

[1] Plaintiffs bring this action anonymously out of a desire to protect their PHI under the Health Insurance Portability and Accountability Act of 1996 and California Law.

Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care from Defendant, as well as the type of medical care, type of physician or specialist, and types of services being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or neurological diseases.

6. Tracking pixels, such as the ones Defendant incorporated into its Website, are created by third-party companies, data brokers, and online advertisers. Defendant implemented and embedded Facebook's tracking pixel ("Pixel") on its Website, and it is simply a snippet of code incorporated for the purpose of tracking every action a user takes, including but not limited to, which buttons they click, the exact search terms or phrases they type into text bars, and any other information that a user communicates to Defendant through the Website. The Pixel shares all the Website visitors' communications and information with its creator, Facebook.

7. The Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel, which events are tracked and transmitted to Facebook and what information from the communications are disclosed.

8. Facebook connects user data from Defendant's Website to the individual's Facebook ID (FID). The FID links the user to his/her Facebook profile, which contains detailed information about the profile owner's identity.

9. Defendant is a healthcare entity and thus its disclosure of health and medical communications is tightly regulated. The United States Department of Health and Human Services (HHS) has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the Health Insurance Portability and Accountability Act of 1996

("HIPAA") Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

10. In addition, as explained further below, HHS has specifically warned healthcare regulated entities that Tracking Tools, like those used by Defendant on its Website, transmit personally identifying information to third parties and that such information should not be transmitted without a HIPAA-acceptable written authorization from patients.

11. The Federal Trade Commission (FTC) has also warned hospitals and other entities that "even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule."

12. In addition, California's Confidentiality of Medical Information Act ("CMIA") prohibits healthcare providers from disclosing medical information regarding its patients without first obtaining their authorization.

13. Despite these warnings, Defendant embedded hidden Tracking Tools on its Website, essentially planting a bug on patients' web browsers that forced them disclose private and confidential communications to third parties. Defendant did not disclose the presence of these Tracking Tools to its patients and Website users.

14. Healthcare patients simply do not anticipate or expect that their trusted healthcare provider will send personally identifying health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients' consent. Neither Plaintiffs nor any other Class Members signed a written authorization permitting Defendant to send their Private Information to Facebook.

15. Defendant breached its statutory and common law obligations to

Plaintiffs and Class Members by, *inter alia*: (i) failing to adequately review its marketing programs and web-based technology to ensure its Website was safe and secure; (ii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (iii) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Tools like the Facebook Pixel; (iv) failing to warn Plaintiffs and Class Members; and (v) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patients' Private Information.

16. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) diminution of value of their Private Information; and (iv) the continued and ongoing risk to their Private Information.

17. Plaintiffs seek to remedy these harms and bring claims for: (1) violation of California Invasion of Privacy Act ("CIPA"); (2) violation of the California Confidentiality of Medical Information Act ("CMIA"); (3) violation of the California Unfair Competition Law ("UCL"); (4) breach confidence; (5) invasion of privacy under the California Constitution; (6) common law invasion of privacy—intrusion upon seclusion; (7) negligence; (8) breach of implied contract; (9) breach of contract; (10) violations of the Electronic Communications Privacy Act ("ECPA") 18 U.S.C. § 2511(1), *et seq*., and (11) violation of title II of the ECPA, 18 U.S.C. § 2702, *et seq*.

PARTIES

18. Plaintiff John Doe 1 is a natural person and citizen of California, residing in Cathedral City, California (Riverside County), where he intends to remain.

19. Plaintiff John Doe 2 is a natural person and citizen of California, residing in San Diego, California (San Diego County), where he intends to remain.

20. Defendant Scripps Health is a non-profit healthcare entity operating throughout the San Diego area and with its principal place of business in San Diego. Defendant provides comprehensive health care to California citizens through five hospital campuses, thirty clinics, and more than 3,000 San Diego doctors.[2] Defendant is a covered entity under HIPAA (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164). Defendant owns and operates www.scripps.org.

JURISDICTION & VENUE

21. This Court has jurisdiction under 28 U.S.C. § 1331. The Court has jurisdiction over the state law claims under 28 U.S.C. § 1367 because those claims are so related to the federal claims brought by Plaintiffs at the time the matter was originally brought that they form part of the same case or controversy, and the Court may continue to exercise jurisdiction even if no federal claim remains.

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. The U.S. Department of Health and Human Services and Federal Trade Commission Have Warned about Use of Tracking Tools by Healthcare Providers

23. Considering Tracking Tools like the Pixel, HHS issued a bulletin instructing regulated entities like Defendant to only use such software in an extremely limited function:

> **Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology**

[2] *Looking for a Doctor?*, Scripps Health, https://www.scripps.org/physicians/find (last visited Dec. 4, 2023).

> **vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures of [electronic protected health information] to tracking technology vendors or any other violations of the HIPAA Rules.[3]

In other words, HHS has expressly stated that entities like Defendant that implement the Facebook Pixel have violated HIPAA Rules unless those entities obtain a HIPAA-complaint authorization.

24. The HHS Bulletin further warns that:

> While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*** [4]

25. Additionally, HHS has warned healthcare providers that Protected Information is not limited exclusively to patient portals like MyChart, and Defendant still has an obligation to protect information on non-password protected pages or unauthenticated pages:

> Tracking technologies on a regulated entity's unauthenticated webpage that **addresses specific symptoms or health conditions**, such as pregnancy or miscarriage, or that permits individuals to **search for doctors or schedule appointments** without entering credentials may have access to PHI in certain circumstances. For example, **tracking**

---

[3] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* U.S. Dep't of Health and Hum. Servs. (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Dec. 4, 2023).

[4] *Id.*

> **technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider.** In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[5]

26. Moreover, HHS and the FTC have recently issued a warning letter directly to Defendant informing it that its use of online Tracking Tools presents serious privacy and security risks, and that Defendant is impermissibly disclosing consumers' sensitive personal health information to third parties. Specifically, the letter provides:

> The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.
>
> Recent research,[] news reports,[] FTC enforcement actions,[] and an OCR bulletin [] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.
>
> Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition,

[5] *Id*. (emphasis added).

> impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.
>
> **Health Insurance Portability and Accountability Act of 1996 (IDP AA)**
>
> If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium.
>
> The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI…
>
> **FTC Act and FTC Health Breach Notification Rule**
>
> Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[6]

B. Underlying Web Technology

27. To understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and Tracking Tools.

---

[6] Attached hereto as **Exhibit A** is a true and correct copy of the July 20, 2023 letter to Defendant from the HHS regarding Defendant's unlawful "Use of Online Tracking Technologies."

28. Devices (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

29. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

30. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **Universal Resource Locator ("URL")**: a web address.
- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL, GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[7]

[7] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

31. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code. Source Code is essentially the back of the website, and the user does not see what happens in the source code.

32. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Pixels are embedded in the Source Code and instructs the Website to send a second set transmissions to the third party's servers, i.e., Facebook and Google.

33. By contrast, the Markup is the façade of the Website and what the user sees.

34. As an example, a patient's HTTP Request seeks specific information from the Defendant's Website (e.g., "Find a Doctor" page), and the HTTP Response provides the requested information in the form of "Markup," forming the webpage's content and features.

35. For example, when a patient visits scripps.org and selects the "Find a Doctor" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that webpage. As depicted below, the user only saw the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

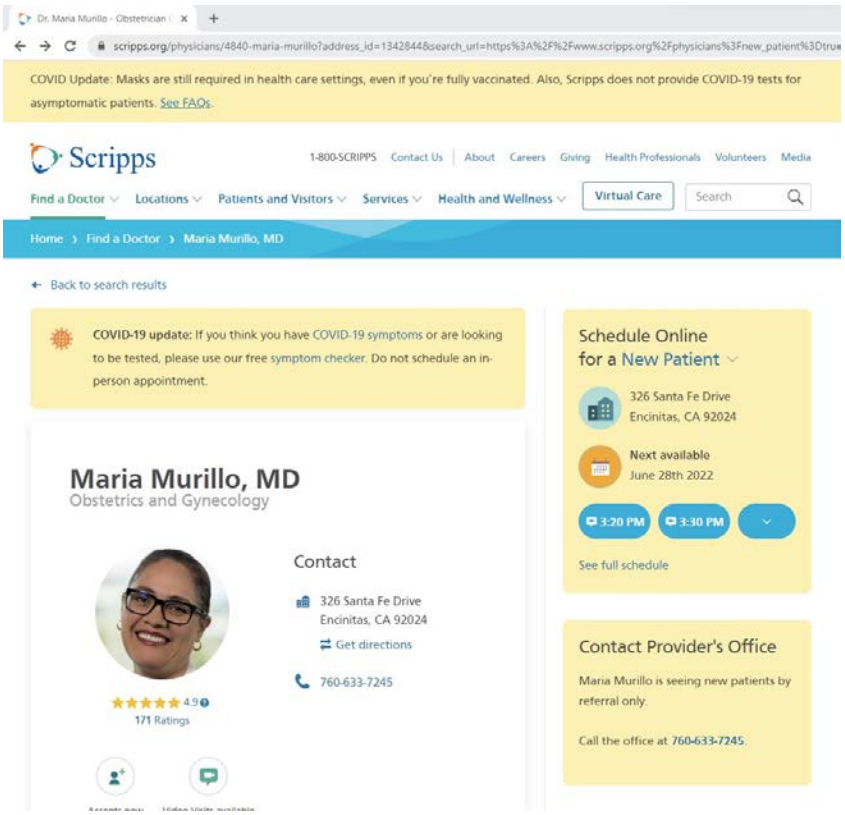


Figure 1. The image above is a screenshot taken from Markup GitHub[8] evidence for its article detailing Defendant's and other hospitals' data practices (screenshot from 4/27/2022).

36. Above is the Markup of Defendant's Webpage. Behind the scenes and in the backdoor of the webpage, Tracking Tools like the Facebook Pixel were embedded in the Source Code, automatically transmitting what the patient did on the webpage and effectively opening a hidden spying window into the patient's browser.[9]

---

[8] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last accessed October 31, 2023).

[9] When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. The Facebook Pixel is a tiny image file that is so small

37. Defendant's source code manipulated the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook. These transmissions occurred contemporaneously, invisibly, and without the patient's knowledge.

38. Thus, without its patients' consent, Defendant effectively used its source code to commandeer and "bug" or "tap" its patients' computing devices, allowing Facebook and other third parties to listen in on all their communications with Defendant and thereby intercept those communications, including Private Information, including, but not limited to, their status as patients, searches for physicians, treatments, treatment locations, conditions, and appointment information.

C. Tracking Tools

39. Third parties, like Facebook and Google, offer Tracking Tools as software that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user communications and activity on those platforms. The Tracking Tools are used to gather, identify, target, and market products and services to individuals.

40. In general, Tracking Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's URL and metadata, button clicks, etc. Advertisers, such as Defendant, can track other user actions and communications and can create their own tracking parameters by customizing the software on their website.

41. When a user accesses a webpage that is hosting Tracking Tools, the user's communications with the host webpage are instantaneously and surreptitiously duplicated and sent to the third party. For example, the Facebook

---

as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

Pixel on Defendant's Website caused the user's web browser to instantaneously duplicate the contents of the communication with the Website and send the duplicate from the user's browser directly to Facebook's server.

42. Notably, transmissions only occur on webpages that contain Tracking Tools.[10] Thus, Plaintiffs' and Class Member's Private Information would not have been disclosed to Facebook or Google via this technology but for Defendant's decisions to install the Tracking Tools on its Website.

43. Sometimes a particularly tech-savvy user attempts to circumvent browser-based wiretap technology, so a website operator can also transmit data directly to Facebook using first-party cookies (CAPI server-to-server transmission). Users cannot detect or prevent transmissions through first-party cookies.

44. CAPI is another Facebook tool that functions as a redundant measure to circumvent any ad blockers or other denials of consent by the website user by transmitting information directly from Defendant's servers to Facebook's servers.[11,] [12] Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you

---

[10] Defendant's Facebook Pixel has its own unique identifier (represented as id=737223089739564), which can be used to identify which of Defendant's webpages contain the Facebook Pixel.

[11] *What is the Facebook Conversions API and how to use it*, Realbot (last updated May 20, 2022), https://revealbot.com/blog/facebook-conversions-api/ (last visited Nov. 28, 2023).

[12] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited Nov. 28, 2023).

better understand how digital advertising impacts both online and offline results."[13]

45. The third parties to whom a website transmits data through Tracking Tools and associated workarounds (CAPI) do not provide any substantive Website content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (*i.e.*, to bolster profits).

46. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

D. Defendant Disclosed Plaintiffs' and Class Members' Private Information to Facebook Using Tracking Technologies in Violation of its Privacy Policy

47. Defendant's *Privacy Policy* provides that: "By using this site, you agree that Scripps may monitor your use of this website and may use the results of such monitoring without limitation… Personally identifiable information may be collected from visitors to our site and provided in an aggregate form to other parties within the Scripps family for marketing, advertising, or other similar uses."[14]

48. However, at no point did Defendant's *Privacy Policy* provide that

---

[13] *About Conversions API*, Meta Business Help Center, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Dec. 4, 2023).

[14] Scripps Health has since updated its *Privacy Policy* and allegedly it has removed tracking technology; however, the previous *Privacy Policy* was recovered using the Wayback Machine, a webtool that catalogues captured pages. The *Privacy Policy* referenced was captured on Defendant's page on June 19, 2022. https://web.archive.org/web/20220619002542/https://www.scripps.org/privacy-policy (last accessed October 31, 2023).

Plaintiffs' and Class Members' sensitive medical information and personally identifiable information may be shared with any third-party sites outside of the "Scripps family," such as Facebook or Google.[15] Indeed, Defendant's *Privacy Policy* clearly does not include Facebook or Google as part of its "Scripps family."

49. Defendant intentionally installed Tracking Tools to secretly track patients by disclosing their communications in violation of its own *Privacy Policy*, common law, contractual, statutory, and regulatory duties and obligations.

50. Defendant's Facebook Pixel had its own unique identifier (represented as id=737223089739564), which was used to identify which of Defendant's webpages contained the Facebook Pixel.

51. The Facebook Pixel allowed Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs. However, Defendant's Website did not rely on the Pixel in order to function.

52. While seeking and using Defendant's services as a medical provider, Plaintiffs and Class Members communicated their Private Information to Defendant via its Website.

53. Plaintiffs and Class Members were not aware that their Private Information would be shared with Facebook as it was communicated to Defendant because, among other reasons, Defendant did not disclose this fact.

54. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

55. Defendant's Pixel and First Party cookies sent non-public Private Information to Facebook, including but not limited to Plaintiffs' and Class

---

[15] *Id.*

Members': (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) desired locations or facilities where treatment was sought; (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers); and (6) searches for and selections of physicians and their specialties conducted via the general search bar.

56. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiffs' and Class Members' Facebook IDs (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identities.[16]

57. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographics and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's FID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the FID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

58. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel and first party cookies) that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

---

[16] Defendant's Website tracked and transmitted data via first party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

E. Defendant's Pixel Disseminates Patient Information via Its Website

59. An example illustrates the point. If a patient used the Website to find a physician and book an appointment, Defendant's Website directed them to communicate Private Information, including the specialty of the physician, the physician's name, the date and time of the desired appointment, and the location of the appointment. Unbeknownst to the patient, every communication was sent to Facebook via Defendant's Pixel.

60. Unbeknownst to ordinary patients, the "Find a Doctor" page and its included appointment section—which was undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contained Defendant's Facebook Pixel. The image below shows the "behind the scenes" portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Facebook Pixel sent this user's information to Facebook.

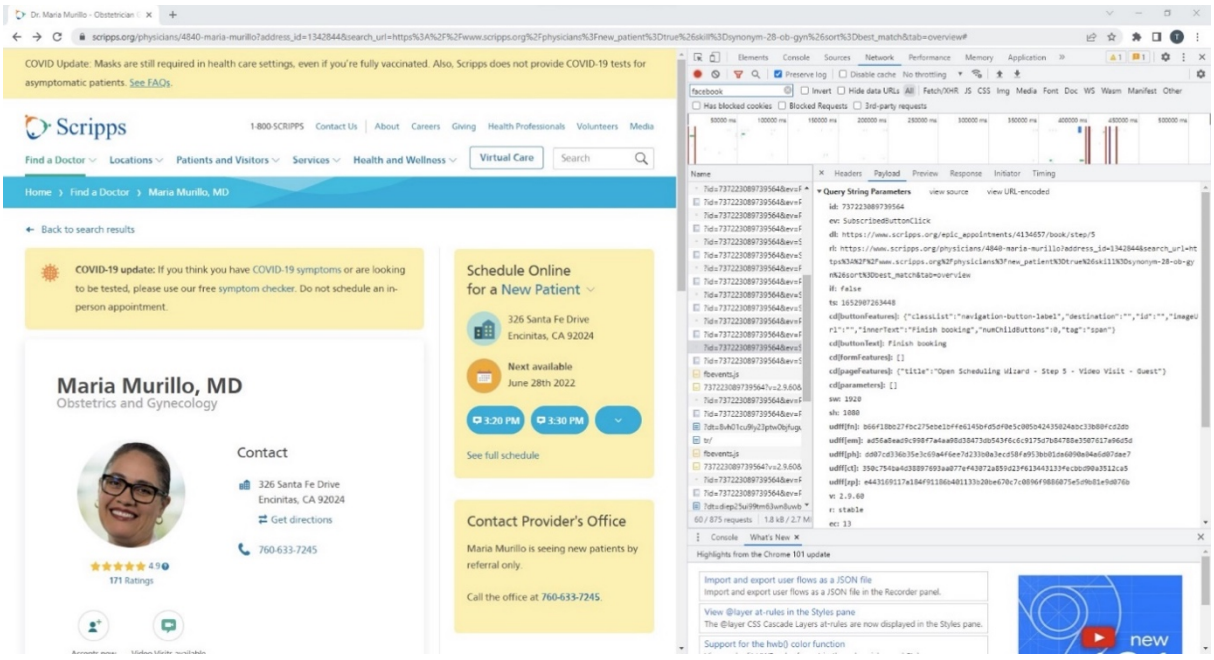


Figure 2. The image above is a screenshot taken from the Markup GitHub research for its article on Defendant's conduct (captured 4/27/2022)

61. Thus, without alerting the user, Defendant's Facebook Pixel sent each

and every communication the user made via the webpage to Facebook, and the images below confirm that the communications Defendant sent to Facebook contained the user's Private Information.

62. The first line of highlighted text, "id:737223089739564", refers to Defendant's Facebook Pixel ID and confirms that Defendant downloaded the Pixel into its source code on this webpage.

63. On the same line of text, "ev= SuscribedButtonClick" identifies and categorizes which actions the user took on the webpage ("ev=" is an abbreviation for event, and "SubsrcibedButtonClick" is the type of event). Thus, this identifies the user as pressing the button labeled "Finish Booking."

64. The additional lines of highlighted text show Defendant had disclosed to Facebook that the user: (1) was a patient seeking medical care from Defendant via scripps.org, even labeling the user as "new patient" to make it painstakingly clear; (2) the user sought treatment from physician Dr. Maria Murillo; (3) the physician is an OB-GYN; and (4) the user "Finish[ed] Booking" an appointment with the specific OB-GYN physician.

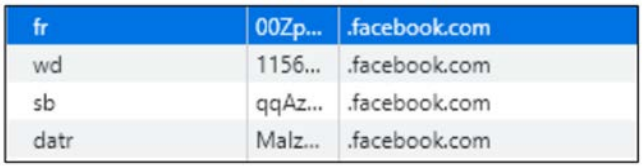
65. Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's FID (c_user ID), thereby allowing the user's communications and actions on the Website to be linked to the user's specific Facebook profile.

66. In the example above, the user's Website activity and the contents of the user's communications were sent to Facebook alongside their personally identifiable information using the c_user cookie that links to Facebook when the user is logged in. Several different methods allow marketers and third parties to identify individual website users other than the interaction between the c_user cookie and the Pixel.

67. Facebook received at least six cookies when Defendant's Website

transmitted information via the Pixel while the user was logged in, including the c_user cookie.

68. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies:[17]



fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 3. Screengrab from Defendant's Website depicting the cookies attached to a recently logged out facebook user when they search Defendant's Website.

69. The fr cookie contains an encrypted FID and browser identifier.[18] Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[19]

70. The cookies referred to above are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible the way individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout its Website.

71. Defendant also revealed its website visitors' identities via first-party

---

[17] The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the fbp cookie, which is transmitted as a first-party cookie.

[18] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Dec. 4, 2023).

[19] *Cookies Policy*, Meta (effective June 16, 2023), https://mbasic.facebook.com/privacy/policies/cookies/printable/ (last visited October 31, 2023).

cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user.[20]

72. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookie and the c_user cookie, the _fbp cookie functions as a first-party cookie—i.e., a cookie that was created and placed on the website by Defendant.[21]

73. The Facebook Pixel uses both first- and third-party cookies.

74. In summation, Facebook, at a minimum, use the fr, _fbp, and c_user cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, patients' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

F. Defendant's Use of Google Analytics

75. Defendant also utilized Google Analytics tracking technology which Defendant did reveal within its *Privacy Policy* during its time using and implementing Google's tracking technology.[22]

76. Defendant stated, "Scripps uses Google Analytics, a web analytics service by Google Inc." and additionally claimed, "We do not use Google Analytics to gather information that personally identifies you."[23] However, the Google Analytics version that was in operation during Defendant's implementation could log and store IP address information, which is personally identifying information

---

[20] *Id.*

[21] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

[22] *Supra* fn. 14.

[23] *Id.*

and impermissible under HIPAA.[24]

77. Additionally, Google Analytics services could be accompanied by a session ID cookie that connects with a user's Google account and personally identifies a patient based on the personal information contained in the patient's Google account such as name, email address, address, phone number, etc.

78. The HHS bulletin states:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the **Privacy Rule does not permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures.** Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.[25]

79. Accordingly, Defendant's statements do not exculpate its impermissible use of tracking technology. Defendant's statements regarding its use of Google Analytics do not reveal the scope of Private Information that is transmitted to Google and how Private Information is used for advertising and marketing data packages.

80. Defendant removed tracking technology and changed its privacy policy, so Plaintiffs are not currently able to discover the scope of Defendant's data sharing practices. Discovery is necessary to find whether Defendant's use of Google

---

[24] In March of 2022, Google announced that it would no longer use IP addresses, phase out previous Analytics software by 2023 and replace all Google analytics technology with GA4 that comes equipped with Privacy features. *See* Kendra Clark, *Google Analytics stops logging IP addresses: here's why it's a big deal for marketers*, The Drum (March 16, 2022), https://www.thedrum.com/news/2022/03/16/google-analytics-nixes-ip-address-logging-new-privacy-play (last visited October 31, 2023).

[25] *Supra* fn. 3 (emphasis added).

Analytics resulted in impermissible disclosures.

81. Defendant did not disclose that the Pixel, first party cookies, Google Analytics, or any other Tracking Tools embedded in the Website's source code tracked, recorded, and transmitted Plaintiffs' and Class Members' Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiffs' and Class Members' private communications to Facebook or Google.

G. Plaintiffs' Experiences

Plaintiff John Doe 1's Experience

82. Plaintiff John Doe 1 has been a patient of Scripps Health since 2015 and has received healthcare services at hospitals and clinics in Defendant's network.

83. On numerous occasions since 2015, and prior to June of 2022, Plaintiff accessed Defendant's Website on his computer and/or mobile device for the purpose of finding and obtaining medical treatment for his lumbar fusion and neurological issues during the Defendant's operation of tracking technology. Plaintiff accessed Defendant's Website to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

84. Plaintiff John Doe 1 used Defendant's Website to search for particular medical physicians that specialize in treating lumbar fusion and neurological ailments, and to send inquiries about healthcare services for his lumbar fusion and neurological issues via the Defendant's Website.

85. Plaintiff John Doe 1 has been a Facebook user since at least 2004.

86. As Defendant's patient, Plaintiff John Doe 1 reasonably expected that his online communications with Defendant were solely between himself and Defendant and that such communications would not be transmitted to or disclosed to a third party. But for his status as Defendant's patient, Plaintiff would not have disclosed his Private Information to Defendant.

87. Plaintiff John Doe 1 provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

88. During his time as a patient, Plaintiff John Doe 1 never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

89. Plaintiff John Doe 1 had a specific medical procedure performed to treat his lumbar fusion and resulting neurological issues and submitted information to Defendant's Website about this procedure, specialists who could perform this procedure, along with other healthcare related items which Defendant simultaneously sent to Facebook.

90. Defendant transmitted to Facebook Plaintiff John Doe 1's personal information and protected health information including but not limited to his email address; phone number; computer or device IP address; appointment information; information entered into Defendant's Website; button/menu selections, and/or content typed into free text boxes; and sensitive medical information such as physicians selected, details about his searches for physicians and specialists, details about his searches for medical services; and other protected health information.

91. Pursuant to the systematic process described in this Complaint, Plaintiff John Doe 1's Private Information was disclosed to Facebook and Google, and this data included his PII, PHI, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiff John Doe 1's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff John Doe 1's Private Information.

92. Notwithstanding, through the Pixel, Defendant transmitted Plaintiff John Doe 1's Private Information to third parties, such as Facebook.

93. After intercepting and collecting this information, Facebook views it, processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a FID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographics and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

94. Indeed, Facebook has viewed, processed, analyzed, and assimilated into datasets Plaintiff John Doe 1's PII and PHI transmitted to it by Defendant because Plaintiff has received targeted ads regarding his specific medical conditions in his Facebook feed after using Defendant's website for health services. Specifically, Plaintiff John Doe 1 used Defendant's website to search for specialists and physicians that would be able to treat his lumbar fusion and neurological issues and related medical services, and then immediately started receiving advertisements on his Facebook feed pertaining to lumbar fusion and neurological ailments. These advertisements included advertisements for different pieces of hardware used to treat lumbar fusion issues, and various medicines commonly used to treat lumbar fusion and neurological issues.

95. In sum, Defendant's Pixel transmitted Plaintiff John Doe 1's highly sensitive communications and Private Information to Facebook, including communications that contained Private and confidential information, without Plaintiff John Doe 1's knowledge, consent, or express written authorization, which Facebook then viewed, processed, analyzed, and assimilated into datasets to target

Plaintiff John Doe 1 with targeted ads for his specific medical condition.

96. Defendant breached Plaintiff John Doe 1's right to privacy and unlawfully disclosed his Private Information to Facebook. Specifically, Plaintiff John Doe 1 had a reasonable expectation of privacy, based on his status as Defendant's patient, that Defendant would not disclose his Private Information to third parties.

97. Defendant did not inform Plaintiff John Doe 1 that it shared his Private Information with Facebook.

98. By doing so without Plaintiff John Doe 1's consent, Defendant breached Plaintiff John Doe 1's and Class Members' right to privacy and unlawfully disclosed Plaintiff John Doe 1's Private Information.

99. Upon information and belief, as a "redundant" measure to ensure Plaintiff John Doe 1's Class Members' Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds to send Plaintiff John Doe 1's and Class Members' Private Information from electronic storage on Defendant's server directly to Facebook.

100. Plaintiff suffered injuries in the form of (i) invasion of privacy; (ii) loss of the benefit of the bargain; (iii) diminution of value of the Private Information; (iv) statutory damages; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff John Doe 1's lumbar fusion and neurological conditions and other confidential information he communicated to Defendant via the Website.

Plaintiff John Doe 2's Experience

101. Plaintiff John Doe 2 received and utilized healthcare services the Defendant has offered since the 1980's.

102. Plaintiff John Doe 2 entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff John Doe 2 disclosed his

Private Information to Defendant.

103. On numerous occasions prior to June of 2022 and continuing to the present, Plaintiff John Doe 2 accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

104. Plaintiff John Doe 2 inquired about healthcare services; researched symptoms, conditions, and treatments; communicated with healthcare professionals; utilized the Website's chat function; took health classes; watched instructional videos; reviewed medical billings and records; and searched for physicians and specialists for ailments he suffers from via the Defendant's Website.

105. Plaintiff John Doe 2 became a Facebook user in 2004.

106. Plaintiff John Doe 2 reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

107. Plaintiff John Doe 2 provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

108. As described herein, Defendant worked along with Facebook to intercept Plaintiff John Doe 2's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff John Doe 2's knowledge, consent, or express written authorization.

109. Defendant transmitted to Facebook Plaintiff John Doe 2's Personal Information including but not limited to his email address; phone number; computer or device IP address; information entered into Defendant's Website; button/menu selections, and/or content typed into free text boxes; and protected health information such as, but not limited to, appointment dates, details about his specific

ailments, and details about the health classes Plaintiff John Doe 2 attended.

110. By doing so without Plaintiff John Doe 2's consent, Defendant breached Plaintiff John Doe 2's right to privacy and unlawfully disclosed Plaintiff John Doe 2's Private Information.

111. Defendant did not inform Plaintiff John Doe 2 that it had shared his Private Information with Facebook. Plaintiff John Doe 2 discovered on his own that Defendant shared his Private Information with Facebook in or around July 2023.

112. Plaintiff John Doe 2 had specific medical ailments including: Crohn's disease, atherosclerosis, a heart valve surgery and peripheral neuropathy, and he treated with a Primary Care Physician, Cardiologist, Dermatologist, Gastroenterologist, Physician's Assistants, Nurse Practitioners and Nurses, and submitted information to Defendant's Website, and searched for information on Defendant's Website, about these ailments along with other healthcare related items which Defendant simultaneously submitted to Facebook.

113. Plaintiff John Doe 2 observed ads on YouTube while watching videos that appeared related to his prior searches on and his use of the Defendant's Website.

H. Defendant's Conduct Is Unlawful and Violated Industry Norms

Defendant Violated HIPAA Standards

114. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[26]

115. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care

[26] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 164.508(a)(3), 164.514(b)(2)(i).

clearinghouses, and those health care providers that conduct certain health care transactions electronically."[27]

116. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

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

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

A. Names;

---

[27] *HIPAA For Professionals*, U.S. Dept. of Health & Hum. Servs., https://www.hhs.gov/hipaa/for-professionals/index.html (last visited October 31, 2023).

> ***
>
> H. Medical record numbers;
>
> ***
>
> J. Account numbers;
>
> ***
>
> M. Device identifiers and serial numbers;
>
> N. Web Universal Resource Locators (URLs);
>
> O. Internet Protocol (IP) address numbers; … and
>
> ***
>
> R. Any other unique identifying number, characteristic, or code…; and
>
> (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

45 C.F.R. § 160.514(b)(2).

119. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

120. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person . . . shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered

entity . . . and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

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

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

123. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS, Office for Civil Rights (OCR) instructs:

> 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.[28]

124. In its guidance for Marketing, OCR 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

[28] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited October 31, 2023).

> 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*. (Emphasis added).[29]

125. As alleged above, the HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[30]

126. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

127. The Bulletin also provides that the use of tracking technologies even on unauthenticated webpages may violate the HIPAA Rules if those webpages have access to PHI.[31]

128. Defendant's actions violated HIPAA Rules. While there is no private right of action under HIPAA and these violations do not constitute a cause of action in and of themselves, the violation of HIPAA Rules provides context for the elements of Plaintiffs' and Class Members' underlying claims, including, *inter alia*: (1) the confidential nature of the information communicated to Defendant; (2) Plaintiffs' and Class Members' reasonable expectation of privacy in their

---

[29] *Marketing*, OCR HIPPA Privacy (created December 3, 2002, revised April 3, 2002), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited October 31, 2023).

[30] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[31] *Id.*

confidential Private Information; (3) the highly offensive nature of Defendant's disclosure of Private Information; and (4) the fact that the Private Information communicated (including searches for specific symptoms, health conditions, or doctors, or the scheduling of appointments) constitutes the "contents" of the communication.

I. Defendant Violated American Medical Association's Industry Standards

129. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

130. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

131. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care. . . . Patient privacy encompasses a number of aspects, including, . . . personal data (informational privacy) . . . . .[32]

132. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship.[33]
>
> Physicians who propose to permit third-party access to specific patient

---

[32] *See* https://code-medical-ethics.ama-assn.org/ethics-opinions/privacy-health-care (last visited October 31, 2023).

[33] *See* https://code-medical-ethics.ama-assn.org/ethics-opinions/access-medical-records-data-collection-companies (last visited October 31, 2023).

information for commercial purposes should:

(a) Only provide data that has been de-identified. [and]

(b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted.

133. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.

Physicians who collect or store patient information electronically . . . must: . . . (c) Release patient information only in keeping ethics guidelines for confidentiality.[34]

J. Plaintiffs' and Class Members' Expectation of Privacy

134. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

135. Indeed, at all times when Plaintiffs and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

136. Plaintiffs and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

---

[34] *See* https://code-medical-ethics.ama-assn.org/ethics-opinions/confidentiality-electronic-medical-records (last visited October 31, 2023).

K. IP Addresses are PII

137. On information and belief, using the Tracking Tools on Defendant's Website, Defendant also disclosed and otherwise assisted third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

138. An IP address is a number that identifies the address of a device connected to the Internet.

139. IP addresses are used to identify and route communications on the Internet.

140. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

141. Facebook tracks every IP address ever associated with a Facebook user.

142. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

143. Under HIPAA, an IP address is considered PII:

- HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

144. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

L. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

145. The primary motivation for, and a determining factor in Defendant's

interception and disclosure of Plaintiffs' and Class Members' Private Information, was to use patient data for advertising in the absence of express written consent, which are criminal and tortious acts in violation of federal and state laws as alleged herein. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the Private Information of its patients, Defendant was compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

146. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

147. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Plaintiffs were personally retargeted with ads related to their medical conditions. Defendant did so through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

148. By utilizing the Pixel, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and Class Members and violating their rights under federal and State law.

M. Plaintiffs' and Class Members' Private Information Had Financial Value

149. Plaintiffs' data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

150. Data harvesting is one of the fastest growing industries in the country,

and consumer data is so valuable that it has been described as the "new oil."[35] Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data.[36] That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.[37]

151. The value of health data is well-known and has been reported upon extensively in the media. For example, Time Magazine published an article in 2017 titled, "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[38]

152. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[39]

---

[35] *See* Joris Toonders Yonego, *Data is the New Oil of the Digital Economy*, Wired https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited October 31, 2023).

[36] *See* Robert Shapiro, *What Your Data Is Really Worth to Facebook*, Washington Monthly (July 12, 2019) https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/#:~:text=In%20the%20end%2C%20we%20calculated,detailed%20data%20that%20companies%20collect. (last visited October 31, 2023).

[37] *Id*.

[38] *See* Adam Turner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, Time (January 9, 2017), https://time.com/4588104/medical-data-industry/ (last visited October 31, 2023).

[39] *See* Christina Farr, *Hospital Execs Say They are Getting Flooded with Requests for Your Health Data*, CNBC (December 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited October 31, 2023).

TOLLING

169. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that their PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

170. Class Definition: Pursuant to 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and other similarly situated individuals (the "Class"), defined as:

> Any and all California citizens who, during the Class Period, used Defendant's Website and were patients of Defendant.

171. The "Class Period" is defined as the period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement.

172. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

173. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiffs currently. However, it is estimated that there are thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party Facebook's records.

174. Typicality. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs used Defendant's Website and had their personally identifiable information and protected health information disclosed to third parties such as Facebook and Google without their express written authorization or knowledge. Plaintiffs' claims are based on the same legal theories as the claims of other Class Members.

175. Adequacy. Plaintiffs are fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the Class Members. Plaintiffs are represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiffs' attorneys are committed to vigorously prosecuting this action on behalf of the Class Members.

176. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

(a) Whether Defendant intentionally tapped the lines of internet communication between patients and their medical providers;

(b) Whether Defendant's Website surreptitiously tracked personally identifiable information, protected health information, and related communications and simultaneously disclosed that information to Facebook and/or other third parties;

(c) Whether Facebook is a third-party eavesdropper;

(d) Whether Defendant's disclosures of personally identifiable

information, protected health information, and related communications constitute an affirmative act of communication;

(e) Whether Defendant's conduct, which allowed Facebook to view Plaintiffs' and Class Members' personally identifiable information and protected health information, resulted in a breach of confidentiality;

(f) Whether Defendant violated Plaintiffs' and Class Members' privacy rights by using Facebook's Pixel to communicate online patients' Private Information and FIDs to Facebook;

(g) Whether Plaintiffs and Class Members are entitled to damages under the CMIA;

(h) Whether Plaintiffs and Class Members are entitled to damages under the CIPA or any other relevant statute;

(i) Whether Defendant's actions violated the Unfair Competition Law;

(j) Whether Defendant's actions violated Plaintiffs' and Class Members' privacy rights as provided by the California Constitution;

(k) Whether Defendant breached a duty to safeguard Plaintiffs' and Class Members' sensitive personal and health information.

(l) Whether Defendant violated the consumer protection statues invoked herein.

Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually,

substantially outweighs potential difficulties in management of this class action. Plaintiffs are unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*

177. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth therein and bring this count individually and on behalf of the proposed Class.

178. The California Invasion of Privacy Act ("CIPA") begins with its statement of purpose.

> The Legislature thereby 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.

179. CIPA prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or 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 California.

180. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

> 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 unlawfully 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 ($2,500).

181. Under CIPA, a defendant must show it had the consent of all parties to a communication.

182. Violations of CIPA are not limited to phone lines, but also apply to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, No. 15-cv-04062, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, No. C06-05289, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history). Indeed, the Facebook Pixel was recently examined by the Northern District of California with the district court concluding that the plaintiffs were likely to succeed on the merits with respect to both CIPA and the analogous Federal Wiretap Act. *See In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *11, 13 (N.D. Cal. Dec. 22, 2022).

183. CIPA affords a private right of action to any person who has been subjected to a violation of the statute to seek injunctive relief and statutory damages of $5,000 per violation, regardless whether they suffered actual damages. Cal. Penal

Code § 637.2.

184. At all relevant times, Defendant aided, employed, agreed with, and conspired with Facebook to track and intercept Plaintiffs' and Class Members' internet communications while accessing Defendant's Website. These communications were transmitted to and intercepted by a third party during the communication and without the knowledge, authorization, or consent of Plaintiffs and Class Members.

185. Defendant intentionally inserted an electronic listening device onto Plaintiffs' and Class Members' web browsers that, without the knowledge and consent of Plaintiffs and Class Members, tracked and transmitted the substance of their confidential communications with Defendant to a third party. Indeed, the Office for Civil Rights at the U.S. Department of Health and Human Services acknowledges in their letter to Defendant that Defendant's "use of online tracking technologies" on its "website or mobile application" is "impermissibly disclosing consumers' sensitive personal health information to third parties."[40]

186. Defendant willingly facilitated Facebook's interception and collection of Plaintiffs' and Class Members' private medical information by embedding the Facebook Pixel on its Website. Moreover, unlike past Facebook business tools such as the Facebook Like Button and older web beacons, Defendant has full control over the Pixel, including which webpages contain the Pixel, what information is tracked and transmitted via the Pixel, and how events are categorized prior to their transmission.

187. Defendant's Pixel and tracking tools constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, these tools fall under the broad catch-all category of "any other manner."

188. Defendant failed to disclose its use of the Facebook Pixel, Google

[40] *See* **Exhibit A**.

Analytics, or other tracking technologies to specifically track and automatically and simultaneously transmit Plaintiffs' and Class Members' private communications with Defendant to undisclosed third parties.

189. The Private Information that Defendant transmitted via the Facebook Pixel, such as searching a particular medical specialty, finding a physician in that specialty, booking an appointment with that physician, utilizing the chat function to speak with healthcare professionals, searching particular health conditions, and reviewing medical bills and records, all constitute information about Plaintiffs' and Class Members' past, present, or future health or health care and therefore constitute protected health information.

190. The Pixel is designed such that it transmits each of the users' actions taken on the Website to a third party alongside and contemporaneously with the user initiating the communication. Thus, the communication is intercepted in transit to the intended recipient, Defendant, and before it reaches Defendant's server.

191. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to intercept and receive its patients' online communications in real time through its Website. Such interception occurred without Plaintiffs' and Class Members' consent, and Facebook, Google, and other third parties would not have received the contents of these communications but for Defendant's actions.

192. By disclosing Plaintiffs' and Class Members' Private Information, Defendant violated Plaintiffs' and Class Members statutorily protected right to privacy.

193. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiffs and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiff has

suffered, or be threatened with, actual damages."

194. Under the statute, Defendant is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

SECOND CAUSE OF ACTION
Violation of the California Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code § 56, *et seq*.

195. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

196. Pursuant to the California Confidentiality of Medical Information Act ("CMIA"), "A provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in subdivision (b) or (c)." § 56.10(a).[41] "An authorization for the release of medical information . . . shall be valid if it:

> (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
>
> (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.

[41] Subdivisions (b) and (c) are not relevant to this case but permit the disclosure of medical information in situations where a government investigation or lawsuit is taking place. For example, Defendant could bypass the authorization requirement if patient medical information was requested pursuant to a lawful court order or by a party to a proceeding before a court or administrative agency pursuant to a subpoena. *See* Cal. Civ. Code §§ 56.10(b)(3) and 56.10(b)(6).

> (c) Is signed and dated . . .
>
> (d) States the specific uses and limitations on the types of medical information to be disclosed.
>
> (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
>
> (f) States the name or functions of the persons or entities authorized to receive the medical information.
>
> (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
>
> (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.
>
> (i) Advises the person signing the authorization of the right to receive a copy of the authorization.

Cal. Civ. Code § 56.11.

197. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as implementing a system that discloses patients' PII and PHI. Cal. Civ. Code § 56.36(c).[42] Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise

[42] "Every provider of health care . . . who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Cal. Civ. Code § 56.101(a).

accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

198. In addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning them in violation of Part 2 of the CMIA for either or both of the following: (1) nominal damages of one thousand dollars ($1,000) (it is not necessary that the patient suffered or was threatened with actual damages); and (2) the amount of actual damages, if any, sustained by the patient. Cal. Civ. Code § 56.36(b).

199. The CMIA prohibits health care providers from disclosing medical information relating to their patients without a patient's authorization. Medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care… regarding a patient's medical history, mental or physical condition, or treatment." 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual..." Cal. Civ. Code § 56.05.

200. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

201. Plaintiffs and Class Members are patients of Defendant and, as health care providers, Defendant has an ongoing obligation to comply with the CMIA's requirements with respect to Plaintiffs' and Class Members' confidential medical information.

202. As set forth above, names, addresses, telephone numbers, email addresses, device identifiers, web URLs, IP addresses, and other characteristics that can uniquely identify Plaintiffs and Class Members are transmitted to, and viewed by, Facebook and Google in combination with patient medical conditions, medical concerns, treatment(s) sought by the patients, medical appointments, medical

specialty of the doctor(s) searched for by patients, prescription drug information and queries, and specific diagnoses and treatment plans available on Defendant's website. This protected health information and personally identifiable information constitutes confidential information under the CMIA.

203. The FID is also an identifier that allows identification of a particular individual. Along with patients' confidential Private Information, Defendant discloses its patients' FIDs to Facebook.

204. Pursuant to the CMIA, the information communicated to Defendant and disclosed to Facebook constitutes medical information because it is patient information derived from a health care provider regarding patients' medical treatment and physical condition and is received by Facebook in combination with individually identifying information. Cal. Civ. Code § 56.05(i).

205. As set forth above, Facebook views, processes, and analyzes the confidential medical information it receives via the Facebook Pixel, Conversions API, cookies, and other Facebook business tools. Facebook then uses the viewed confidential information to create Audiences for advertising and marketing purposes.

206. Defendant failed to obtain Plaintiffs' and Class Members' authorization for the disclosure of medical information.

207. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must: (1) be "clearly separate from any other language present on the same page and … executed by a signature which serves no other purpose than to execute the authorization;" (2) be signed and dated by the patient or their representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. The information set forth on Defendant's Website, including the Website Privacy Policy and Notice of Privacy Practices, does not qualify as a valid authorization.

208. Defendant violated the CMIA by disclosing its patients' medical information to Facebook along with the patients' individually identifying information.

209. Plaintiffs and Class Members seek nominal damages, compensatory damages, punitive damages, attorneys' fees, and costs of litigation for Defendant's violations of the CMIA.

THIRD CAUSE OF ACTION
Violation of the Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq.*

210. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

211. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

212. Defendant engaged in unlawful business practices in connection with its disclosure of Plaintiffs' and Class Members' Private Information to unrelated third parties, including Facebook, in violation of the UCL.

213. The acts, omissions, and conduct of Defendant as alleged therein constitute "business practices" within the meaning of the UCL.

214. Defendant violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiffs' and Class Members' constitutional rights to privacy, state and federal privacy statutes, and state consumer protection statutes.

215. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged therein, offended public policy (including the federal and state privacy statutes and state consumer protection statutes, such as CIPA) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and

Class Members.

216. The harm caused by the Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests other than Defendant's conduct described therein.

217. As result of Defendant's violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant for services and/or other valuable consideration, *e.g.*, access to their private and personal data. Plaintiff and Class Members would not have used Defendant's services, or would have paid less for them, had they known the Defendant was breaching confidentiality and disclosing their Private Information to third parties such as Facebook.

218. The unauthorized access to Plaintiffs' and Class Members' private and personal data also has diminished the value of that information.

219. In the alternative to those claims seeking remedies at law, Plaintiffs and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices. Further, no private legal remedy exists under HIPAA. Therefore, Plaintiffs and members of the proposed Class are entitled to equitable relief to restore Plaintiffs and Class Members to position they would have been in had Defendant not engaged in unfair competition, including restitution and disgorgement of all profits paid to Defendant because of its unlawful and unfair practices.

FOURTH CAUSE OF ACTION
Common Law– Breach of Confidence

220. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

221. Plaintiffs and Class Members disclosed in confidence their health and private information with the Defendant through the Defendant's Website.

222. Plaintiffs and Class Members have an interest in keeping their protected private and medical information in confidence with their health services provider, the Defendant.

223. The information disclosed in confidence is protected health and private information the Defendant had knowledge was confidential due to Federal and State laws that protect such information (i.e., CIPA, CMIA, and HIPAA).

224. Plaintiffs and Class Members had an expectation that the confidential information disclosed to Defendant would be kept in confidence with Defendant due to their relationship with Defendant as a health services provider and Federal and State laws that protect such information (i.e., CIPA and HIPAA).

225. Defendant violated Defendant's duty to protect the confidentiality of Plaintiffs' and Class Members' information by using Facebook's Pixel to communicate patients' FIDs and other individually identifying information alongside their confidential medical communications with third parties, including Facebook.

226. Defendant disclosed Plaintiffs' and Class Members' confidential information for Defendant's own economic benefit in Defendant's own business and disclosed it without Plaintiffs' and Class Members' consent.

227. At no time did Defendant offer to purchase or financially compensate Plaintiffs and Class Members for the use of their confidential information for Defendant's advertisement purposes.

228. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to a breach of their confidence.

229. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's breach of their confidence and are entitled to just

compensation, including monetary damages.

230. Plaintiffs also seek such other relief as the Court may deem just and proper.

FIFTH CAUSE OF ACTION
Invasion of Privacy Under California's Constitution

231. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

232. Plaintiffs and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites for the provision of health care without being subjected to wiretaps without Plaintiffs' and Class Members' knowledge or consent.

233. At all relevant times, by using Facebook's Pixel to communicate patients' FIDs and other individually identifying information alongside their confidential medical communications, Defendant intentionally invaded Plaintiffs' and Class Members' privacy rights under the California Constitution.

234. Plaintiffs and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential, and that Defendant would not install wiretaps on its Website to secretly transmit their communications to a third party.

235. Plaintiffs and Class Members did not authorize Defendant to transmit Plaintiffs' and Class Members' private medical communications alongside their personally identifiable health information to Facebook or to allow Facebook to intercept, receive, and view those communications.

236. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right.

237. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

238. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

239. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests because of its intrusions upon Plaintiffs' and Class Members' privacy.

240. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant's from engaging in such conduct in the future.

241. Plaintiffs also seek such other relief as the Court may deem just and proper.

SIXTH CAUSE OF ACTION
Common Law Invasion of Privacy – Intrusion Upon Seclusion

242. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

243. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communications

platforms and services therein.

244. Plaintiffs and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended only for Defendant to receive and that they understood Defendant would keep private.

245. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

246. Defendant's conduct is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion because Defendant facilitated third parties' simultaneous eavesdropping and wiretapping of confidential communications.

247. Plaintiffs and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential, and that Defendant would not install wiretaps on its Website to secretly transmit their communications to unauthorized third parties.

248. Defendant was authorized to obtain Private Information from Plaintiffs' and Class Members' web browsers for itself but was not authorized to force Plaintiffs' and Class Members' web browsers to transmit information to Facebook, Google, and/or other third parties without their consent or authorization.

249. Defendant therefore obtained Plaintiffs' and Class Members' Private Information under false pretenses and/or exceeded its authority to obtain the Private Information.

250. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

251. Plaintiffs and Class Members have been damaged as a direct and

proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

252. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests because of its intrusions upon Plaintiffs' and Class Members' privacy.

253. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant's from engaging in such conduct in the future.

254. Plaintiffs also seek such other relief as the Court may deem just and proper.

SEVENTH CAUSE OF ACTION
Negligence

224. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

225. Plaintiffs and Class Members entrusted their sensitive and protected medical information and individually identifiable information to Defendant.

226. Defendant had a duty to safeguard and protect Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information from unauthorized third parties.

227. Defendant maintained a duty to safeguard Plaintiffs' and Class Members' sensitive and protected medical information and identifiable information under its obligations to protect personally identifying health information as outlined by the statutory obligations for HIPAA and regulations from HHS.

228. Defendant maintained a duty to safeguard Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information as part of Facebook's Pixel policy to only share information with Facebook that Defendant has the right to collect, use, and share.[43]

229. Defendant maintained a duty to inform Plaintiffs and Class Members of a breach and disclosure of their protected medical information under federal laws like HIPAA and FTC that require notification of a health data breach.

230. Defendant could have configured the Facebook Pixel and other software to not record, track, and transmit Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information.

231. Defendant breached its duty to notify patients of a data breach when it failed to send a timely letter informing patients of the nature and scope of the information in the hands of third parties as required by federal law.

232. Defendant breached its duty to safeguard Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information when Defendant failed to properly configure the Facebook Pixel in a way that would not record, track, and transmit such information, thereby causing Plaintiffs' and Class Members' protected medical information and individually identifiable information to be recorded, tracked, and transmitted to Facebook and Google.

233. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

---

[43] "We require partners to have the right to collect, use and share your information before giving it to us." *Information from partners, vendors and other third parties*, FACEBOOK, https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors (last visited October 31, 2023).

234. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's negligence and are entitled to just compensation, including monetary damages.

235. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests because of its breach of duty to safeguard sensitive and protected information.

236. Plaintiffs also seek such other relief as the Court may deem just and proper.

EIGHTH CAUSE OF ACTION
Breach of Implied Contract

237. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

238. Plaintiffs and Class Members delivered their sensitive and protected medical information and individually identifiable information to Defendant as part of the process of obtaining medical services provided by Defendant.

239. Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to only provide their personally identifiable information to "other parties within the Scripps family for marketing, advertising or other similar uses."[44] Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiffs' and Class Member's data in a manner which comported with the *Privacy Policy*.

240. In providing their sensitive and protected medical information and individually identifiable information, Plaintiffs and Class Members entered an

[44] *Supra* fn. 14.

implied contract with Defendant whereby Defendant, in receiving such data, became obligated to only share Plaintiffs' and Class Member's sensitive and protected medical information and individually identifiable information in a manner that comports with the *Privacy Policy*.

241. In delivering their sensitive and protected medical information and individually identifiable information to Defendant, Plaintiffs and Class Members intended and understood that Defendant would only share their information in a manner that comported with the *Privacy Policy*.

242. Plaintiffs and the Class Members would not have entrusted their sensitive and protected medical information and individually identifiable information to Defendant in the absence of such an implied contract.

243. Defendant accepted possession of Plaintiffs' and Class Members' personal data for the purpose of providing medical services to Plaintiffs and Class Members.

244. Had Defendant disclosed to Plaintiffs and Class Members that Defendant would be sending their sensitive and protected medical information and individually identifiable information to Facebook and Google, and that Defendant did not intent to comply with the provisions of the *Privacy Policy*, Plaintiffs and members of the Class would not have provided their information to Defendant.

245. Defendant recognized that its patient's sensitive and protected medical information and individually identifiable information is highly sensitive and must not be shared with unauthorized third parties, and that this obligation was of material importance as part of the bargain to Plaintiffs and Class Members.

246. Plaintiffs and the Class fully performed all their obligations under the implied contract with Defendant.

247. Defendant breached the implied contract with Plaintiffs and Class Members by failing to adhere to the *Privacy Policy* when it shared Plaintiffs' and

Class Members' sensitive and protected medical information and individually identifiable information with Facebook and Google.

248. Defendant breached the implied contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and acquisition of their sensitive and protected medical information and individually identifiable information by Facebook and Google.

249. As a direct and proximate result of Defendant's breach of its contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, unlawful transmission, and unauthorized use of Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information; (c) economic costs associated with the time spent in response to Defendant's unlawful transmission of their information, including loss of productivity; (d) monetary costs associated with Defendant's unlawful transmission of their information; (e) economic costs, including time and money, related to incidents stemming from Defendant's unlawful transmission of their information; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their sensitive and protected medical information and individually identifiable information; (g) the diminution in the value of the services bargained for, as Plaintiffs and Class Members were deprived of the data protection, security, and information transmission practices that Defendant promised when Plaintiffs and Class Members entrusted Defendant with their sensitive and protected medical information and individually identifiable information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information, which remains in the Defendant's possession with inadequate measures to protect such information.

NINTH CAUSE OF ACTION
Breach of Contract

250. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

251. Plaintiffs and Class Members provided their sensitive and protected medical information and individually identifiable information to Defendant as part of the process of obtaining medical services provided by Defendant.

252. As alleged herein and above, Plaintiffs and Class Members entered into contracts with Defendant under which Defendant agreed to only provide personally identifiable information to "other parties within the Scripps family for marketing, advertising or other similar uses."[45] Each such contractual relationship imposed on Defendant an obligation which required Defendant to perform their obligations and protect Plaintiffs' and Class Member's sensitive and protected medical information and individually identifiable information, and to only share such information in a manner which comported with Defendant's *Privacy Policy*.[46]

253. In providing their sensitive and protected medical information and individually identifiable information, Plaintiffs and Class Members entered a contract with Defendant whereby Defendant, in receiving such data, became obligated to protect Plaintiffs' and the other Class Members' information, and to only share such information in a manner which comported with Defendant's *Privacy Policy*.

254. In delivering their sensitive and protected medical information and individually identifiable information to Defendant, Plaintiffs and Class Members intended and understood that Defendant would only share their information in

---

[45] *Supra* fn. 14.
[46] *Id.*

compliance with Defendant's *Privacy Policy*.

255. Plaintiffs and the Class Members would not have entrusted their sensitive and protected medical information and individually identifiable information to Defendant in the absence of such a contract.

256. Defendant accepted possession of Plaintiffs' and Class Members' personal and medical data for the purpose of providing medical services to Plaintiffs and Class Members.

257. Had Defendant disclosed to Plaintiffs and Class Members that Defendant would be sending their sensitive and protected medical information and individually identifiable information to Facebook and Google, and that Defendant did not intent to comply with the provisions of the *Privacy Policy*, Plaintiffs and members of the Class would not have provided their information to Defendant.

258. Defendant recognized that its patient's sensitive and protected medical information and individually identifiable information is highly sensitive and must not be shared with unauthorized third parties, and that this obligation was of material importance as part of the bargain to Plaintiffs and Class Members.

259. Plaintiffs and the Class fully performed all their obligations under the contract with Defendant.

260. Defendant breached the contract with Plaintiffs and Class Members by failing to adhere to the *Privacy Policy* when it shared Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information with Facebook and Google.

261. Defendant breached the contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and acquisition of their sensitive and protected medical information and individually identifiable information by Facebook and Google.

262. As a direct and proximate result of Defendant's breach of its contractual

duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, unlawful transmission, and unauthorized use of Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information; (c) economic costs associated with the time spent in response to Defendant's unlawful transmission of their information, including loss of productivity; (d) monetary costs associated with Defendant's unlawful transmission of their information; (e) economic costs, including time and money, related to incidents stemming from Defendant's unlawful transmission of their information; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their sensitive and protected medical information and individually identifiable information; (g) the diminution in the value of the services bargained for, as Plaintiffs and Class Members were deprived of the data protection, security, and information transmission practices that Defendant promised when Plaintiffs and Class Members entrusted Defendant with their sensitive and protected medical information and individually identifiable information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information, which remains in the Defendant's possession with inadequate measures to protect such information.

TENTH CAUSE OF ACTION
Violations of Electronic Communications Privacy Act ("ECPA")
18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use, and Disclosure

263. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

264. The ECPA protects both sending and receipt of communications.

265. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

266. The transmissions of Plaintiffs' PII and PHI to Defendant's website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

267. **Electronic Communications.** The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

268. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include [] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

269. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents…include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

270. **Electronic, Mechanical, or Other Device.** The ECPA defines "electronic, mechanical, or other device" as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's webservers; and

d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications.

271. By utilizing and embedding the Pixel on its website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

272. Specifically, Defendant accepted Plaintiffs' and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' PII to Facebook. Indeed, by Defendant's action of embedding the Pixel on its website, which Defendant knew would track, store, and unlawfully transmit Plaintiffs' and Class Members' PII to Facebook, Defendant procured Facebook to intercept Plaintiffs and Class Members' electronic communications. *See* 18 U.S.C. § 2511(1)(a).

273. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

274. By intentionally disclosing or endeavoring to disclose the electronic communications of the Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

275. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

276. **Unauthorized Purpose.** Defendant intentionally intercepted, and procured Facebook to intercept or endeavor to intercept, the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

277. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain including but not limited to using the tracked PII and PHI to target Plaintiffs and Class Members with advertisements on Facebook and other third-party platforms for marketing and retargeting purposes.

278. Defendant was not acting under color of law to intercept or procure Facebook or any other third-party platform to intercept or endeavor to intercept, Plaintiffs and the Class Member's wire or electronic communications.

279. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy by transmitting their PII and PHI via the Pixel to Facebook or any other third-party platforms.

280. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

281. In transmitting, acquiring, and procuring Facebook to intercept or endeavor to intercept the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violations of the CIPA, CMIA, and UCL.

ELEVENTH CAUSE OF ACTION

Violation of Title II of the Electronic Communications Privacy Act
Unauthorized Divulgence by Electronic Communications Service
18 U.S.C. § 2702, *et seq*.
Stored Communications Act

297. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

298. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

299. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

300. Defendant intentionally procures and embeds various Plaintiffs' PII and PHI through the Pixel used on Defendant's website, which qualifies as an Electronic Communication Service.

301. **Electronic Storage.** ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

302. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's website and files associated with it.

303. When Plaintiffs or Class Members make a website communication the content of that communication is immediately placed into storage and is transmitted to Facebook via the Pixel.

304. Defendant knowingly divulges the contents of Plaintiffs' and Class Members' communications through the Pixel.

305. **Exceptions Do Not Apply.** Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney

> General has determined and certified to Congress satisfies Section 2523."

306. Defendant did not divulge the contents of Plaintiffs' and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiffs and Class Members.

307. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

308. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

309. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

310. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

311. Defendant's divulgence of the contents of user communications on Defendant's website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of

their communications; and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

312. Moreover, Defendant divulged the contents of Plaintiffs and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

313. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

314. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs and Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:

D. For an award of damages, including, but not limited to, actual,

consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Respectfully Submitted,

DATE: December 4, 2023

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

s/Rachele R. Byrd
RACHELE R. BYRD

RACHELE R. BYRD (190634)
ALEX J. TRAMONTANO (276666)
FERDEZA ZEKIRI (335507)
750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599
byrd@whafh.com
tramontano@whafh.com
zekiri@whafh.com

M. ANDERSON BERRY (262879)
GREGORY HAROUTUNIAN (330263)
BRANDON P. JACK (325584)
CLAYEO C. ARNOLD A PROFESSIONAL CORPORATION
6200 Canoga Avenue, Suite 375
Woodland Hills, CA 91367
Tel: (747) 777-7748
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

John J. Nelson (317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760

San Diego, CA 92101
Telephone: (858) 209-6941
Email: *jnelson@milberg.com*

Counsel for Plaintiffs and the Proposed Class

29838

ClassAction.org