Vess A. Miller (278020)
Natalie A. Lyons (293026)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
(317) 636-2593 (facsimile)
nlyons@cohenandmalad.com
vmiller@cohenandmalad.com

Matthew J. Langley (SBN 342846)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
t: 312-576-3024
matt@almeidalawgroup.com

J. Gerard Stranch, IV*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Andrew G. Gunem (354042)
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
andrew@straussborrelli.com

*To move for *pro hac vice* admission

Counsel for Plaintiffs and the Proposed Class

SUPERIOR COURT FOR THE STATE OF CALIFORNIA
FOR THE COUNTY OF SAN DIEGO

JANE DOE No, 1, JANE DOE No. 2, JANE DOE No. 3, B.W., B.A., and B.B., Individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

SAN DIEGO FERTILITY CENTER MEDICAL GROUP, INC. d/b/a SAN DIEGO FERTILITY CENTER

Defendants.

Case No. 37-2024-00006118-CU-BC-CTL

SECOND AMENDED CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF BASED ON:

(1) Negligence
(2) Invasion of Privacy
(3) Breach of Implied Contract
(4) Unjust Enrichment
(5) Breach of Fiduciary Duty
(6) Violation of the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq.*
(7) Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101
(8) Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502
(9) Violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(10) Electronic Communications Privacy Act 18 U.S.C. § 2511(1), *et seq.*

(11) Violation of Cal. Cons. Art. § 1
(12) Larceny/Receipt of Stolen Property in Violation of Cal. Pen. Code. § 496(a) & (c)

JURY TRIAL DEMANDED

AMENDED CLASS ACTION COMPLAINT

Plaintiffs, JANE DOE no. 1, JANE DOE no. 2, JANE DOE no. 3, B.W., B.A., and B.B., individually, on behalf of themselves, and all others similarly situated, (hereinafter "Plaintiffs") bring this Amended Class Action Complaint against Defendants, SAN DIEGO FERTILITY CENTER MEDICAL GROUP, INC. d/b/a SAN DIEGO FERTILITY CENTER ("SDFC") and IVY FERTILITY SERVICES, LLC ("Ivy" and, collectively with SDFC, "Defendants"), and alleges, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiffs bring this class action to address Defendants' improper practice of disclosing the confidential Personally Identifying Information ("PII")[1] and/or Protected Health Information ("PHI")[2] (collectively, "Private Information") of Plaintiffs and the proposed Class

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are

Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),[3] Google, LLC ("Google"), Microsoft, Inc. ("Microsoft"), X Corp., DoubleClick Ads, PostHog, and potentially others ("the Disclosure") via tracking technologies used on their many clinical websites, portals, and patient appointment webpages (collectively, "Web Properties"), associated with various fertility clinics around the country affiliated with Ivy, including the following:

- San Diego Fertility Center – https://www.sdfertility.com/ and https://app.ivyfertility.com/contact-us/sdfc/scheduleconsultation
- Fertility Centers of Orange County – https://fertilitycentersoc.com/iui.html
- Reproductive Partners Medical Group – https://www.reproductivepartners.com/
- Pacific NW Fertility – https://pnwfertility.com/
- Fertility Associates of Memphis – https://www.fertilitymemphis.com/
- Idaho Fertility Center – https://www.idahofertility.com/
- Ivy Fertility – https://www.ivyfertility.com/
- Nevada Center for Reproductive Medicine – https://nevadafertility.com/
- Nevada Fertility Center – https://www.nvfertility.com/
- Utah Fertility Center – https://utahfertility.com/

---

considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). SDFC and the clinics associated with Ivy's Web Properties are clearly "covered entities" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiffs' reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

- Virginia Fertility and IVF – https://www.vafertility.com/

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendants,' that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[4] OCR and FTC agree that such tracking technologies, like those present on Defendants' Web Properties, "can track a user's online activities" and "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."[5] OCR and FTC warn that "[i]mpermissible 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, 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."[6]

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace and denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be

[4] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services (July 20, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last accessed June 26, 2024), **attached as Exhibit A.**
[5] *Id.*
[6] *Id*.

less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 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 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.

5. In December 2022, HHS released a bulletin on its website regarding the use of tracking technologies by entities covered by HIPAA—healthcare entities like Defendant—and its business associates (the "December 2022 Bulletin").[7]

6. Therein, HHS defined tracking technologies, explaining:

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors.[8]

[7] *See* archived version of the December 2022 Bulletin at *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS.gov (Dec. 1, 2022), https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed June 26, 2024).
[8] *Id*.

7. In the Bulletin, HHS was clear in unambiguous terms 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.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[9,10]

8. On March 18, 2024, HHS updated its December 2022 bulletin, "to increase clarity for regulated entities and the public" and reiterating the above basic privacy obligations.[11,12]

9. Based in San Diego, California, SDFC is a medical provider which "for over 20 years" has provided fertility treatment to "patients across California, the US, and the entire world[,]" and "a leading destination for fertility tourism and travel."[13]

10. Defendant Ivy Fertility, is "an internationally recognized network of fertility clinics, offers advanced reproductive technologies across the United States," including California.[14]

11. Despite their unique position as trusted healthcare providers, Defendants knowingly configured and implemented into their Web Properties code-based tracking devices

---

[9] *Id*. (bold emphasis in original)
[10] Citing *to* 45 CFR 164.508(a)(3); s*ee also* 45 CFR 164.501 (definition of "Marketing").
[11] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022, updated Mar. 18, 2024), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last acc. June 26, 2024).
[12] On June 20, 2024, in *American Hospital Association, et al. v. Xavier Becerra, et al.,* Case No. 4:23-cv-01110-P (N.D. Tx., Jun. 20, 2024, Doc. 67), the U.S. District Court for the Northern District of Texas vacated HHS's March 14, 2024 Bulletin as to the "Proscribed Combination," *but* acknowledged that the Proscribed Combination could be PHI in certain circumstances.
[13] San Diego Fertility Center, https://www.sdfertility.com/ (last accessed June 26, 2024).
[14] *See* https://www.ivyfertility.com/about (last visited Jan. 31, 2024).

known as "trackers" or "tracking technologies," which collected and transmitted patients' Private Information to Facebook, and other third parties, without patients' knowledge or authorization.

12. Defendants encourage patients to use their Web Properties, along with their various web-based tools and services (collectively, the "Online Platforms"), to learn about Defendants on their website pages to search for medical conditions, symptoms, and treatment options,[15] to find treatment services,[16] to schedule appointments,[17] to search for fertility treatment doctors,[18] to pay bills[19] and more.

13. Plaintiffs and the Class Members visited Defendants' Web Properties and Online Platforms in relation to their past, present, and future health, healthcare and/or payment for health care.

14. When Plaintiffs and Class Members used Defendants' Web Properties and Online Platforms, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendants embedded pixels from Facebook and others into their Web Properties and Online Platforms, surreptitiously forcing Plaintiffs and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

15. A tracker (also referred to as "tracking technology") is a snippet of code embedded

---

[15] E.g., search for "anxiety," avail. at https://www.sdfertility.com/search?q=anxiety (last acc. June 26, 2024).

[16] E.g., "Fertility Treatments," "IUI: Intrauterine Insemination," avail. at https://www.sdfertility.com/fertility-treatments/iui (last acc. June 26, 2024).

[17] "Appointments," available at https://app.ivyfertility.com/contact-us/sdfc?_ga=2.68613777.1256896430.1704726226-1089803368.1704491289&_gl=1*1cm04aj*_ga*MTA4OTgwMzM2OC4xNzA0NDkxMjg5*_ga_N3DJ2SLYBQ*MTcwNDgxODcxMi41LjEuMTcwNDgyMDEzNS41OS4wLjA. (last acc. June 26, 2024).

[18] "Why SDFC," "Meet Our Fertility Doctors," avail. at https://www.sdfertility.com/why-sdfc/fertility-doctor (last acc. June 26, 2024).

[19] https://www.sdfertility.com/fertility-financing/pay-your-bill-online?amount= (last acc. June 26, 2024).

into a website that tracks information about its visitors and their website interactions.[20] When a person visits a website with an tracker, it tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[21] Then, the tracker transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[22]

16. Among the trackers Defendants embedded into the Web Properties is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a Web Properties user's device and the URLs and domains they visit.[23] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[24] Additionally, the Meta Pixel can link a visitor's Web Properties interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[25]

17. Operating as designed and as implemented by Defendants, the Meta Pixel allowed Defendants to unlawfully disclose Plaintiffs' and Class Members' private health information,

---

[20] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

[21] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).

[22] *Id.*

[23] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).

[24] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).

[25] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

alongside identifying details to Facebook. By installing the Meta Pixel on the Web Properties, Defendants effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

18. Facebook encourages and recommends use of its Conversions Application Programming Interface ("CAPI") alongside use of the Meta Pixel.[26]

19. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interactions from the website owner's private servers, which transmits the data directly to Facebook, without involvement from the website user's browser.[27, 28]

20. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendants to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly. For this reason, 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 better understand how digital advertising

---

[26] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[27] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[28] "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." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

impacts both online and offline results."[29]

21. Defendants utilized data from these trackers to market their services and bolster their profits. Facebook utilizes data from the Meta Pixel and CAPI to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells for profit.

22. The information that Defendants' Meta Pixel, and possibly CAPI, sent to Facebook included the Private Information that Plaintiffs and the Class Members submitted to Defendants' Web Properties including, *inter alia*,: the pages they viewed, the buttons they clicked, information regarding users' keyword searches, their appointment activities, their browsing details, bill pay activities, as well as identifying information, including IP address information and the "c_user" cookie which Facebook uses to identify users.

23. Such information allows third parties (e.g., Facebook) to learn of a particular individual's health conditions and seeking of medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers, who then target Plaintiffs and Class Members with online advertisements, based on the information they communicated to Defendants via the Web Properties. Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

24. In addition to the Facebook Pixel, and likely CAPI, on information and belief, Defendants installed other tracking technologies, which operate similarly to the Meta Pixel and transmitted Plaintiffs' and Class Members' Private Information to unauthorized third parties.

[29] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

25. Healthcare patients simply do not anticipate that their trusted healthcare provider will send their private health information to a hidden third party—let alone Facebook, a company with a sordid history of violating consumer privacy in pursuit of ever-increasing advertising revenue.

26. Neither Plaintiffs nor any Class Member signed a written authorization permitting Defendants to send their Private Information to Facebook or other third parties uninvolved in their treatment.

27. Despite willfully and intentionally incorporating the Meta Pixel, potentially CAPI, and other third-party trackers into their Web Properties and servers, Defendants has never disclosed to Plaintiffs or Class Members that they shared their Private Information with Facebook, Microsoft, Inc. ("Microsoft"), X Corp., DoubleClick Ads, PostHog, and possibly others.

28. Defendants further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendants.

29. Defendants owed common law, contractual or equitable, statutory, and regulatory duties to keep Plaintiffs' and Class Members' communications and Private Information safe, secure, and confidential.

30. Upon information and belief, Defendants utilized the Meta Pixel and other tracker data to improve and to save costs on their marketing campaigns, improve their data analytics, attract new patients, and generate sales.

31. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and to safeguard their information from unauthorized disclosure.

32. Defendants breached their common law, contractual or equitable, and statutory obligations to Plaintiffs and Class Members by, *inter alia*, (i) failing to adequately review their marketing programs and web-based technology to ensure their Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiffs' and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiffs and Class Members; and (vii) otherwise failing to design and monitor their Web Properties to maintain the confidentiality and integrity of patient Private Information.

33. Plaintiffs seek to remedy these harms and brings causes of action for (I) Negligence; (II) Invasion of Privacy; (III) Breach of Implied Contract; (IV) Unjust Enrichment; (V) Breach of Fiduciary Duty; (VI) Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq.*; (VII) Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101; (VIII) Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and, (IX) Violation of Cal. Bus. & Prof. Code §§ 17200, *et. seq*.

PARTIES

34. Plaintiff Jane Doe No. 1 is a natural person and resident of the city of San Diego in San Diego County, California.

35. Plaintiff, Jane Doe No. 2, is a natural person and resident and citizen of the State of

California, where she intends to remain, with a principal residence in Lakeside, California in San Diego County. She is a patient of Defendants and victim of their unauthorized Disclosure of Private Information.

36. Plaintiff Jane Doe No. 3, is a natural person and resident and citizens of the State of California, where she intends to remain, with a principal residence in San Diego County.

37. Plaintiff B.W. is a natural person and resident of the city of San Diego in San Diego County, California.

38. Plaintiff B.A. is a natural person and resident of the city of Draper, Utah.

39. Plaintiff B.B. is a natural person and resident of the city of Idaho Falls, Idaho.

40. Defendant San Diego Fertility Center Medical Group, Inc., d/b/a San Diego Fertility Center, is a corporation organized and existing under the laws of the State of California with its principal place of business located at 11425 El Camino Real, San Diego, California 92130 in San Diego County.

41. Defendant Ivy Fertility is a Delaware corporation with its principal place of business and corporate headquarters at 16870 West Bernardo Drive, Suite 120, San Diego, California in San Diego County.

42. Defendants are jointly engaged in the business of providing fertility health care in the Sate of California at Defendants' facilities in San Diego, California.

JURISDICTION AND VENUE

43. The Court has personal jurisdiction over Defendants because Defendants reside in and/or do business in the State of California.

44. This is a class action brought pursuant to Cal. Civ. Proc. Code § 382, and this Court has jurisdiction over the Plaintiffs' claims because the amount in controversy exceeds this Court's

jurisdictional minimum.

45. Venue is proper under Cal. Civ. Proc. Code § 395(a) because Defendant SDFC resides in this County.

COMMON FACTUAL ALLEGATIONS

A. Background

46. At their clinics, Defendants provide fertility treatment services, including infertility diagnosis and testing;[30] Intrauterine Insemination;[31] INVOcell;[32] In-Vitro Fertilization ("IVF"),[33] Natural IVF/Mini IVF,[34] and Intracytoplasmic Sperm Injection (ICSI);[35] eSET[36] and Embryo Grading;[37] Egg donor programs;[38] surrogacy programs, such as Gestational Surrogacy;[39] Genetic Testing;[40] Male Infertility Treatments;[41] Egg Freezing/Fertility Preservation;[42] and LGBT Family Building.[43]

47. Defendants publicizes their "Top Fertility Doctors," as "nationally recognized in

---

[30] https://www.sdfertility.com/fertility-treatments/infertility-diagnosis-testing (last acc. June 26, 2024).
[31] https://www.sdfertility.com/fertility-treatments/iui (last acc. June 26, 2024).
[32] https://www.sdfertility.com/fertility-treatments/invocell (last acc. June 26, 2024).
[33] https://www.sdfertility.com/fertility-treatments/ivf-procedure (last acc. June 26, 2024).
[34] https://www.sdfertility.com/fertility-treatments/ivf-procedure/natural-minimal-stimulation-ivf (last acc. June 26, 2024).
[35] https://www.sdfertility.com/fertility-treatments/ivf-procedure/icsi (last acc. June 26, 2024).
[36] https://www.sdfertility.com/fertility-treatments/eset (last acc. June 26, 2024).
[37] https://www.sdfertility.com/fertility-treatments/eset/embryo-grading (last acc. June 26, 2024).
[38] *See*, e.g., https://www.sdfertility.com/fertility-treatments/egg-donation (last acc. June 26, 2024).
[39] *See*, e.g., https://www.sdfertility.com/fertility-treatments/gestational-surrogacy (last acc. June 26, 2024).
[40] *See*, e.g., Genetic Testing, https://www.sdfertility.com/fertility-treatments/genetic-testing (last acc. June 26, 2024).
[41] https://www.sdfertility.com/fertility-treatments/male-infertility-overview (last acc. June 26, 2024).
[42] https://www.sdfertility.com/fertility-treatments/egg-freezing-fertility-preservation (last acc. June 26, 2024).
[43] https://www.sdfertility.com/fertility-treatments/lgbt-fertility-clinic (last acc. June 26, 2024).

In-Vitro Fertilization (IVF), reproductive endocrinology, and the diagnosis and treatment of infertility."[44]

48. Moreover, Defendants promote the quality of their facilities, including SDFC's Del Mar location, "an achievement in clinical fertility care," which includes:

- A CAP-accredited (College of American Pathologists), state-of-the-art IVF laboratory with a full glass window for viewing.
- A state-of-the-art surgical center that is AAAHC-accredited (Accreditation Association for Ambulatory Health Care) and MediCal certified.
- Two floors of clinic space, with the first floor specially designed for educational enrichment activities and support services for both small and large groups.
- Increased space in exam, consultation, and patient education rooms, that allow for expanded clinical appointment availability.
- Industry leading air handling system and room air monitoring system that offers the most pristine air quality.
- Facilities to accommodate small and large groups for educational enrichment activities, patient education, patient support and enrichment activities.
- Teaching facilities that offer conference and class room space as well as a viewing/window and integrated monitors that allow for observation and collaboration with professional colleges.
- An [sic] beautiful and sunny location in San Diego, California - "America's Finest City".[45]

49. Further still, Defendants promote themselves as having "industry-leading physicians, state-of-the-art laboratories, and a steadfast commitment to the patient experience."[46] And SDFC, one of Ivy's many fertility centers, touts itself as being an "International Destination for Fertility Tourism," or "the practice of traveling for fertility treatment abroad or to another region with the same country. Patients try fertility tourism when they realize that superior treatment and/or superior fertility doctors are available in other regions."[47]

50. Defendants state that "[w]ith exceptional patient care and published IVF success

[44] https://www.sdfertility.com/why-sdfc/fertility-doctor (last acc. June 26, 2024).
[45] https://www.sdfertility.com/why-sdfc/fertility-clinic (last acc. June 26, 2024).
[46] https://www.ivyfertility.com/about (last acc. October 30, 2024)
[47] https://www.sdfertility.com/fertility-tourism (last acc. June 26, 2024).

rates, San Diego Fertility Center is recognized as one of the top fertility clinics worldwide for infertility treatment, including egg donation, IVF, IUI, and surrogacy," touting their San Diego and New York locations, and their international patients from Australia, New Zealand, the United Kingdom, Germany, France, Spain, Canada, Mexico, Brazil, Argentina, China, Korea and more.[48] Altogether, Defendant Ivy purports to have fifty-two physicians across more than twenty-six locations.[49]

51. Defendants serve many of their patients via their Web Properties and Online Platforms, which they encourage patients to use to learn about them on their main website pages,[50] to search for medical conditions, symptoms, and treatment options,[51] to find treatment services,[52] to schedule appointments,[53] to view fertility treatment doctors,[54] and more, including to pay bills.[55]

52. In furtherance of that goal, Defendants purposely installed the Meta Pixel and other trackers onto their Web Properties, for the purpose of gathering information about Plaintiffs and Class Members to further their marketing efforts. But Defendants did not only generate information for their own use: it also shared patient information, including Private Information belonging to Plaintiffs and Class Members, with Facebook, other unauthorized third parties.

---

[48] *Id.*
[49] https://www.ivyfertility.com/about (last acc. October 30, 2024)
[50] E.g., https://www.sdfertility.com/ (last acc. June 26, 2024).
[51] E.g., search for "anxiety," avail. at https://www.sdfertility.com/search?q=anxiety (last acc. June 26, 2024).
[52] E.g., "Fertility Treatments," "IUI: Intrauterine Insemination," avail. at https://www.sdfertility.com/fertility-treatments/iui (last acc. June 26, 2024).
[53] "Appointments," available at https://app.ivyfertility.com/contact-us/sdfc?_ga=2.68613777.1256896430.1704726226-1089803368.1704491289&_gl=1*1cm04aj*_ga*MTA4OTgwMzM2OC4xNzA0NDkxMjg5*_ga_N3DJ2SLYBQ*MTcwNDgxODcxMi41LjEuMTcwNDgyMDEzNS41OS4wLjA. (last acc. June 26, 2024).
[54] "Why SDFC," "Meet Our Fertility Doctors," avail. at https://www.sdfertility.com/why-sdfc/fertility-doctor (last acc. June 26, 2024).
[55] https://www.sdfertility.com/fertility-financing/pay-your-bill-online?amount= (last acc. June 26, 2024).

53. To better understand Defendants' unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

54. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[56]

55. In conjunction with its advertising business, Facebook encourages and promotes its "Business Tools" to be used to gather customer data, identify customers and potential customers, target advertisements to those individuals, and market products and services.

56. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

57. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, clicks a button, fills out a form, and more.[57] Businesses that want to target customers and advertise their services can also create their own tracking parameters by building a "custom event."[58]

58. The Meta Pixel is a Business Tool used to "track[] the people and type of actions

---

[56] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

[57] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[58] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

they take" on a website.[59] When an individual accesses a webpage containing the Meta Pixel, the communications with that webpage are instantaneously and surreptitiously duplicated and sent to Facebook, traveling directly from the user's browser to Facebook's server, based off instructions from the Meta Pixel.

59. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy, such as a homepage, and disable it on pages that do implicate patient privacy, such as Defendants' medical services page.[60]

60. The Meta Pixel's primary purpose is to enhance online marketing, improve online ad targeting, and generate sales.[61]

61. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[62]

62. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** [Emphasis added.]
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
> **Optional Values** – Developers and marketers can optionally choose to send

---

[59] Retargeting, META, https://www.facebook.com/business/goals/retargeting.
[60] E.g., "Fertility Treatments," "IUI: Intrauterine Insemination," avail. at https://www.sdfertility.com/fertility-treatments/iui (last acc. June 26, 2024).
[61] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[62] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.

Form Field Names – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[63]

63. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[64]

64. Facebook likewise benefits from Meta Pixel data and uses it to enhance its own ad targeting abilities.

ii. Defendants' method of transmitting Plaintiffs' and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

65. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (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).

66. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users'

[63] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[64] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

client devices via their web browsers.

67. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[65]

68. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

69. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information. The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

70. 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.

71. 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.

72. In this way, the Meta Pixel acts much like a traditional wiretap: intercepting and transmitting communications intended only for the website host and diverting them to Facebook.

[65] "Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

73. Separate from the Meta Pixel, third parties place cookies in the browsers of web users. These cookies can uniquely identify the user, allowing the third party to track the user as they browse the internet—on the third-party site and beyond. Facebook uses its own cookie to identify users of a Meta-Pixel-enabled website and connect their activities on that site to their individual identity. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the user associated with the information it has intercepted.

74. With substantial work and technical know-how, internet users can sometimes circumvent these browser-based wiretap technologies. To counteract this, third parties bent on gathering data implement workarounds that are difficult for web users to detect or evade. Facebook's workaround is Conversions API, which "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[66] This makes Conversions API a particularly effective tool because it allows sends Facebook data directly from the website server to Facebook, without relying on the user's web browser. Notably, client devices do not have access to host servers containing Conversions API, and thus, they cannot prevent (or even detect) this transmission of information to Facebook.

75. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the website server, Facebook instructs companies like Defendants to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website

[66] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

events [with Facebook] that the pixel may lose."[67] Consequently, if a website owner utilizes the Meta Pixel on its website, it is also reasonable to infer that it implemented the Conversions API on its website server(s), in accordance with Facebook's documentation.

76. The Meta Pixel, Conversions API, and other third-party trackers do not provide any substantive content on the host website. Rather, their only purpose is to collect information to be used for marketing and sales purposes.

77. Accordingly, without any knowledge, authorization, or action by a user, a website owner can use its website source code to commandeer its users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Facebook, and others.

78. In this case, Defendants employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

79. Consequently, when Plaintiffs and Class Members visited Defendants' Web Properties and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

iii. Defendants' Other Trackers: Google Analytics with Google Tag Manager, Facebook Events, Microsoft Universal Events, Twitter Business, DoubleClick Ads, and PostHog.

80. Defendants also employed other trackers such as Google Analytics with Google Tag Manager, Facebook Events, Microsoft Universal Events, Twitter Business, DoubleClick Ads, and PostHog, which, on information and belief, likewise transmitted Plaintiffs' and the Class Members' Private Information to third parties without Plaintiffs' and Class Members' knowledge

[67] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

or authorization.

81. Most basically, "Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business."[68] Once a business implants the Google Analytics tracking measurement code on a its website, every time a user visits a webpage, the tracking code will collect information about how that user interacted with the page.[69]

82. Google Analytics allows businesses like Defendants to track and share with Google (1) who uses its website; (2) what is performed on its website; (3) when users visit its website; (4) where on the website users perform these actions; and (5) how users navigate through the website to perform these actions. Google gathers this information using trackers embedded on Defendants' Web Properties and generates corresponding reports.[70]

83. To help Google generate reports (usually in real time), trackers embedded in a website send Google (1) information about the user's device; (2) client- and user-specific identifiers; and (3) information about what event the user performed.

84. According to Google, "Google Tag Manager is a tag management system (TMS) that allows you to quickly and easily update measurement codes and related code fragments collectively known as ***tags*** on your website or mobile app. Once the small segment of Tag Manager code has been added to your project, you can safely and easily deploy analytics and measurement

[68] Google, *Analytics Help, Introduction to Analytics How Google Analytics works*, avail. at https://support.google.com/analytics/answer/12159447?hl=en&ref_topic=14089939&sjid=3016588406699844463-NC

[69] *Id*.

[70] *See generally*, MarketLyrics, *A big list of what Google Analytics can & cannot do*, avail. at https://marketlytics.com/blog/list-of-things-google-analytics-can-and-cannot-do/

tag configurations from a web-based user interface."[71]

85. As Google goes onto describe:

> When Tag Manager is installed, your website or app will be able to communicate with the Tag Manager servers. You can then use Tag Manager's web-based user interface to set up tags, establish ***triggers*** that cause your tag to fire when certain events occur, and create ***variables*** that can be used to simplify and automate your tag configurations.
>
> A collection of tags, triggers, variables, and related configurations installed on a given website or mobile app is called a ***container***. A Tag Manager container can replace all other manually-coded tags on a site or app, including tags from Google Ads, Google Analytics, Floodlight, and 3rd party tags.[72]

86. Defendants also utilize Microsoft Universal Events, which allows business such as Defendants to "[t]rack what your customers are doing after they click on your ad."[73]

87. As Microsoft goes onto explain, "Universal Event Tracking (UET) is a powerful tool that records what customers do on your website. By creating one UET tag and placing it across your website, Microsoft Advertising will collect data that allows you to track conversion goals and target audiences with remarketing lists."

88. Microsoft touts the benefits of UET as enabling businesses to:

> **Maximize returns**
>
> This approach allows you to optimize the overall value obtained from the conversions you achieve. By incorporating Target Return on Ad Spend (tROAS), you have an extra level of control to ensure that you generate the maximum possible conversion value or revenue while maintaining an adequate return on your ad spend.

---

[71] *See Google Tag Manager Overview,* available at https://support.google.com/tagmanager/answer/6102821?hl=EN#:~:text=Google%20Tag%20Manager%20is%20a,your%20website%20or%20mobile%20app (last acc. June 26, 2024).

[72] *Id*.

[73] *Microsoft Advertising*, available at https://about.ads.microsoft.com/en/tools/performance/conversion-tracking#:~:text=Universal%20Event%20Tracking%20(UET)%20is,target%20audiences%20with%20remarketing%20lists (last acc. June 26, 2024).

Maximize conversions

Focused on achieving the maximum number of conversions within the limits of your budget. By incorporating Target CPA (tCPA), you gain an extra level of control that allows you to optimize the number of conversions while keeping the cost per acquisition at a desired level.

Precise audience targeting

A technique that allows advertisers to reach a specific audience by using a combination of data and technology to deliver personalized messages to the right people. This can be achieved through various methods such as retargeting, contact targeting, and predictive targeting.[74]

89. Defendants also utilizes X Corp.'s Twitter Business tracker, which is a "…platform [which] shows people relevant ads based on how likely they are to engage with the ad and the brand's goals. Further hone in on your audience by using our powerful targeting tools to get your brand and message in front of the right people, when they're most receptive."[75]

90. The Twitter Business tracker can "[u]se demographic targeting to reach people based on location, language, device, age, and gender[,]" as well as "audience targeting to serve ads based on conversations, events, interests, movies and TV shows, keywords, follower look-alikes, and engagement" and targeting audiences to "known audiences, such as your followers and Custom Audiences."[76]

91. Defendants also utilize Double Click Ads. Google's DoubleClick is "an integrated ad technology platform that enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns."[77]

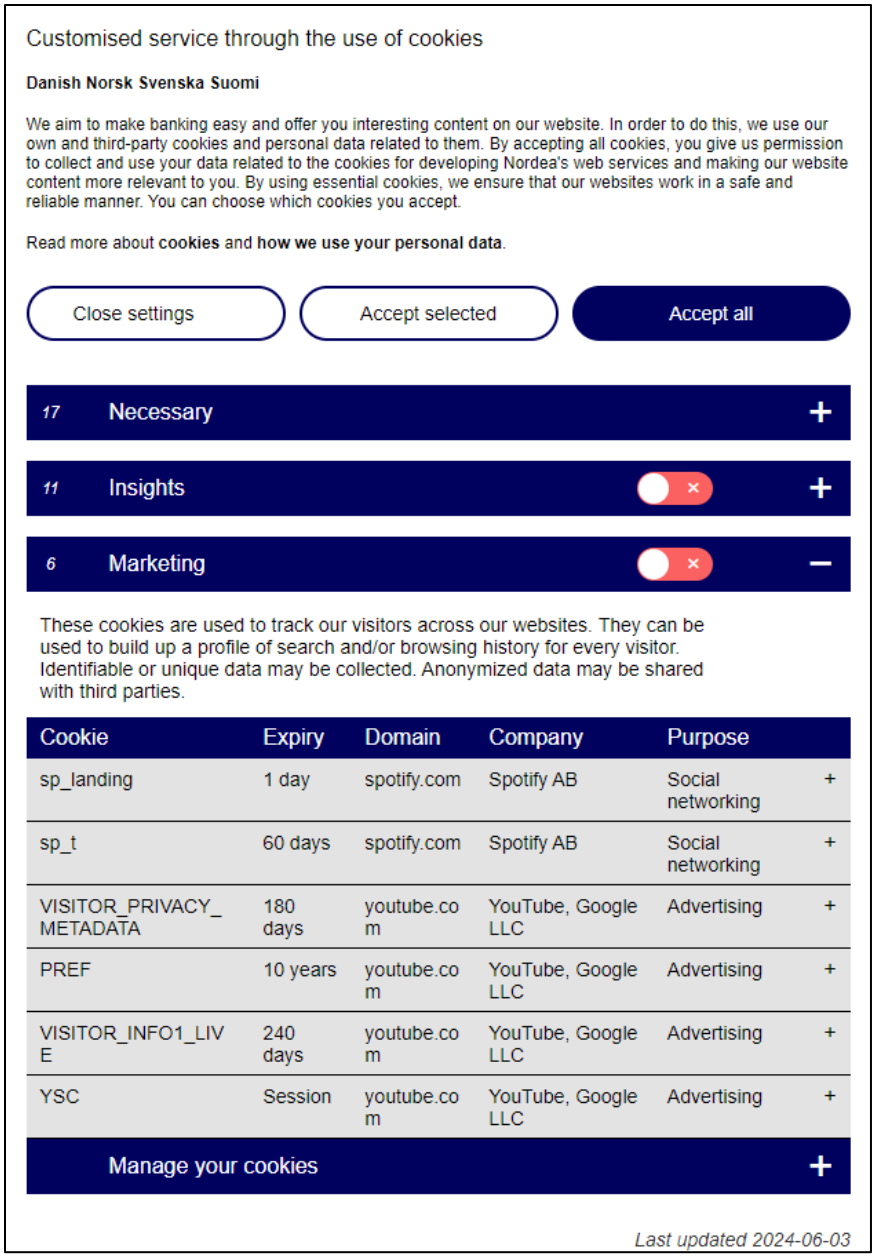
---

[74] *Id*.
[75] Twitter Business, available via Wayback machine at https://web.archive.org/web/20220123055435/https:/business.twitter.com/en/advertising/targeting.html (last acc. June 26, 2024).
[76] *Id*.
[77] Google Help, DoubleClick Digital Marketing, avail. at https://support.google.com/faqs/answer/2727482?hl=en (last acc. June 26, 2024).

92. DoubleClick includes DoubleClick Digital Marketing Manager ("Ad serving and management solutions for your digital advertising campaigns, including trafficking and reporting"), Google Analytics, and more.[78]

93. Information gathered through DoubleClick can be used by Google to personalize the advertisements users are targeted with across the web. *See*, e.g., https://www.nordea.com/en/doubleclick-cookies:

[78] *Id*.



94. Lastly, Defendants utilized PostHog, which allows businesses to "[e]nable aggregate website analytics with one click…"[79] and includes features of: "**Top paths"** to "[s]ee the most visited pages on your site[;]" "**Top referrers"** to "[d]iscover where traffic is coming from[;]" "**Device types"** to "[b]reak down traffic by device[;]" "**World map"** to [v]isualize users across planet earth[;]" "**Retention cohorts**" to "[a]nalyze retention by week[;]" as well as other

[79] https://posthog.com/ (last acc. June 26, 2024).

features such as UTM tracking, Scroll tracking, Bounce tracking, and Duration tracking.[80]

iv. Defendants Violated their own Privacy Policies

95. Defendants Web Properties contain disclaimers and privacy policies posted on and applicable to their Web Properties.[81]

96. For example, SDFC's Privacy Policy states that, "[w]e are committed to respecting your privacy. We urge all users of www.sdfertility.com (the 'Site') to read this Privacy Policy to learn more about the policies and practices that we have developed **to safeguard your personal information**."[82]

97. In this Privacy Policy, Defendants represent, and promise that, "[w]e do not accept or host online advertisement and follow the guidelines set by the American Medical Association (Guidelines for medical and health information sites in the internet. JAMA 2000; 283:1600-6)." [83]

98. Moreover, as follows, Defendants specifically promise patients that, "[w]e do not share tracking information with unaffiliated companies, and we do not allow other companies to place cookies on our Site." [84]

99. In its Privacy Policy, Defendants describes the information they collect on the Web Properties, including information provided on Online Contact Forms, IP Addresses, and Cookies.

100. With respect to information provided on Online Contact Forms, Defendants' Privacy Policy states:

Online Contact Forms

---

[80] PostHog, Web Analytics, avail. at https://posthog.com/web-analytics#features (last acc. June 26, 2024)

[81] E.g., SDFC Disclaimer and Privacy Policy, available at https://www.sdfertility.com/resources/disclaimer (last acc. June 26, 2024) **attached as Exhibit B.**

[82] *Id*. (bold emphasis added)

[83] *Id*.

[84] *Id*.

> You may choose to share information with us through interactive forms on our Web site. **For example, you may submit a request for an appointment to us online through our Web site.** The use of these forms is voluntary and the information you submit is forwarded to representatives of San Diego Fertility Center who are best suited to review and act upon the information provided.
> **We use SSL for the online contact forms, which ensures that all communications between you and our mail server will be encrypted** (https:// instead of http:// in the address bar of contact forms). **Your message contents will be hidden from prying eyes and encryption helps mitigate identity theft, the sending of false messages, etc.** However, since the form messages are transmitted over the Internet, SDFC cannot assure that the messages are completely secure. If you are uncomfortable with such risks, you may decide not to use the online forms to communicate with SDFC. You must be aware that the messages may be delayed or undelivered.[85]

101. In addition, as to IP Addresses, Defendants states in its Privacy Policy, "**IP Address** We record the Internet Protocol (IP) address of your computer when you visit the Site. **The IP address does not identify you personally,** but it is what allows us to maintain communications with you as you move about the Site." [86]

102. Finally with respect to cookies, Defendants state that:

> **Cookies**
>
> We also collect information about your use of the Site through cookies and similar technology. A "cookie" is a unique numeric code that we transfer to your computer so that we can keep track of your interests and preferences and recognize you as a return visitor to the Site. Cookie technology allows us to collect "clickstream" data, which is not personally identifying information, but that which reflects your activities on the Site, including your interest in certain Site categories. **We do not share tracking information with unaffiliated companies, and we do not allow other companies to place cookies on our Site.**[87]

103. Nowhere in Defendants' Privacy Policy do they disclose to patients the use of the Meta Pixel or related tracking technologies nor the disclosure of their Private Information to third parties uninvolved in their fertility medical treatment for marketing purposes, but just the opposite,

[85] *Id*. (bold underline emphasis added)
[86] *Id*. (bold emphasis added)
[87] *Id*. (bold underline emphasis added)

as stated above. The same is true for each Privacy Policy posted to each of Defendants' many Web Properties.

104. In fact, in the SDFC Privacy Policy, Defendants go on to specifically describe how they use Web Properties users' and patients' information, stating, merely, "[w]e use the information about your use of the services and activities on the Site to monitor user traffic patterns and try to analyze what our users prefer so that we can design better services and activities for you."[88]

105. None of the purposes for which Defendants state they may disclose medical information, PHI/Private Information include the unauthorized Disclosure of Private Information for marketing purposes via the Meta Pixel and other tracking technologies that is the subject of this Complaint.

106. Despite these representations in its Privacy Policies, Defendants do indeed transfer Private Information to third parties for marketing purposes, without written authorization. Using the Meta Pixel and other tracking technologies, Defendants used and disclosed Plaintiffs' and Class Member's Private Information and confidential communications to Facebook, and likely other unauthorized third parties such as Google, Microsoft, X Corp., DoubleClick Ads, and PostHog, without written authorization, and in violation of its Privacy Policies.

v. Defendants Unauthorizedly Disclosed Plaintiffs' and the Class's Private Information

107. On information and belief, Defendants disclosed Plaintiffs' and Class Members' Private Information and confidential communications to Facebook via the Meta Pixel and to other third parties such as Google, Microsoft, Inc., X Corp., DoubleClick Ads, and PostHog, via other

[88] *Id*.

tracking technologies, for marketing purposes.

108. Through the use of the Meta Pixel, Defendants disclosed to Facebook the Private Information that Plaintiffs and the Class Members submitted to Defendants' Web Properties including, *inter alia*: the pages they viewed; the buttons they clicked; information regarding users' keyword searches; their appointment activities; their browsing details; bill pay activities; as well as identifying information, including IP address information and the "c_user" cookie which Facebook uses to identify users.

109. Since at least June 2020, Defendants have utilized Meta Pixels on their Online Platforms, at that time employing **Pixel1** which was configured with Advanced Matching Parameters, which "allow Meta to connect collected event data to users, even if they do not have Facebook's browser cookies."[89] Defendants configured Advanced Matching Parameters on Pixel1 to send hashed values of the following user inputted information: email, first name, last name, gender, phone, city, state, and zip code.

110. As of January 16, 2024, Defendants installed a number of Metal Pixels with the following IDs: 951372101648912 ("Pixel1"), 1024940958846869 ("Pixel2"), 239912582243072 ("Pixel3"), 6707064245994307 ("Pixel4"), 1666143710464689 ("Pixel5"), and 305890348536996 ("Pixel6"). Defendants also previously installed another Meta Pixel with the ID 544941696777245 ("Pixel7") as of January 1, 2023.

111. By way of example, through the use of these Meta Pixels, Defendants disclosed the following Private Information of patients, including Plaintiffs and the proposed Class Members, to Facebook.

[89] See https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector#advanced-matching-parameters (last acc. June 26, 2024).

Defendants Disclose the Website Pages Users View

112. Upon a user's arrival on one of the homepages for Defendants Web Properties, for example, Defendants immediately transmit PageView events notifying Facebook that the user is on the page for "sdfertility.com."

113. Historically, Defendants also would have transmitted a Microdata event along with the PageView event. The Microdata event reveals additional information about what the user was viewing. For example, the Microdata event for a visitor to the SDFC website would reveal that the user was learning about SDFC, which is "a leading Southern California fertility clinic for infertility treatment including IVF, egg donation, and surrogacy in San Diego, California."

114. As users move beyond the homepage, Defendants continue to disclose information about the users' browsing details and activities. Through PageView, Microdata, ViewContent, SubscribedButtonClick, and Lead events, Defendants inform Facebook about users': keyword searches; appointment activities; browsing details; and bill pay activities.

Defendants Disclose Users' Keyword Searches

115. Defendants shared details about users' searches. When a user searches for the keyword, IVF, for example, Defendants inform Facebook that the user clicked to search via a SubscribedButtonClick event. Furthermore, Defendants inform Facebook about the user's specific keyword query for "q=ivf" in a PageView event. This occurred on each of Defendants' Web Properties.

116. Historically, Defendants also transmitted a Microdata event along with a PageView event upon the user loading their IVF search results. Through the Microdata event, Defendants inform Facebook that the user was learning about "San Diego Fertility Center's doctors and specialists," who "are leaders in IVF, egg donation, surrogacy, and other female and male

infertility treatments."

117. Defendants not only share users' keywords, but also shares how users interact with their search results. Again, this occurred across Defendants' Web Properties.

118. For instance, when the user loads a page about Defendants' IVF treatment program from their search results page, Defendants send a PageView event revealing the user navigated from their search query for IVF to the page about "fertility-treatments/ivf-procedure."

Defendants Disclose Users' Appointment Activities

119. Defendants inform Facebook about users' appointment activities. Users can fill out an appointment form on Defendants' Web Properties to request an appointment. To navigate to the appointment form, a user can click to open the menu from the homepage and then click on the option for appointments. As a user clicks on each button, Defendants transmit a SubscribedButtonClick event for each.

120. The SubscribedButtonClick events reveals that the user clicked for "MENU" and "APPOINTMENTS," respectively.

121. Next, when the Appointments page opens, Defendants transmit PageView events. In the past, Defendants also transmitted a Microdata event when they sent the PageView event.

122. The user may then fill out their contact information and submit the appointment form to request an appointment. When the user clicks to submit the form, Defendants inform Facebook with Lead and SubscribedButtonClick events. A Lead event indicates to Facebook that "[a] submission of information by a customer with the understanding that they may be contacted at a later date by your business"[90] has occurred.

[90] https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last acc. June 26, 2024).

123. Using the SDFC website as an example, the SubscribedButtonClick event reveals to Facebook that the user clicked to "Submit Message" on a page titled "Start your journey with San Diego Fertility Center." Moreover, Defendants transmit the user's submitted email and phone number in the SubscribedButtonClick event through the udff[em] and udff[ph] parameters. Again, this occurred across Defendants' Web Properties.

Defendants Disclose Users' Browsing Details

124. Defendants share details about users' browsing activities. For example, when a user browses male fertility treatment offered by Defendants, Defendants inform Facebook about those activities.

125. As a user loads the Male Infertility Treatments page, Defendants transmit a Pageview event revealing that the user is on the page for "fertility-treatments/male-infertility-overview." Then, as the user loads another page to learn more about microscopic testicular sperm extraction ("TESE"), Defendants transmit another PageView event, informing Facebook the user navigated from a page about fertility treatments for male infertility to a page about "tese-sperm-extraction."

126. Previously, Defendants would have also sent Microdata events alongside the PageView events as the user opened the pages for male infertility overview and TESE sperm extraction. The Microdata events provide additional information about what the user was viewing. For example, the Microdata event Defendants would have sent upon the user's visit to the sperm extraction page would have revealed that the user was on a page with a video of a "male infertility doctor specialists perform[ing] Microscopic Testicular Extraction (TESE) infertility treatment."

127. Defendants also inform Facebook when users contact each of Defendants' Web Properties.

128. When the user clicks to call SDFC from the male infertility page, for instance, SDFC transmits a Lead event disclosing that the user made a "phone-click" to call SDFC on the page about "fertility-treatments/male-infertility-overview."

Defendants Disclose Users' Bill Pay Activities

129. Moreover, Defendants share details about users' bill pay activities.

130. For example, upon a user's navigation to the Pay Your Bill Online page, SDFC sends a PageView event informing Facebook that the user is on the Pay Your Bill page, which in the case of SDFC is "https://www.sdfertility.com/fertility-financing/pay-your-bill-online."

131. Historically, SDFC would have also sent a Microdata event further revealing that the user was on a page to "Make Payments Online at San Diego Fertility Center®."

132. As the user fills out their information and clicks to make a payment online, SDFC sends a SubscribedButtonClick event to Facebook. The event reveals that the user clicked to "MAKE A SECURE PAYMENT" to the "San Diego Fertility Center." Furthermore, SDFC transmits the hashed values of the user's inputted first name and last name from the payment form.

133. All this occurred across Defendants' Web Properties.

Defendants Disclose Users' Identifying Information

134. Defendants also disclose User's identifying information, on information and belief including their IP addresses.

135. For example, in each of the Meta Pixel events that the Web Properties send to Facebook, the event includes the "c_user" cookie, which Facebook uses to identify users.

136. Facebook could therefore connect cookie data from the Web Properties with specific users. Furthermore, Facebook's "Your activity off Meta technologies" report confirms that Facebook received the data Defendants' Web Properties shared with Facebook.

137. This occurred across Defendants' Web Properties.

vi. Facebook Receives Private Information from Defendants and then Processes It and Sells Access to the Data in the Form of Targeted Advertisements

138. Through the Meta Pixels, Defendants collected and transmitted user interactions with Defendants' Web Properties and sent records of those interactions to Facebook. For example, when a patient visits Defendants' Web Properties and searches for medical information in relation to their past, present, and future health, healthcare and/or payment for health care using the search query, e.g., "fertility treatments," the individual's browser sends a request to Defendants' server requesting that it load the webpage. Then, the Meta Pixel sends secret instructions back to the individual's browser, causing it to imperceptibly record the patient's communication with Defendants and transmit the patient's search query and related information to Facebook's servers, alongside the patient's IP address, and sometimes, the patient's unique Facebook ID. Thus, the patient's search for information related to their healthcare, alongside identifying information is reported back to Facebook, thereby revealing the patient's Private Information.

139. After receiving information from Defendants, Facebook processes it, analyzes it, and assimilates it into its own massive datasets, before selling access to this data in the form of targeted advertisements. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond to your ad."[91] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[92] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app,

[91] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[92] *Id.*

or buying a product bought a product;[93] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[94]

140. Defendants could have chosen not to use the Meta Pixel and other tracking technology, or it could have configured it to limit the information that it communicated to third parties, but it did not. Instead, it intentionally took advantage of these trackers' features and functions, resulting in the Disclosure of Plaintiffs' and Class Members' Private Information.

141. Defendants used and disclosed Plaintiffs' and Class Members' Private Information to Facebook, Google, Microsoft, X Corp., Double Click and Post Hog for the purpose of marketing its services and increasing its profits and reducing its marketing costs.

142. On information and belief, Defendants shared, traded, or sold Plaintiffs' and Class Members' Private Information with Facebook, Microsoft, X Corp., Double Click and Post Hog in exchange for improved targeting and marketing services and reduced marketing costs.

143. Plaintiffs and the Class never consented, agreed, authorized, or otherwise permitted Defendants to intercept their communications or to use or disclose their Private Information for marketing purposes. Plaintiffs and the Class were never provided with any written notice that Defendants disclosed their patients' Protected Health Information to Facebook, Google, Microsoft, X Corp., Double Click and Post Hog nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiffs' Protected Health Information to unauthorized entities.

144. Plaintiffs and Class Members relied on Defendants to keep their Private

[93] *Id.*

[94] How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).

Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

145. Furthermore, Defendants actively misrepresented that they would preserve the security and privacy of Plaintiffs' and Class Members' Private Information. In actuality, Defendants shared data about Plaintiffs' and Class Members' activities on the Online Platforms alongside identifying details about the Plaintiffs and Class Members, such as their IP addresses.

146. By law, Plaintiffs and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. Defendants deprived Plaintiffs and Class Members of their privacy rights when they (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook, Google, Microsoft, X Corp., Double Click, and Post Hog; and (3) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

B. Plaintiff Jane Doe No. 1's Experience

147. Plaintiff Jane Doe No. 1 accessed and used the SDFC Website using her personal phone while located in California to seek medical treatment for infertility starting in September 2017.

148. Plaintiff Jane Doe No. 1 accessed and used the Defendants' Web Properties using her personal phone while located in California to seek medical treatment for infertility starting in September 2017.

149. Jane Doe No. 1 has been a patient of SDFC since September 2017. She set appointments and was treated for fertility issues, including infertility diagnosis and testing.

150. Jane Doe No. 1 began using Defendants' Web Properties in September 2017 to, among other things, look up egg freezing, cost of the egg freezing treatment and insurance options for fertility treatments she was seeking from Defendants, make online appointments at SDFC, and to pay bills for egg freezing and other services she sought from Defendants.

151. Information that Jane Doe No. 1 provided to Defendants via their Web Properties included her personal information such as name, email address, and phone number, as well as her medical history, answers to queries about her medical conditions, and fertility treatments sought such as egg freezing.

152. Jane Doe No. 1 has had an active Facebook account for more than 10 years including during the time she was providing her Private Information to Defendants via their Web Properties.

153. After she provided information to Defendants and looked for egg freezing and other fertility treatments on the SDFC Website, Jane Doe No. 1 began receiving ads for fertility treatments on her Meta accounts (Facebook and Instagram).

154. The amount of ads targeting Plaintiff Jane Doe No. 1 was excessive and overwhelming, causing her extreme emotional distress.

155. Furthermore, Jane Doe No. 1 began to receive phone calls from fertility clinics, including those located in Mexico, on her personal phone number that she provided to Defendants in the process of seeking medical services.

156. These calls were extremely intrusive and exacerbated her emotional distress.

157. Plaintiff Jane Doe No. 1 reasonably expected that her communications with Defendants via the Web Properties were confidential, solely between herself and Defendants, and that such communications would not be transmitted to or intercepted by any third party without

her full knowledge and informed consent.

158. Plaintiff Jane Doe No. 1 provided her Private Information to Defendants and trusted that the information would be safeguarded according to Defendants' policies and state and federal law.

159. As described herein, Defendants worked along with Facebook to intercept Plaintiff Jane Doe No. 1's communications, including those that contained confidential Private Information, while Plaintiff Jane Doe No. 1 was within the state of California.

160. Defendants willfully facilitated these interceptions without Plaintiff Jane Doe No. 1's knowledge, consent, or express written authorization.

161. Within the State of California, Defendants transmitted Plaintiff Jane Doe No. 1's email address, phone number, FID, computer IP address, location, information such as treatment sought, and, upon information and good faith belief, appointment type, physician(s) selected, and medical history to Facebook.

162. By doing so without her consent, Defendants breached Plaintiff Jane Doe No. 1's right to privacy and unlawfully disclosed her Private Information.

163. Defendants did not inform Plaintiff Jane Doe No. 1 that they shared her Private Information with Facebook.

164. Plaintiff Jane Doe No. 1 suffered damages in, inter alia, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

165. Plaintiff Jane Doe No. 1 has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure. Plaintiff Jane Doe

No. 1 wants to continue to communicate with Defendants; healthcare providers through online platforms but has no practical way of knowing if her communications are being intercepted and disclosed to Facebook, and thus continues to be at risk of harm from Defendants' conduct.

166. Plaintiff Jane Doe No. 1's experience is representative of the experience of the Class across Defendants' Web Properties.

C. Plaintiff Jane Doe No. 2's Experience

167. Plaintiff Jane Doe No. 2 has been a patient of SDFC for over five years since September 2018 and has received healthcare services from Defendants and physicians in Defendants' network for In Vitro Fertilization (IVF).

168. Plaintiff Jane Doe No. 2 relied on Defendants' Website and Online Platforms to communicate confidential patient information. She began using the Website and Online Platforms in 2018 and last visited the Website and Online Platforms in Summer of 2022 to research fertility doctors and treatments, such as IVF.

169. Specifically, Plaintiff Jane Doe No. 2 used the Website to view IVF treatments on Defendants' Treatment pages,[95] and to find fertility doctors on the "Why SDFC?," "Fertility Doctors" pages.[96]

170. After using Defendants' Online Platforms, advertisements for Defendants began appearing on Plaintiff Jane Doe No. 2's Instagram account.

171. Plaintiff Jane Doe No. 2 accessed Defendants' Online Platforms at Defendants direction and encouragement in relation to her past, present, and future health and healthcare.

[95] E.g., "Fertility Treatments," "IUI: Intrauterine Insemination," avail. at https://www.sdfertility.com/fertility-treatments/iui (last acc. June 26, 2024).

[96] "Why SDFC," "Meet Our Fertility Doctors," avail. at https://www.sdfertility.com/why-sdfc/fertility-doctor (last acc. June 26, 2024).

172. Plaintiff Jane Doe No. 2 reasonably expected that her online communications with Defendants were confidential, solely between herself and Defendants, and that, as such, those communications would not be transmitted to or intercepted by a third party.

173. Plaintiff Jane Doe No. 2 provided her Private Information to Defendants and trusted that the information would be safeguarded according to Defendants' privacy policies and the law.

174. Through its use of the Meta Pixel, Defendants disclosed to Facebook:

a. The pages Plaintiff Jane Doe No. 2 viewed, including fertility doctors she viewed;

b. Plaintiff Jane Doe No. 2's browsing details, including the medical treatments she viewed;

c. Plaintiff Jane Doe No. 2's seeking of medical treatment;

d. Plaintiff Jane Doe No. 2's status as a patient;

e. Plaintiff Jane Doe No. 2's identity via her IP addresses and/or "c_user" cookie which Facebook uses to identify users.

175. As a result of Defendants' Disclosure of Plaintiff Jane Doe No. 2's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff has suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of her Private Information; unauthorized access of his Private Information by third parties;

b. Plaintiff Jane Doe No. 2 now receives targeted health-related advertisements on Instagram for SDFC, reflecting her private medical treatment information;

c. Plaintiff Jane Doe No. 2 paid Defendants for medical services and the services she paid for included reasonable privacy and data security protections for her Private Information, but Plaintiff Jane Doe No. 2 did not receive the privacy and security protections for which she paid, due to Defendants' Disclosure;

d. The portion of Defendants' revenues and profits attributable to collecting Plaintiff Jane Doe No. 2's Private Information without authorization and sharing it with third parties;

e. The portion of Defendants' savings in marketing costs attributable to collecting Plaintiff Jane Doe No. 2's Private Information without authorization and sharing it with third parties.

f. The portion of Defendants' revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff Jane Doe No. 2 as a result of collecting Plaintiffs' Private Information without authorization and sharing it with third parties;

g. Value to Plaintiff Jane Doe No. 2 to knowingly surrender her choice to keep his Private Information private and allow Defendants to track her data. The amount of these damages can be based on a baseline monthly compensation provided to participants in a Google consumer research study, the Ipsos Screenwise Panel where the baseline compensation to participants was $3 per device per month;

h. Embarrassment, humiliation, frustration, and emotional distress;

i. Decreased value of Plaintiff Jane Doe No. 2's Personal Information

j. Lost benefit of the bargain;

k. Increased risk of future harm resulting from future use and disclosure of her Private Information.

176. Plaintiff Jane Doe No. 2's experience is representative of the experience of the Class across Defendants' Web Properties.

D. Plaintiff Jane Doe No. 3's Experience

177. Plaintiff Jane Doe No. 3 is a patient of SDFC and has received healthcare services from Defendants and physicians in Defendants' network.

178. Plaintiff Jane Doe No. 3 relied on Defendants' Website and Online Platforms to communicate confidential patient information. She used the Website and Online Platforms.

179. After using Defendants' Online Platforms, advertisements for Defendants began appearing on Plaintiff Jane Doe No. 3's social media accounts.

180. Plaintiff Jane Doe No. 3 accessed Defendants' Online Platforms at Defendants direction and encouragement in relation to her past, present, and future health and healthcare.

181. Plaintiff Jane Doe No. 3 reasonably expected that her online communications with Defendants were confidential, solely between herself and Defendants, and that, as such, those communications would not be transmitted to or intercepted by a third party.

182. Plaintiff Jane Doe No. 3 provided her Private Information to Defendants and trusted that the information would be safeguarded according to Defendants' privacy policies and the law.

183. Through its use of the Meta Pixel, Defendants disclosed to Facebook:

a. The pages Plaintiff Jane Doe No. 3 viewed, including fertility doctors she viewed;

b. Plaintiff Jane Doe No. 3's browsing details, including the medical treatments she viewed;

c. Plaintiff Jane Doe No. 3's seeking of medical treatment;

d. Plaintiff Jane Doe No. 3's status as a patient;

e. Plaintiff Jane Doe No. 3's identity via her IP addresses and/or "c_user" cookie which Facebook uses to identify users.

184. As a result of Defendants' Disclosure of Plaintiff Jane Doe No. 3's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff has suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of her Private Information; unauthorized access of his Private Information by third parties;

b. Plaintiff Jane Doe No. 3 now receives targeted health-related advertisements on social media for SDFC, reflecting her private medical treatment information;

c. Plaintiff Jane Doe No. 3 paid Defendants for medical services and the services she paid for included reasonable privacy and data security protections for her Private Information, but Plaintiff Jane Doe No. 3 did not receive the privacy and security protections for which she paid, due to Defendants' Disclosure;

d. The portion of Defendants' revenues and profits attributable to collecting Plaintiff Jane Doe No. 3's Private Information without authorization and sharing it with third parties;

e. The portion of Defendants' savings in marketing costs attributable to

collecting Plaintiff Jane Doe No. 3's Private Information without authorization and sharing it with third parties.

f. The portion of Defendants' revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff Jane Doe No. 3 as a result of collecting Plaintiffs' Private Information without authorization and sharing it with third parties;

g. Value to Plaintiff Jane Doe No. 3 to knowingly surrender her choice to keep his Private Information private and allow Defendants to track her data. The amount of these damages can be based on a baseline monthly compensation provided to participants in a Google consumer research study, the Ipsos Screenwise Panel where the baseline compensation to participants was $3 per device per month;

h. Embarrassment, humiliation, frustration, and emotional distress;

i. Decreased value of Plaintiff Jane Doe No. 3's Personal Information

j. Lost benefit of the bargain;

k. Increased risk of future harm resulting from future use and disclosure of her Private Information.

185. Plaintiff Jane Doe No. 3's experience is representative of the experience of the Class across Defendants' Web Properties.

E. Plaintiff B.W.'s Experience

186. Plaintiff B.W. accessed and used the SDFC Website using her personal phone and tablet while located in California to seek medical treatment for infertility as recently as September 2023

187. B.W. has been a patient of SDFC since approximately September 2023. She was treated for fertility issues, including infertility diagnosis and testing.

188. B.W. began using Defendants' Web Properties in September 2023 to, among other things, look up the cost of treatments and insurance options for fertility treatments she was seeking from Defendants.

189. Information that B.W. provided to Defendants via their Web Properties included queries about her medical conditions as well as for testing and diagnosis for depression, infertility, and her symptoms and treatment for uterine polyps or fibroids (which occur in the endometrium and are associated with endometriosis and infertility).

190. B.W. has had an active Facebook account for more than 10 years including during the time she was providing her Private Information to Defendants via their Web Properties.

191. After she provided information to Defendants and looked for infertility treatments on the Web Properties, B.W. began receiving ads for clinical trials related to endometriosis and fibroids, as well as depression, on her Meta accounts (Facebook and Instagram).

192. Plaintiff B.W. reasonably expected that her communications with Defendants via the Web Properties were confidential, solely between themselves and Defendants, and that such communications would not be transmitted to or intercepted by any third party without her full knowledge and informed consent.

193. Plaintiff B.W. provided her Private Information to Defendants and trusted that the information would be safeguarded according to Defendants' policies and state and federal law.

194. As described herein, Defendants worked along with Facebook to intercept Plaintiff B.W.'s communications, including those that contained confidential Private Information, while Plaintiff B.W. was within the state of California.

195. Defendants willfully facilitated these interceptions without Plaintiff B.W.'s knowledge, consent, or express written authorization.

196. Within the State of California, Defendants transmitted Plaintiff B.W.'s FID, computer IP address, location, information such as treatment sought, and, upon information and good faith belief, appointment type, physician(s) selected, and medical history to Facebook.

197. By doing so without her consent, Defendants breached Plaintiff B.W.'s right to privacy and unlawfully disclosed her Private Information.

198. Defendants did not inform Plaintiff B.W. that they shared her Private Information with Facebook.

199. Plaintiff B.W. suffered damages in, inter alia, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

200. Plaintiff B.W. has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure. Plaintiff B.W. wants to continue to communicate with Defendants; healthcare providers through online platforms but has no practical way of knowing if her communications are being intercepted and disclosed to Facebook, and thus continues to be at risk of harm from Defendants' conduct.

201. Plaintiff B.W.'s experience is representative of the experience of the Class across Defendants' Web Properties.

F. Plaintiff B.A.'s Experience

202. Plaintiff B.A. accessed and used the Utah Fertility Center Website using her personal phone and computer while located in Utah to seek medical treatment for fertility issues

since 2017.

203. Plaintiff B.A. has been a patient of Defendants since 2017. She was treated for fertility issues, including IVF and embryo creation.

204. Plaintiff B.A. began using Defendants' Web Properties in 2017 to, among other things, check lab results, make payments, and research IVF treatment sections.

205. Information that Plaintiff B.A. provided to Defendants via their Web Properties included intake forms containing private medical information including sperm count, modality, and mobility data.

206. Plaintiff B.A. has had an active Facebook account since 2006 including during the time she was providing her Private Information to Defendants via their Web Properties.

207. After she provided information to Defendants and looked for fertility treatments on the Web Properties, Plaintiff B.A. began receiving ads for IVF and surrogacy services on her Meta accounts (Facebook and Instagram).

208. Plaintiff B.A. reasonably expected that her communications with Defendants via the Web Properties were confidential, solely between herself and Defendants, and that such communications would not be transmitted to or intercepted by any third party without her full knowledge and informed consent..

209. Plaintiff B.A. provided her Private Information to Defendants and trusted that the information would be safeguarded according to Defendants' policies and state and federal law.

210. As described herein, Defendants worked along with Facebook to intercept Plaintiff B.A.'s communications, including those that contained confidential Private Information.

211. Defendants willfully facilitated these interceptions without Plaintiff B.A.'s knowledge, consent, or express written authorization.

212. Defendants transmitted Plaintiff B.A.'s FID, computer IP address, location, information such as treatment sought, and, upon information and good faith belief, lab results, medical data, and appointment type to Facebook.

213. By doing so without her consent, Defendants breached Plaintiff B.A.'s right to privacy and unlawfully disclosed her Private Information.

214. Defendants did not inform Plaintiff B.A. that they shared her Private Information with Facebook.

215. Plaintiff B.A. suffered damages in, inter alia, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

216. Plaintiff B.A. has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure. Plaintiff B.A. wants to continue to communicate with Defendants' healthcare providers through online platforms but has no practical way of knowing if her communications are being intercepted and disclosed to Facebook, and thus continues to be at risk of harm from Defendants' conduct.

217. Plaintiff B.A.'s experience is representative of the experience of the Class across Defendants' Web Properties.

G. Plaintiff B.B.'s Experience

218. Plaintiff B.B. accessed and used the Idaho Fertility Center Website using her personal phone and computer to seek medical treatment for fertility issues since 2022.

219. Plaintiff B.B. has been a patient of Defendants since 2022. She was treated for fertility issues, including IUI, egg retrieval, and egg implantation.

220. Plaintiff B.B. began using Defendants' Web Properties in 2022 to, among other things, access payments, send messages to nurses, view her treatment calendar, and research fertility treatments.

221. Information that Plaintiff B.B. provided to Defendants via their Web Properties included comprehensive medical history forms containing previous treatments, infertility issues, and other sensitive medical information.

222. Plaintiff B.B. has had an active Facebook account since 2011 including during the time she was providing her Private Information to Defendants via their Web Properties.

223. After she provided information to Defendants and looked for fertility treatments on the Web Properties, Plaintiff B.B. began receiving ads for Idaho Fertility Center, IVF payment plans, egg storage services, and umbilical cord services on her Meta accounts (Facebook and Instagram).

224. Plaintiff B.B. reasonably expected that her communications with Defendants via the Web Properties were confidential, solely between herself and Defendants, and that such communications would not be transmitted to or intercepted by any third party without her full knowledge and informed consent.

225. Plaintiff B.B. provided her Private Information to Defendants and trusted that the information would be safeguarded according to Defendants' policies and state and federal law.

226. As described herein, Defendants worked along with Facebook to intercept Plaintiff B.B.'s communications, including those that contained confidential Private Information, while Plaintiff B.B. was within the state of Idaho..

227. Defendants willfully facilitated these interceptions without Plaintiff B.B.'s knowledge, consent, or express written authorization.

228. Within the State of Idaho, Defendants transmitted Plaintiff B.B.'s FID, computer IP address, location, information such as treatment sought, and, upon information and good faith belief, medical history, appointment type, and fertility treatment details to Facebook.

229. By doing so without her consent, Defendants breached Plaintiff B.B.'s right to privacy and unlawfully disclosed her Private Information.

230. Defendants did not inform Plaintiff B.B. that they shared her Private Information with Facebook.

231. Plaintiff B.B. suffered damages in, inter alia, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

232. Plaintiff B.B. has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure. Plaintiff B.B. wants to continue to communicate with Defendants' healthcare providers through online platforms but has no practical way of knowing if her communications are being intercepted and disclosed to Facebook, and thus continues to be at risk of harm from Defendants' conduct.

233. Plaintiff B.B.'s experience is representative of the experience of the Class across Defendants' Web Properties.

H. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

234. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[97] This failure to protect users' data enabled thousands of developers

[97] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

235. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[98]

236. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[99] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with

[98] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.

[99] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

users' information."[100]

237. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[101]

238. In June 2022, an investigation by The Markup[102] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[103] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[104] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[105]

239. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about

---

[100] *Id.*
[101] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[102] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[103] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[104] *Id.*
[105] *Id.*

their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[106]

240. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[107]

241. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[108]

I. Defendants Violated HIPAA Standards

242. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[109]

243. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

244. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department 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

[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

a certain clinic, then this information would be PHI.[110]

245. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[111]

246. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology (the "December 2022 Bulletin").[112]

247. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[113]

248. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with

---

[110] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[111] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[112] *See* archived version of the December 2022 Bulletin at *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS.gov (Dec. 1, 2022), https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Mar. 30, 2024).

[113] *Id.*

such vendors. **Regulated 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**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI 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 identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. 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. [114]

249. In other words, HHS has expressly stated that Defendants' implementing the Meta Pixel is a violation of HIPAA Rules.

J. Defendants Violated FTC Standards, and the FTC and HHS Take Action

250. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[115]

251. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online

[114] *Id.* (emphasis in original) (internal citations omitted).

[115] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **attached as Exhibit A.**

activities."[116]

252. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules"[117] and that "[t]her is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes."[118]

253. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[119]

254. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health]

---

[116] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

[117] *Id.*

[118] *Id.*

[119] *Statement of the Commission: On Breaches by Health Apps and Other Connected Devices,* U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf) (emphasis added).

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."[120]

255. As such, the FTC and HHS have expressly stated that conduct like Defendants' runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

256. On March 18, 2024, HHS would update its December 2022 bulletin in the "March 2024 Bulletin," expanding the circumstances in which HHS would consider information from any unauthenticated website visitor to be considered PHI, and its disclosure to be a violation of HIPAA.[121]

257. The March 2024 Bulletin added guidance on when the disclosure of individually identifiable health information ("IIHI") is impermissible under HIPAA, explaining that: "the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI ***if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care***."[122]

258. However, in contrast, when a user visits a website related to his or her past, present,

---

[120] *See, e.g., U.S. v. Easy Healthcare Corp*., Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.,* FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.,* Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc*; In the Matter of Flo Health Inc.,* FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

[121] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022, updated Mar. 18, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last acc. May 3, 2024).

[122] *Id.* (bold, italicized emphasis added).

or future health, health care, or payment for health care, such as "…looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care[,]" such that the disclosure of their information would be PHI, HIPAA rules apply, and that disclosure would be a violation of HIPAA.[123, 124]

K. Defendants Violated Industry Standards

259. A medical provider's duty of confidentiality is a cardinal rule, embedded in doctor-patient and hospital-patient relationships.

260. The American Medical Association's ("AMA") Code of Medical Ethics requires the protection of patient privacy and communications, and these rules are applicable to Defendants and its physicians.

261. 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).

262. 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. Physicians who

[123] *Id.*

[124] As stated prior, on June 20, 2024, in *American Hospital Association, et al. v. Xavier Becerra, et al.,* Case No. 4:23-cv-01110-P (N.D. Tx., Jun. 20, 2024, Doc. 67), the U.S. District Court for the Northern District of Texas vacated HHS's March 14, 2024 Bulletin as to the "Proscribed Combination," *but* acknowledged that the Proscribed Combination could be PHI in certain circumstances.

> propose to permit third-party access to specific patient 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 purposes for which access would be granted.

263. 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 . . . release patient information only in keeping ethics guidelines for confidentiality.

L. Plaintiffs' and Class Members' Expectation of Privacy

264. At all times when Plaintiffs and Class Members provided their Private Information to Defendants, they had a reasonable expectation that the information would remain private and that Defendants would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

M. IP Addresses are Personally Identifiable Information

265. Defendants also disclosed Plaintiffs' and Class Members' IP addresses to Facebook, and others including Google, Microsoft, X Corp., Double Click and Post Hog, through its use of the Meta Pixel and other tracking technologies.

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

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

268. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party trackers to facilitate and track Internet communications.

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

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

271. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code," specifically listing IP addresses as an example of PII. *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).

272. Consequently, by disclosing IP addresses, Defendants business practices violated HIPAA and industry privacy standards.

N. Defendants Were Enriched by and Benefitted from the Use of Plaintiffs and Class Members' Private Information

273. Defendants' use of the Meta Pixel and other tracking technology were for the tortious purpose of invading Plaintiffs and Class Members' privacy, breaching its fiduciary duty, and violating HIPAA, all for marketing and profits.

274. In exchange for disclosing the Private Information of its patients, Defendants are compensated by Facebook and likely others including Google, Microsoft, X Corp., Double Click, and Post Hog in the form of enhanced advertising services and more cost-efficient marketing on its platform.

275. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendants re-targeted patients and potential patients.

276. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendants.

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

277. The data concerning Plaintiffs and Class Members, collected and shared by

Defendants, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[125] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[126] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[127]

278. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[128]

279. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates

[125] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[126] *Id.*
[127] *See* How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).
[128] *See* Here's How Big Facebook's Ad Business Really Is, CNN, https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html (last visited Aug. 14, 2023).

for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

280. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, it described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[129]

281. 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."[130]

TOLLING, CONCEALMENT, AND ESTOPPEL

282. The applicable statutes of limitation have been tolled as a result of Defendants' knowing and active concealment and denial of the facts alleged herein.

283. Defendants seamlessly incorporated Meta Pixel and other trackers into their Web Properties and Online Platforms while providing patients with no indication that the Web Properties usage was being tracked and transmitted to third parties. Defendants knew that its Web Properties incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiffs and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, Google, Microsoft, X Corp., Double Click and Post Hog and potentially others.

284. Even while exercising due diligence, Plaintiffs and Class Members could not have

[129] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.

[130] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

discovered the full scope of Defendants' conduct, because there were no disclosures or other indications that they were interacting with Web Properties employing Meta Pixel or any other tracking technology.

285. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendants' illegal interception and disclosure of Plaintiffs' Private Information has continued unabated through the present. What is more, Defendants was under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendants are therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

286. Plaintiffs bring this statewide class action on behalf of herself, and on behalf of other similarly situated persons, defined below as the "Class."

287. The Class that Plaintiffs seek to represent is defined as follows:

> **All United States residents whose Private Information was disclosed by Defendants to third parties through the Meta Pixel and related technologies without authorization across Defendants' Web Properties and Online Platforms.**

288. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

289. Plaintiffs reserve the right to modify or amend the definition of the proposed classes

before the Court determines whether certification is appropriate.

290. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendants, and the Class is identifiable within Defendants' records.

291. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. whether and to what extent Defendants had a duty to protect Plaintiffs' and Class Members' Private Information;

b. whether Defendants had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. whether Defendants had duties not to use Plaintiffs' and Class Members' Private Information for non-healthcare purposes;

d. whether Defendants had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. whether Defendants failed to adequately Plaintiffs' and Class Members' Private Information;

f. whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. whether Defendants failed to properly implement and configure the tracking

software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendants committed invasion of privacy;

j. whether Defendants breached its implied contract with Plaintiffs and the Class Members; or in the alternate, whether Defendants were unjustly enriched; and,

k. whether Defendants breached fiduciary duties to Plaintiffs and the Class Members.

l. whether Defendants violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq*.;

m. whether Defendants violated the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, and 56.101;

n. whether Defendants violated the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502;

o. whether Defendants engaged in unfair, unlawful, or deceptive practices in violation of Cal. Bus. & Prof. Code §§ 17200, *et. seq*.

292. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendants' use and incorporation of Meta Pixel and other tracking technology.

293. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with

respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

294. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiffs have suffered is typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

295. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

296. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged. If the class action device were not used, Defendants would necessarily gain an unconscionable advantage because it would

be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

297. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

298. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

299. Unless a Class-wide injunction is issued, Defendants may continue in their unlawful use and disclosure of Plaintiffs and Class Members' Private Information and refusal to provide proper notification to and obtain proper consent.

300. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

301. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to

a. whether Defendants owed a legal duty to Plaintiffs and Class Members to

exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. whether Defendants breached the implied contract;

f. in the alternate, whether Defendants were unjustly enriched;

g. whether Defendants adequately and accurately informed Plaintiffs and Class Members that their Private Information had been used and disclosed to third parties;

h. whether Defendants failed to implement and maintain reasonable security procedures and practices;

i. whether Defendants committed an invasion of privacy;

j. whether Defendants had fiduciary duties to Plaintiffs and the Class Members;

k. whether Defendants breached their fiduciary duties;

l. whether Defendants violated the California Invasion of Privacy Act

("CIPA"), Cal. Penal Code §§ 630, *et seq*.;

m. whether Defendants violated the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, and 56.101;

n. whether Defendants violated the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502;

o. whether Defendants engaged in unfair, unlawful, or deceptive practices in violation of Cal. Bus. & Prof. Code §§ 17200, *et. seq*.; and,

p. whether Plaintiffs and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

302. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

303. Defendants owed to Plaintiffs and Class Members a duty to exercise reasonable care in handling and using Plaintiffs and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

304. Defendants acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendants.

305. Defendants owed these duties to Plaintiffs and Class Members because they are

members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' Disclosure of their Private Information to benefit third parties and Defendants. Defendants actively sought and obtained Plaintiffs' and Class Members' Private Information.

306. Private Information is highly valuable, and Defendants knew, or should have known, the harm that would be inflicted on Plaintiffs and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendants by way of data harvesting, advertising, and increased sales.

307. Defendants breached their common law duties by failing to exercise reasonable care in the handling and securing of Private Information of Plaintiffs and Class Members and in the supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private Information of Plaintiffs and Class Members. This failure actually and proximately caused Plaintiffs' and Class Members' injuries.

308. In addition, the standards of care owed by Defendants are established by statute, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, under which Defendants were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Private Information.

309. Plaintiffs and Class Members are within the class of persons that these statutes and rules were designed to protect.

310. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information, PII and PHI.

311. Defendants owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Private Information, PII and PHI, being improperly disclosed to unauthorized third parties.

312. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information, PII and PHI, in compliance with applicable laws would result in an unauthorized third-parties such as Facebook, Google, Microsoft, X Corp., Double Click and Post Hog, gaining access to Plaintiffs' and Class Members' PII and PHI, and resulting in Defendants' liability under principles of negligence *per se*.

313. Defendants violated the standards of care under Section 5 of the FTC Act and under HIPAA and attendant regulations by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

314. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements, and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

315. Plaintiffs' and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendants' negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

316. Defendants' breach of its common-law duties to exercise reasonable care proximately caused Plaintiffs' and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information and diminution in value, emotional distress, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' negligence. These injuries are ongoing, imminent, immediate, and continuing.

317. In failing to secure Plaintiffs' and Class Members' Private Information, PII and PHI, Defendants are guilty of oppression, fraud, or malice. Defendants acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs and Class Members' rights. Plaintiffs, in addition to seeking actual damages, also seeks punitive damages on behalf of themselves and the Class.

318. Defendants' negligence directly and proximately caused the unauthorized access and Disclosure of Plaintiffs' and Class Members' Private Information, PII and PHI, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendants' conduct. Plaintiffs and Class Members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendants' negligence and negligence *per se*.

COUNT II
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Class)

319. Plaintiffs re-allege and incorporates the above allegations as if fully set forth herein.

320. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendants via its Web Properties and Online Platforms.

321. Plaintiffs and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendants to receive and that they understood Defendants would keep private.

322. Defendants' 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 in their private affairs and concerns.

323. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendants' representations in its Privacy Policy, and elsewhere. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendants' disclosure of PHI coupled with PII is highly offensive to the reasonable person.

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

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

326. 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 as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

327. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter

Defendants from engaging in such conduct in the future.

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

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

329. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

330. As a condition of receiving medical care from Defendants, Plaintiffs and the Class provided their Private Information and paid compensation for fertility and related medical treatment received. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, in its Privacy Policy, and elsewhere, to keep such information secure and confidential.

331. Implicit in the agreement between Defendants and their patients, Plaintiffs and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

332. Defendants had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits, and "…to monitor user traffic patterns and try to analyze what our users prefer so that we can design better services and activities for you."[131]

333. Defendants had an implied duty to protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses.

334. Additionally, Defendants explicitly promised to keep their patients' Private Information secure and confidential, stating in its Privacy Policy it would "…safeguard [their]

[131] SDFC Privacy Policy, **Exhibit B.**

personal information[,]" and would "…not share tracking information with unaffiliated companies, and we do not allow other companies to place cookies on our Site."[132]

335. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants, but Defendants did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendants in the absence of their implied contracts with Defendants that their Private Information would be kept in confidence and would instead have retained the opportunity to control their Private Information for uses other than receiving medical treatment from Defendants.

336. Defendants breached the implied contracts with Plaintiffs and Class members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties.

337. Defendants' acts and omissions have materially affected the intended purpose of the implied contracts that required Plaintiffs and Class Members to provide their Private Information in exchange for medical treatment and benefits.

338. As a direct and proximate result of Defendants' breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information and diminution in value, emotional distress, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendants' negligence. These injuries are ongoing, imminent, immediate, and continuing.

339. As a direct and proximate result of Defendants' above-described breach of contract,

[132] *Id*.

Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

340. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

341. This claim is pleaded solely in the alternative to Plaintiffs' breach of implied contract claim.

342. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of valuable sensitive medical information that Defendants collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendants collected, used, and disclosed this information for its own gain, for marketing purposes, and for sale or trade with third parties.

343. Plaintiffs and Class Members would not have used Defendants' services or would have paid less for those services, if they had known that Defendants would collect, use, and disclose their Private Information to third parties.

344. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

345. As a result of Defendants' conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy practices and procedures that they received.

346. The benefits that Defendants derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members themselves. Under unjust enrichment principles, it would be inequitable for Defendants to retain the profit and/or other benefits it derived from the unfair

and unconscionable methods, acts, and trade practices alleged in this Complaint.

347. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the unauthorized Disclosure alleged herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

348. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

349. A relationship existed between Plaintiffs and the Class, on the one hand, and Defendants, on the other, in which Plaintiffs and the Class put their trust in Defendants to protect the Private Information of Plaintiffs and the Class, and Defendants accepted that trust.

350. Defendants breached the fiduciary duty that it owed to Plaintiffs and the Class Members by failing to act with the utmost good faith, fairness, and honesty; failing to act with the highest and finest loyalty; and failing to protect and, indeed, intentionally disclosing, their Private Information.

351. Defendants' breach of fiduciary duty was a legal cause of injury-in-fact and damages to Plaintiffs and the Class.

352. But for Defendants' breach of fiduciary duty, the injury-in-fact and damages to Plaintiffs and the Class would not have occurred.

353. Defendants' breach of fiduciary duty substantially contributed to the injury and damages to the Plaintiffs and the Class.

354. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT VI
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CAL. PENAL CODE §§ 630, *ET SEQ*.
(On Behalf of Plaintiffs and the Class)

355. Plaintiffs re-alleges and incorporates the above allegations as if fully set forth herein.

356. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA") declaring 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.
>
> The Legislature by this chapter intends to protect the right of privacy of the people of this state.

Cal. Penal Code §§ 630.

357. Cal. Penal Code § 631(a) prohibits persons from "aid[ing], agree[ing] with, employ[ing], or conspir[ing] with" a third party to "read[], or attempt[] 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" "by means of any machine, instrument, or contrivance, or in any other manner…" Cal. Penal Code § 631(a).

358. Cal. Penal Code § 632(a) prohibits persons from intentionally recording confidential communications without consent of all parties to the communication.

359. All alleged communications between Plaintiffs or Class Members and Defendants qualify as protected communications under CIPA because each communication is made using

personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

360. As alleged in the preceding paragraphs, by use of the Meta Pixel and other tracking technologies, Defendants used a recording device to record the confidential communications without the consent of Plaintiffs or Class members and then transmitted such information to others, such as Facebook, Google, Microsoft, X Corp., Double Click and Post Hog.

361. At all relevant times, Defendants' aiding of Facebook, and other third parties including Google, Microsoft, X Corp., Double Click and Post Hog to learn the contents of communications and Defendants' recording of confidential communications was without Plaintiffs' and the Class Members' authorization and consent.

362. Plaintiffs and Class Members had a reasonable expectation of privacy regarding the confidentiality of their communications with Defendants. Defendants promised them that it would safeguard their personal information, and that it would "…not share tracking information with unaffiliated companies, and [] do[es] not allow other companies to place cookies on our Site," and to only use Plaintiffs' and the Class Members' "information about your use of the services and activities on the Site to monitor user traffic patterns and try to analyze what our users prefer so that we can design better services and activities for you."[133] Defendants never received any authorization and disclosed Plaintiffs' and the Class's Private Information anyways.

363. Defendants engaged in and continued to engage in interception by aiding others (including Facebook) to secretly record the contents of Plaintiffs' and Class Members' wire communications.

[133] SDFC Privacy Policy, Exhibit B.

364. The intercepting devices used in this case include, but are not limited to:

a. those to which Plaintiffs' and Class Members' communications were disclosed;

b. Plaintiffs' and Class Members' personal computing devices;

c. Plaintiffs' and Class Members' web browsers;

d. Plaintiffs' and Class Members' browser-managed files;

e. the Meta Pixel;

f. internet cookies;

g. other pixels, trackers, and/or tracking technology such as Google Analytics with Google Tag Manager, Facebook Events, Microsoft Universal Events, Twitter Business, DoubleClick Ads, and PostHog, installed on Defendants' Web Properties and/or server;

h. Defendants' computer servers;

i. third-party source code utilized by Defendant; and

j. computer servers of third parties (including Facebook).

365. Defendants aided in the interception of contents in that the data from the communications between Plaintiffs and/or Class Members and Defendants that were redirected to and recorded by the third parties, including Facebook, include information which identifies the parties to each communication, their existence, and their contents.

366. Plaintiffs and Class Members reasonably expected that their Private Information was not being intercepted, recorded, and disclosed to Facebook, and other third parties such as Google, Microsoft, X Corp., Double Click and Post Hog.

367. No legitimate purpose was served by Defendants' willful and intentional disclosure

of Plaintiffs' and Class Members' Private Information to Facebook, and other third parties. Neither Plaintiffs nor Class Members consented to the disclosure of their Private Information by Defendants to Facebook, and other third parties.

368. The tracking pixels that Defendants utilized are designed such that they transmitted each of a Web Properties user's actions to third parties alongside and contemporaneously with the user initiating the communication. Thus, Plaintiffs and Class Members' communications were intercepted in transit to the intended recipient (Defendant) before they reached Defendants' servers.

369. Defendants willingly facilitated Facebook's interception and collection of Plaintiffs' and Class Members' Private Information by embedding pixels on its Online Platforms. Moreover, Defendants had full control over these tracking pixels, including which webpages contained the pixels, what information was tracked and shared, and how events were categorized prior to transmission.

370. Defendants gave substantial assistance to Facebook in violating the privacy rights of Defendants' patients, despite the fact that Defendants' conduct constituted a breach of the duties of confidentiality that medical providers owe their patients. Defendants knew that the installation of the Meta Pixel on their Web Properties would result in the unauthorized disclosure of its patients' communications to Facebook, yet nevertheless did so anyway.

371. Plaintiffs' and Class Members' electronic communications were intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their Private Information, including using their sensitive medical information to develop marketing and advertising strategies. The private information that Defendants assisted Facebook, and other third parties such as Google, Microsoft, X Corp., Double Click and Post Hog, with reading, learning,

and exploiting, including Plaintiffs' and Class Member's medical conditions, their medical concerns, and their past, present, and future medical treatment.

372. Plaintiffs and the Class Members seek statutory damages under Cal. Penal Code § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

373. In addition to statutory damages, Defendants' violations caused Plaintiffs and Class Members the following damages.

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private.

b. Defendants eroded the essential confidential nature of the doctor-patient relationship.

c. Defendants took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality; and

e. Defendants' actions diminished the value of Plaintiffs' and Class Members' personal information.

374. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT VII
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA"), CAL. CIVIL CODE §§ 56.06, 56.10, 56.101
(On behalf of Plaintiffs and the Class)

375. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

376. Defendants are providers of health care under Cal. Civil Code. § 56.06, subdivisions (a) and (b), because they maintains medical information and offers software to consumers that is designed to maintain medical information for the purposes of allowing their users to manage their information or for the diagnosis, treatment, or management of a medical condition.

377. Defendants are therefore subject to the requirements of the CMIA and obligated under subdivision (d) to maintain the same standards of confidentiality required of a provider of health care with respect to medical information disclosed to it.

378. By conduct complained of in the preceding paragraphs, Defendants violated Cal. Civil Code § 56.06 by failing to maintain the confidentiality of users' medical information, Private Information, and instead, disclosing Plaintiffs' and Class Members' medical information/Private Information to Facebook, and other third parties such as Google, Microsoft, X Corp., Double Click and Post Hog, without consent. This information was intentionally shared with Facebook and others such as Google, Microsoft, X Corp., Double Click and Post Hog, whose business is to sell advertisements based on the data that they collect about individuals, including the data Plaintiffs and the Class Members shared with Defendants.

379. As set forth above, Defendants knowingly shared information such as identities, device identifiers, IP addresses, web URLs, the "c_user cookie" which Facebook uses to identify users and/or Facebook IDs, and other data that could be used to identify Plaintiffs and Class Members in combination with their health information, such as searches for programs. This

information constitutes confidential information under the CMIA.

380. Defendants knowingly and willfully, or negligently, disclosed medical information without consent to Facebook for financial gain. Defendants' acts were knowing and willful as Defendants was aware that Facebook would collect all data inputted while using their Web Properties, yet intentionally embedded Meta Pixel anyway.

381. Defendants' decision to affirmatively share and communicate their patients' PHI/Private Information with Facebook resulted in one or more unauthorized persons improperly accessing and reviewing Plaintiffs' and the Class Members' PHI.

382. Cal. Civil Code § 56.10(a) prohibits a health care provider from disclosing medical information without first obtaining an authorization, unless a statutory exception applies.

383. By conduct complained of in the preceding paragraphs, Defendants disclosed medical information, Private Information, of Plaintiffs and the Class Members without first obtaining authorization when it disclosed their sensitive medical information to Facebook, and other third parties such as Google, Microsoft, X Corp., Double Click and Post Hog, without consent, including PHI and PII. No statutory exception applies.

384. As a result, Defendants violated Cal. Civil Code § 56.10(a).

385. Cal. Civil Code § 56.101(a) requires that 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."

386. Any health care provider who "negligently creates, maintains, preservers, 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."

387. By conduct complained of in the preceding paragraphs, Defendants failed to

maintain, preserve, and store medical information/Private Information of Plaintiffs and the Class Members in a manner that preserves the confidentiality of the information contained therein by disclosing their PHI/Private Information to Facebook, and other third parties such as Google, Microsoft, X Corp., Double Click and Post Hog, without consent.

388. Defendants' failure to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information was, at the least, negligent and violates Cal. Civil Code § 56.36(b) and (c).

389. Accordingly, as a result of Defendants' violations of Cal. Civil Code §§ 56.06, 56.10, and Cal. Civil Code 56.101, Plaintiffs and Class Members are entitled to: (1) nominal damages of $1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36(c); and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

390. In addition to statutory damages, Defendants' breach of Cal. Civil Code §§ 56.06, 56.10, and 56.101, caused Plaintiffs and Class Members, at minimum, the following damages:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private.

b. Defendants eroded the essential confidential nature of the doctor-patient relationship.

c. Defendants took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiffs and Class Members did not get the full value of the medical

services for which they paid, which included Defendants' duty to maintain confidentiality; and

e. Defendants' actions diminished the value of Plaintiffs' and Class Members' personal information.

263. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT VIII
VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502.
(On Behalf of Plaintiffs and the Class)

264. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

265. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, CAL. PENAL CODE § 502 ("CDAFA") to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems," and finding and declaring "that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data." Cal. Penal Code § 502(a).

266. In enacting the CDAFA, the Legislature further found and declared "that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

267. Plaintiffs' and the Class Members' devices on which they accessed Defendants' Online Platforms and Web Properties, including their computers, smart phones, and tablets,

constitute computers or "computer systems" within the meaning of CDAFA. Cal. Penal Code § 502(b)(5).

268. By conduct complained of in the preceding paragraphs, Defendants violated Section 502(c)(1)(B) of CDAFA by knowingly accessing without permission Plaintiffs' and Class Members' devices in order to wrongfully obtain and use their personal data, including their sensitive medical information, all Private Information, in violation of Plaintiffs' and Class Members' reasonable expectations of privacy in their devices and data.

269. Defendants violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking, copying, and using Plaintiffs' and the Class Members' Private Information, PHI and PII, including their sensitive medical information.

270. Defendants used Plaintiffs' and Class Members' data as part of a scheme to defraud them and wrongfully obtain their data and other economic benefits. Specifically, Defendants intentionally concealed from Plaintiffs and Class Members that Defendants had secretly installed tracking pixels on their Online Platforms that surreptitiously shared patient data with third party advertising companies like Facebook. Had Plaintiffs and Class Members been aware of this practice, they would not have used Defendant' Web Properties and Online Platforms.

271. The computers and mobile devices that Plaintiffs and Class Members used when accessing Defendants' Online Platforms all have and operate "computer services" within the meaning of CDAFA. Defendants violated §§ 502(c)(3) and (7) of CDAFA by knowingly and without permission accessing and using those devices and computer services, and/or causing them to be accessed and used, *inter alia*, in connection with Facebook's wrongful collection of such data.

272. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any

set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information."

273. Defendants violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via Meta Pixel embedded into the Online Platforms which intercepted Plaintiffs' and the Class Members' private and sensitive medical information.

274. Defendants' violation of the CDAFA caused Plaintiffs and Class Members, at minimum, the following damages:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private.

b. Defendants eroded the essential confidential nature of the doctor-patient relationship.

c. Defendants took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality; and

e. Defendants' actions diminished the value of Plaintiffs' and Class Members' Private Information.

275. Plaintiffs and the Class Members seek compensatory damages in accordance with Cal. Penal Code § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable

relief; as well as punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) as Defendants' violations were willful and, upon information and belief, Defendants are guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294; and reasonable attorney's fees under § 502(e)(2).

276. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT IX
VIOLATION OF CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*
(On Behalf of Plaintiffs and the Class)

277. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

278. Plaintiffs and Defendants are each "persons" under Cal. Bus. & Prof. Code § 17201.

279. The California Business and Professions Code §§ 17201, *et seq*. prohibits acts of unfair competition, which includes unlawful business practices.

280. Defendant' business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* (the "UCL") because, as alleged above, Defendants violated California common law, and other statutes and causes of action alleged herein.

281. Defendants engaged in unlawful acts and practices by imbedding the Pixel on its Web Properties, which tracks, records, and transmits Plaintiffs' and Class Members' PHI/Private Information they disclose to Defendants in confidence via the Online Platforms and Web Properties to third parties without Plaintiffs' and Class Members' knowledge and/or consent, in violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq*.; the California Confidentiality of Medical Information Act ("CMIA"), CAL. CIVIL CODE §§ 56.06, 56.10, 56.101; the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and by representing that their services have characteristics, uses, or benefits that they

do not have in violation of Civil Code § 1770.

282. When using Defendant' Web Properties, Online Platforms, and services, Plaintiffs and Class Members relied on Defendants' status as healthcare providers.

283. Inconsistent with its role as a healthcare provider, Defendants disclosed Plaintiffs' and Class Members' PHI/Private Information to third parties without their consent and for marketing purposes. Thus, Defendants represented that its services have characteristics, uses, or benefits that they do not have and represented that its services are of a particular standard, quality, or grade when they were not, in violation of Cal. Civil Code § 1770.

284. Plaintiffs and Class Members were reasonable to assume, and did assume, that Defendants would take appropriate measures to keep their PHI/Private Information secure and not share it with third parties without their express consent. Defendants also had a duty to disclose that it was sharing its patients' Personal Health Information with third parties. However, Defendants did not disclose at any time that it was sharing this PHI/Private Information with third parties via the Meta Pixel and other tracking technologies such as Google Analytics with Google Tag Manager, Facebook Events, Microsoft Universal Events, Twitter Business, DoubleClick Ads, and PostHog.

285. Had Plaintiffs and Class Members known that Defendants would intercept, collect, and transmit their PHI/Private Information to Facebook and other third parties such as Google, Microsoft, X Corp., Double Click and Post Hog, Plaintiffs and the Class Members would not have used Defendants' services.

286. Plaintiffs and Class Members have a property interest in their PHI/Private Information. By surreptitiously collecting and otherwise misusing Plaintiffs' and Class Members' PHI/Private Information, Defendants have taken property from Plaintiffs and Class Members

without providing just (or indeed any) compensation.

287. By deceptively collecting, using, and sharing Plaintiffs' and Class Members' PHI/Private Information with Facebook and other third parties, Defendants have taken money or property from Plaintiffs and Class Members. Accordingly, Plaintiffs seek restitution on behalf of herself and the Class.

288. Defendants' business acts and practices also meet the unfairness prong of California's Unfair Competition Law ("UCL") according to all three theories of unfairness.

289. First, Defendants' business acts and practices are "unfair" under the UCL pursuant to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142 Cal. App. 4th 1394, 1403: (a) Plaintiffs and Class Members suffered substantial injury due to Defendants' Disclosure of their PHI/Private Information; (b) Defendants' disclosure of Plaintiffs' and Class Members' PHI/Private Information provides no benefit to consumers, let alone any countervailing benefit that could justify Defendants' Disclosure of PHI/Private Information without consent for marketing purposes or other pecuniary gain; and (c) Plaintiffs and Class Members could not have readily avoided this injury because they had no way of knowing that Defendants were implementing the Meta Pixel.

290. Second, Defendants' business acts and practices are "unfair" under the UCL because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to Plaintiffs and Class Members, and "the utility of [Defendants'] conduct," if any, does not "outweigh the gravity of the harm" to Plaintiffs and Class Members. *Drum v. San Fernando Valley Bar Ass'n,* (2010) 182 Cal. App. 4th 247, 257. Defendants secretly collected, disclosed, and otherwise misused Plaintiffs' and Class Members' PHI/Private Information by bartering it to Facebook and other third parties in return for access to the Pixel tool. This surreptitious, willful,

and undisclosed conduct is immoral, unethical, oppressive, unscrupulous, and substantially injurious. Moreover, no benefit inheres in this conduct, the gravity of which is significant.

291. Third, Defendant' business acts and practices are "unfair" under the UCL because they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App. 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy of protecting consumers' privacy interests, including consumers' and patients' personal data, as codified in California's Constitution in Article I, section 1; the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq*.; the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101; the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502, among other statutes.

292. Defendants violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise exploiting Plaintiffs and Class Members' PHI/Private Information by sharing that information with Facebook and other third parties via the Tracking Pixel without Plaintiffs' and/or Class Members' consent.

293. Had Plaintiffs and Class Members known Defendants would intercept, collect, and transmit their PHI/Private Information to Facebook and other third parties, Plaintiffs and Class Members would not have used Defendant' services.

294. Plaintiffs and Class Members were reasonable to assume, and did assume, that Defendants would take appropriate measures to keep their PHI/Private Information secure and not share it with third parties without their express consent. Defendants were in sole possession of and had a duty to disclose the material information that Patient Plaintiffs' and Class Members' Personal Health Information would be shared with third parties via the Meta Pixel. Defendants did not disclose at any time that they were sharing this PHI/Private Information with third parties via the

Tracking Pixel.

295. Plaintiffs and Class Members have a property interest in their PHI/Private Information. By surreptitiously collecting and otherwise misusing Plaintiffs' and Class Members' Personal Health Information, Defendants have taken property from Plaintiffs and Class Members without providing just (or indeed any) compensation.

296. Plaintiffs and Class Members have lost money and property due to Defendant' conduct in violation of the UCL. PHI/Private Information such as that which Defendants collected and transmitted to third parties has objective monetary value. Companies are willing to pay for PHI, like the information Defendants unlawfully collected and transmitted to third parties, such as Facebook. For example, Pfizer annually pays approximately $12 million to purchase health data from various sources.[134]

297. Consumers also value their personal health data. According to the annual Financial Trust Index Survey conducted by the University of Chicago's Booth School of Business and Northwestern University's Kellogg School of Management, which interviewed more than 1,000 Americans, 93 percent of survey participants would not share their health data with a digital platform for free. Half of the survey participants would only share their data for $100,000 or more, and 22 percent would only share their data if they received between $1,000 and $100,000. [135]

298. By deceptively collecting, using, and sharing Plaintiffs' and Class Members' PHI/Private Information with Facebook and other third parties, Defendants have taken money and/or property from Plaintiffs and Class Members. Accordingly, Plaintiffs seeks restitution on

[134] https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

[135] https://www.beckershospitalreview.com/healthcare-information-technology/how-much-should-health-data-cost-100k-or-more-according-to-patients.html (last acc. June 26, 2024).

behalf of herself and the Class.

299. As a direct and proximate result of Defendant' unfair and unlawful methods and practices of competition, Plaintiffs and Class Members suffered actual damages, including, but not limited to, the loss of the value of their Private Health Information.

300. As a direct and proximate result of their unfair and unlawful business practices, Defendants have been unjustly enriched and should be required to make restitution to Plaintiffs and Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement of all profits accruing to Defendants because of its unlawful and unfair business practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

COUNT X
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2511(1), et seq.
(On Behalf of Plaintiffs and the Class)

301. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

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

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

304. 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.

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

306. Electronic Communications. The transmission of PII and PHI between Plaintiffs and Class Members and Defendants' Web Properties 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).

307. 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) (emphasis added).

308. Interception. The ECPA defines an 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).

309. Electronical, 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).

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

a. The cookies Defendants and Meta use to track Plaintiffs' and the Class Members' communications;

b. Plaintiffs' and Class Members' browsers;

c. Plaintiffs' and Class Members' computing devices;

d. Defendants' web-servers and

e. The Pixels deployed by Defendants to effectuate sending and acquiring Users' and

f. patients' sensitive communications.

311. Plaintiffs and Class Members' interactions with Defendants' Web Properties are

electronic communications under the ECPA.

312. By utilizing and embedding the Pixel on their Web Properties, Defendants intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

313. Specifically, Defendants intercepted Plaintiffs' and Class Members' electronic communications via the Meta Pixel, CAPI and other tracking technologies, which tracked, stored and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such as Facebook.

314. Defendants intercepted communications that include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, including email, phone number, IP address, Facebook ID, treatment information, and, upon information and good faith belief, medical history, medications and appointment scheduling details. Additionally, through the above-described tracking tools, Defendants transmitted the communications about doctors, treatments and conditions, including but not limited to the name(s), location(s) and specialty(s) of physicians' Plaintiffs searched for on Defendants' Web Properties. This information was, in turn, used by third parties, such as Facebook, to 1) place Plaintiffs in specific health-related categories and 2) target Plaintiffs with particular advertising associated with Plaintiffs' specific reproductive health conditions. Defendants knowingly transmit this data and do so for the purpose of financial gain.

315. By intentionally disclosing or endeavoring to disclose Plaintiffs' and Class Members' electronic communications 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), Defendants violated 18 U.S.C. § 2511(1)(c).

316. By intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, 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), Defendants violated 18 U.S.C. § 2511(1)(d).

317. Unauthorized Purpose. Defendants intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of California—namely, invasion of privacy, among others.

318. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendants violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information (IIHI) to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) *relates 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 (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[136]

319. Plaintiffs' information that Defendants disclosed to third parties qualifies as IIHI,

[136] Id. § 1320d-(6) (emphasis added).

and Defendants violated Plaintiffs' expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6).

320. Defendants used the wire or electronic communications to increase its profit margins. Defendants specifically used the Pixels to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

321. Defendants were not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communication.

322. Plaintiffs and Class Members did not authorize Defendants to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code. Plaintiffs and absent class members (all of whom are patients) had a reasonable expectation that Defendants would not re-direct their communications content to Facebook, Google or others attached to their personal identifiers in the absence of their knowledge or consent.

323. Any purported consent that Defendants received from Plaintiffs and Class Members was not valid.

324. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendants' Web Properties, researching medical conditions and treatment and scheduling appointments with doctors, Defendants' purpose was tortious, criminal and designed to violate federal and state legal provisions including a knowing intrusion into a private place or matter that would be highly offensive to a reasonable person.

325. Consumers have the right to rely upon the promises that companies make to them. Defendants accomplished their tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause Facebook pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other

tracking technologies to be deposited on Plaintiffs' and Class members' computing devices as "first-party" cookies that are not blocked.

326. Defendants' scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the claims below;

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendants' Website rather than a third-party cookie from Meta.

327. Defendants acted with the intent to defraud in that they willfully invaded and took Plaintiffs' and Class Members' property:

a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

328. Defendants acted with the intent to defraud in that they willfully invaded and took Plaintiffs' and Class Members' property:

a. with knowledge that (1) Defendants did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their Private Information based on their activities on Defendants' Websites; (4) "a reasonable Facebook user would be shocked to realize" the extent of Meta's collection of Private Information; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Meta's consent decrees with the FTC and (6) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their Private Information for any purpose not related to the provision of their healthcare; and

b. with the intent to (1) acquire Plaintiffs and Class Members' Private Information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiffs' and Class Members' Private Information without their authorization and (3) gain access to

Plaintiffs' and Class Members' personal computing devices through the 'fbp' cookie disguised as a first-party cookie.

329. A person who violates § 2511(1)(a) is liable for $10,000 in statutory damages to any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used.

330. As a direct and proximate result of Defendants' violation of the ECPA, Plaintiffs and Class Members were damaged by Defendants' conduct.

331. For the same reasons as set forth above for Plaintiffs' CIPA Claims, Defendants are liable to Plaintiffs and Class Members for violations of the ECPA.

332. Based on the foregoing, Plaintiffs and Nationwide Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT XI
INVASION OF PRIVACY—CALIFORNIA CONSTITUION ART. 1 § 1
(On Behalf of Plaintiffs and the Class)

333. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

334. 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 without being subjected to wiretaps without Plaintiffs' and Class Members' knowledge or consent.

335. At all relevant times, by using Facebook's and other third parties' tracking pixel(s) to record and communicate patients' FIDs and other individually identifying information alongside their confidential medical communications, Defendants intentionally invaded Plaintiffs' and Class

Members' privacy rights under the California Constitution.

336. Plaintiffs and Class Members had a reasonable expectation that their communications, identity, health information, and other data would remain confidential, and that Defendants would not install wiretaps on their Web Properties to secretly transmit communications to a third party.

337. Plaintiffs and Class Members did not authorize Defendants to record and transmit Plaintiffs' and Class Members' private medical communications alongside their personally identifiable health information.

338. 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.

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

340. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages and an injunction that prevents Defendants from engaging in the same or similar conduct in the future.

341. Plaintiffs and Class Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of the intrusion(s) upon Plaintiffs' and Class Members' privacy.

342. Plaintiffs and Class Members are further entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring

Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

343. Plaintiffs seek all other relief as the Court may deem just, proper, and available for invasion of privacy under the California Constitution.

COUNT XII
LARCENY/RECEIPT OF STOLEN PROPERTY (VIOLATION OF CALIFORNIA PENAL CODE § 496(a) & (c))
(On Behalf of Plaintiffs and the Class)

344. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

345. Internet users have a property interest in their personal information and data.

346. Cal. Penal Code §496(c) permits "any" person who has been injured by a violation of section 496(a) to recover three times the amount of actual damages, costs of suit and attorney's fees in a civil suit.

347. Penal Code § 496(a) creates an action against "any" person who (1) receives "any" property that has been stolen or obtained in any manner constituting theft, knowing the property to be stolen or obtained, or (2) conceals, sells, withholds, or aids in concealing or withholding "any" property from the owner, knowing the property to be so stolen or illegally obtained.

348. Under Penal Code § 1.07(a)(38), "person" means "an individual, corporation, or association." Thus, Defendants are a person under section 496(a).

349. As set forth herein, Plaintiffs' and Class Members' Private Information was stolen or obtained by theft, without limitation, under Penal Code §484, by false or fraudulent representations or pretenses. At no point did the Defendants have Plaintiffs' and Class Members' consent to duplicate their searches and send them to Facebook.

350. 370. Defendants meet the grounds for liability of section 496(a) because Defendants:

a. knew the Private Information was stolen or obtained by theft and/or false pretenses; and, with such knowledge;

b. transmitted such information to unauthorized third parties, like Facebook.

351. 371. Defendants violated the second ground for liability of section 496(a) because Defendants:

a. knew the Private Information was stolen or obtained by theft; and, with such knowledge;

b. concealed, withheld, or aided in concealing or withholding said data from their rightful owners by unlawfully tracking the data and disclosing it to unauthorized third parties, like Facebook.

352. As a direct and proximate result of the acts and omissions described above, Plaintiffs and California Subclass Members were injured by Defendants' violations of section 496(a).

353. Pursuant to California Penal Code § 496(c), Plaintiffs and California Subclass Members seek actual damages, treble damages, costs of suit, and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, Individually, and on behalf of all others similarly situated, prays for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiffs as Class Representative and Plaintiffs' counsel as Class Counsel;

B. for an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

C. for equitable relief enjoining Defendants from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

D. for equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

E. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. an order that Defendants to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

G. for an award of punitive damages, as allowable by law;

H. for an award of attorneys' fees under the common fund doctrine, and any other applicable law;

I. costs and any other expenses, including expert witness fees incurred by Plaintiffs in connection with this action;

J. pre- and post-judgment interest on any amounts awarded; and

K. such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, by counsel, hereby demands a trial by jury on all issues so triable.

Dated: January 27, 2025

Respectfully submitted,

Vess A. Miller (278020)
Natalie A. Lyons (293026)

COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
vmiller@cohenandmalad.com
nlyons@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Andrew G. Gunem (SBN 354042)
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
andrew@straussborrelli.com

Matthew J. Langley (SBN 342846)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
t: 312-576-3024
matt@almeidalawgroup.com

Counsel for Plaintiffs and the Proposed Class

Exhibit A

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

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,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] 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

---

[1] *See, e.g.,* Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[2] *See, e.g.,* Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

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, 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 (HIPAA)

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. HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.[5] This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies.

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. This is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes. 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.[6] 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.[7] Within the last

[5] *Id.*
[6] *See supra* note 3.
[7] *See* Federal Trade Comm'n, *Statement of the Commission on Breaches by Health Apps and Other Connected Devices* (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

few months, the FTC has issued a series of guidance pieces addressed to entities collecting, using, or disclosing sensitive health information.[8]

OCR and the FTC remain committed to ensuring that consumers' health privacy remains protected with respect to this critical issue. Both agencies are closely watching developments in this area. To the extent you are using the tracking technologies described in this letter on your website or app, we strongly encourage you to review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information.[9]

Sincerely,

/s/

Melanie Fontes Rainer
Director
Office for Civil Rights
U.S. Department of Health and Human Services

/s/

Samuel Levine
Director
Bureau of Consumer Protection
Federal Trade Commission

[8] *See, e.g.*, FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking* (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking; Lesley Fair, *First FTC Health Breach Notification Rule case addresses GoodRx's not-so-good privacy practices* (Feb. 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices; Federal Trade Comm'n and the U.S. Department of Health & Human Services' Office of the National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR), and Food and Drug Administration (FDA), *Mobile Health App Interactive Tool* (Dec. 2022), https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool; Kristin Cohen, *Location, health, and other sensitive information: FTC Committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[9] In addition to the HIPAA Rules, the FTC Act, and the FTC Health Breach Notification Rule, you may also be subject to other state or federal statutes that prohibit the disclosure of personal health information.

Exhibit B

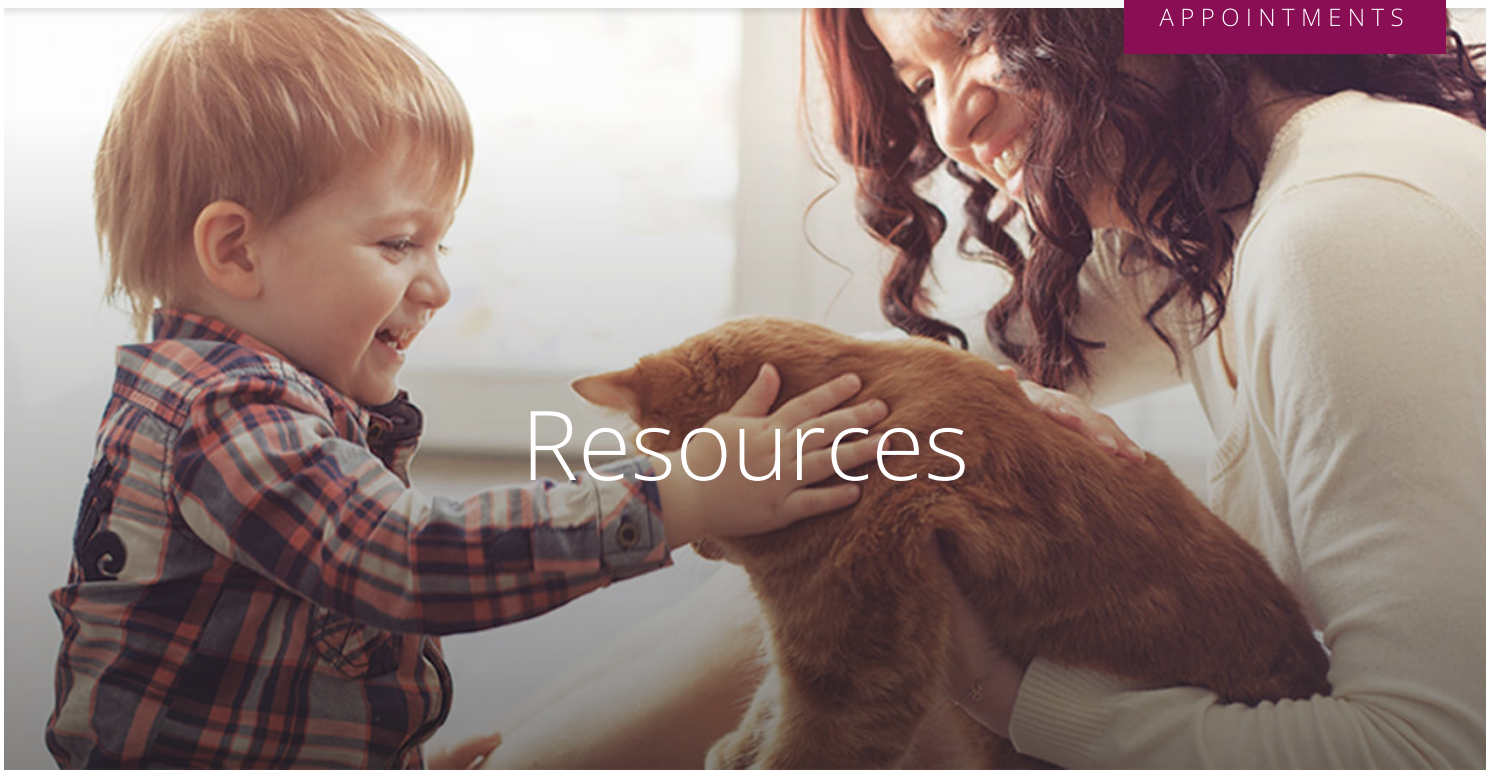
SAN DIEGO Fertility Center

Call Today! +1 858 461 6332

MENU

Call Today! +1 858 461 6332

APPOINTMENTS



SDFC › Resources › Disclaimer and Privacy Policy

Disclaimer and Privacy Policy

San Diego Fertility Center Disclaimer and Privacy Policy

"Every person that we came into contact with was kind,

Legal Disclaimer

Unless otherwise indicated, this website and its contents are the property of the San Diego Fertility Center, Incorporated, an independently operated fertility clinic. This website has been funded by San Diego Fertility Center Medical Group, Inc. and it is protected, without limitation, pursuant to U.S. and foreign copyright and trademark laws. Sponsorships or other funding from an affiliated company are not present unless clearly indicated on the specific content page. We do not accept or host online advertisement and follow the guidelines set by the American Medical Association (Guidelines for medical and health information sites in the internet. JAMA 2000; 283:1600-6).

Review Process of Website Content

Content is reviewed regularly for accuracy and reliability by our website editorial board. The Editorial Board for medical content consists of Dr. Michael Kettel and Lisa Souza Van Dolah, RN. Non-medical content is passing regular quality review process of our Administrative Editorial Board, which consists of Dr. Michael Kettel, CEO Lisa Souza and staff members with expertise in their particular department.

The Editorial Board holds ongoing update and review meetings [illegible] In addition, input into the [illegible] items is provided by individual [illegible] Board members as new content is developed, in line with their particular expertise. Dates on which content is posted, revised or updated are clearly indicated on each individual page.

SDFC MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THIS WEBSITE OR ITS CONTENTS OR ANY WEBSITE WITH WHICH IT IS LINKED. ALL INFORMATION IS PROVIDED FOR USE "AS IS." THIS WEBSITE DOES NOT ACCEPT OR HOST ANY ADVERTISEMENT. SDFC ALSO MAKES NO REPRESENTATIONS OR WARRANTIES AS TO WHETHER THE INFORMATION ACCESSIBLE VIA THIS WEBSITE, OR ANY WEBSITE WITH WHICH IT IS LINKED, IS ACCURATE, COMPLETE, OR CURRENT. IN NO EVENT SHALL SDFC OR ITS EMPLOYEES, AGENTS, SUPPLIERS, OR CONTRACTORS BE LIABLE FOR ANY DAMAGES OR ANY KIND OR CHARACTER, INCLUDING WITHOUT LIMITATION ANY COMPENSATORY, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, LOSS OF USE, LOSS OF DATA, LOSS OF INCOME OR PROFIT, LOSS OF OR DAMAGE TO PROPERTY, CLAIMS OF THIRD PARTIES, OR OTHER LOSSES OF ANY KIND OR CHARACTER, EVEN IF SDFC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS WEBSITE OR ANY WEBSITE WITH WHICH IT IS LINKED.

Portions of this Site (e.g. patient testimonials) may provide a forum for you to post and exchange opinions. Be advised that postings do not necessarily reflect the views of SDFC. In no event shall SDFC assume or have any responsibility or liability for the postings or for any claims, damages or losses resulting from their use and/or appearance on this Site. You hereby represent and warrant that you have all necessary rights in and to all postings you provide and all information they contain and that such postings shall not infringe any proprietary or other rights of third parties or contain any libelous, tortuous, or otherwise unlawful information. You hereby authorize SDFC to use and/or authorize others to use your postings in any manner, format or medium that SDFC sees fit.

Medical Disclaimer

The information posted here by the San Diego Fertility Center Medical Group, Inc. should not be considered medical advice and is not intended to replace consultation with a qualified medical professional. We cannot answer specific medical questions in your e-mail requests. We can answer questions related to the provision of services, insurance and financial information, brochure requests, and other Center specific matters. Please feel free to contact us by e-mail, phone, fax, or letter.

Additional Guidelines for Linking / Repurposing / Permission

us with this information will also allow us to notify you in the event that the URL for our site changes, or if we remove content from our site. If you wish to have your website listed with us, or wish to exchange links with us, please click here. All requests can be sent to our marketing department. Note however that the current practice known as "framing" where a link is established in such a way as to display our content in some form other than it is displayed in full view by our server, or otherwise displaying our content only partially, or without our copyright notice, is definitely uninvited and unwelcome. Please read our legal statement for details.

Privacy Policy

We are committed to respecting your privacy. We urge all users of www.sdfertility.com (the "Site") to read this Privacy Policy to learn more about the policies and practices that we have developed to safeguard your personal information.

Information We Collect

Online Contact Forms

You may choose to share information with us through interactive forms on our Web site. For example, you may submit a request for an appointment to us online through our Web site. The use of these forms is voluntary and the information you submit is forwarded

We use SSL for the online contact forms, which ensures that all communications between you and our mail server will be encrypted (https:// instead of http:// in the address bar of contact forms). Your message contents will be hidden from prying eyes and encryption helps mitigate identity theft, the sending of false messages, etc. However, since the form messages are transmitted over the Internet, SDFC cannot assure that the messages are completely secure. If you are uncomfortable with such risks, you may decide not to use the online forms to communicate with SDFC. You must be aware that the messages may be delayed or undelivered.

We also have access to the following categories of information regarding you and your visit to the Site.

IP Address

We record the Internet Protocol (IP) address of your computer when you visit the Site. The IP address does not identify you personally, but it is what allows us to maintain communications with you as you move about the Site.

Cookies

We also collect information about your use of the Site through cookies and similar technology. A "cookie" is a unique numeric code that we transfer to your computer so that we can keep track of your interests and

your interest in certain Site categories. We do not share tracking information with unaffiliated companies, and we do not allow other companies to place cookies on our Site.

How We Use Your Information

We use the information about your use of the services and activities on the Site to monitor user traffic patterns and try to analyze what our users prefer so that we can design better services and activities for you.

Changes in Our Privacy Policy

We will occasionally update this privacy statement. For material changes to this statement, we will notify you by placing a prominent notice on our Web site.

Visit San Diego Fertility Center – Coast to Coast

San Diego Fertility Center® is a world-class fertility center with locations in Southern California

SDFC is a leading nationwide provider of IVF and fertility care.

Our California and New York offices are not only conveniently located for our United States patients but are also accessible for the international community, making SDFC an exceptional destination for fertility tourism.

Our Fertility Clinics in California & New York

11425 El Camino Real San Diego, CA, 92130

591 Camino De La Reina, Suite 1250, San Diego, CA, 92108

44274 George Cushman Ct, Suite 201, Temecula, CA, 92592

501 Fifth Avenue, Suite 1900, New York, NY,10017

Call Today! +1 858 461 6332

SAN DIEGO Fertility Center

Call Today! +1 858 461 6332

MENU

Call Today! +1 858 461 6332

APPOINTMENTS

Our Fertility Center

- Fertility Doctors & Specialists
- Infertility Clinic
- IVF Success Rates
- Egg Donor Program
- Become an Egg Donor
- Paid Egg Donor
- Gestational Surrogacy Program

Fertility Treatments

- Infertility Testing & Diagnosis
- IVF - In-Vitro Fertilization
- PGD - PGS - Gender Selection
- LGBT Fertility
- Male Infertility
- Egg Freezing
- Fertility Preservation

International Care

- Fertility Tourism
- Fertility Travel
- FIV
- Donación de Óvulos
- Subrogación Gestacional
- Korean Fertility Program
- Chinese Fertility Program

Make a Bill Payment Online

Enter the A

PAY ONLINE

Sign Up for Our Newsletter

Enter Your

SUBSCRIBE

World Class Fertility Care in California & New York

San Diego Fertility Center® is one of the most respected fertility centers in the USA with fertility clinics in Southern California and New York City. With exceptional patient care, a track record of IVF success and a sunny fertility tourism destination, San Diego Fertility Center is an international location for egg donation, IVF, IUI, PGD/PGS, gender selection, egg freezing, surrogacy and other infertility treatments. Our dedicated team is fluent in Spanish, Mandarin Chinese and Korean.

Our three fertility clinics in California are conveniently located in Del Mar, Mission Valley, and Temecula, making it easy for patients from San Diego County (La Jolla, Encinitas, etc.), Riverside County (Moreno Valley, Murrieta, etc.), Orange County (Irvine, Newport Beach, etc.), and beyond to have access to high-tech, high-touch fertility care. On the East Coast, our New York City fertility clinic is easily accessible to patients throughout the Tri-State Area.

SAN DIEGO Fertility Center

MENU

Call Today! +1 858 461 6332

Call Today! +1 858 461 6332

APPOINTMENTS

San