John R. Parker, Jr. (SBN 257761)
jrparker@almeidalawgroup.com
ALMEIDA LAW GROUP LLC
3550 Watt Avenue, Suite 140
Sacramento, California 95608
Tel: (916) 616-2936

Attorneys for Plaintiff & the Classes

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA

B.W. and JANE DOE, *individually and on behalf of all others similarly situated*, and

Plaintiffs,

v.

SAN DIEGO FERTILITY CENTER MEDICAL GROUP, INC., and IVY FERTILITY SERVICES, LLC.

Defendants.

Case No. '24CV0237 LL BLM

CLASS ACTION COMPLAINT

FOR:

1. **ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2511(1), *et seq.*;**
2. **VIOLATION OF CAL. PENAL CODE §§ 630, *et seq.*;**
3. **VIOLATION OF CAL. CIVIL CODE §§ 56, *et seq.*;**
4. **VIOLATION OF CAL. CONST. ART. 1 § 1;**
5. **INTRUSION UPON SECLUSION;**
6. **BREACH OF IMPLIED CONTRACT;**
7. **LARCENY/RECEIPT OF STOLEN PROPERTY, VIOLATION OF**

CALIFORNIA PENAL CODESECTION 496(a) and (c); AND

8. UNJUST ENRICHMENT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs B.W. and Jane Doe ("Plaintiffs") bring this class action lawsuit, on behalf of themselves and all others similarly situated (the "Class Members"), against San Diego Fertility Center Medical Group, Inc. ("SDFC") and Ivy Fertility Services, LLC. ("Ivy Fertility," collectively "Defendants"). The allegations set forth herein are based on Plaintiffs' personal knowledge and on information and good faith belief as to all other matters based upon investigation by counsel.

INTRODUCTION

1. One in 8 couples has trouble getting pregnant or carrying a pregnancy, and 7.4 million women have received infertility treatment.[1] Despite the prevalence of infertility, information concerning fertility and reproductive health is among the most confidential and sensitive information

[1] *See How to Support Someone Experiencing Infertility*, https://www.nm.org/healthbeat/healthy-tips/emotional-health/How-to-Support-Someone-Experiencing-Infertility (last visited February 1, 2024).

in our society. According to a recent study, most infertile women choose to keep their struggle private from family or friends.[2]

2. Regarding the need to keep information about reproductive health private, the Department of Health and Human Services has noted:

> A positive, trusting relationship between individuals and their health care providers is essential to an individual's health and well-being. The prospect of releasing highly sensitive PHI can result in medical mistrust and the deterioration of the confidential, safe environment that is necessary to quality health care, a functional health care system, and the public's health generally. That is even more true in the context of reproductive health care, given the potential for stigmatization and other adverse consequences to individuals resulting from disclosures they do not want or expect.[3]

3. The mishandling of such private and sensitive health information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[4] Simply put, if people do not trust that their sensitive private

---

[2] *See What to Say to Someone Struggling With Infertility*, https://www.nytimes.com/2020/04/17/parenting/support-friend-infertility.html (last visited February 1, 2024).

[3] *See HIPAA Privacy Rule To Support Reproductive Health Care Privacy*, https://www.federalregister.gov/documents/2023/04/17/2023-07517/hipaa-privacy-rule-to-support-reproductive-health-care-privacy (last visited February 1, 2024).

[4] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more

information will be kept private and secure, they may be less likely to seek medical and fertility treatment which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

Defendants Collect a Significant Amount of Private Information

4. Defendant Ivy Fertility, is "an internationally recognized network of fertility clinics, offers advanced reproductive technologies across the United States," including California.[5]

5. Ivy Fertility "unites top-performing reproductive clinics," including Defendant SDFC "behind a common goal: providing patients extraordinary medical care for their family-building needs."[6]

6. Among the many clinical websites, portals, and patient appointment webpages (collectively, "Web Properties") owned and operated by Defendant Ivy Fertility are the following:

- San Diego Fertility Center – https://www.sdfertility.com/ and https://app.ivyfertility.com/contact-us/sdfc/scheduleconsultation

---

verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."), https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited Jan. 30, 2024).

[5] *See* https://www.ivyfertility.com/about (last visited Jan. 31, 2024).

[6] *Id*.

- 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/
- Nevada Center for Reproductive Medicine – https://nevadafertility.com/
- Nevada Fertility Center – https://www.nvfertility.com/
- Utah Fertility Center – https://utahfertility.com/
- Virginia Fertility and IVF – https://www.vafertility.com/

7. Defendant SDFC, a privately held California corporation established in 1996, operates four fertility clinics, with three locations in California (in Del Mar, Mission Valley and Temecula) and one in New York City.[7]

8. SDFC offers fertility treatments, including infertility testing and diagnosis, in-vitro fertilization ("IVF"), PGD-PGS gender selection, LGBT fertility, male infertility, egg freezing, and fertility preservation.[8]

9. As part of the medical services it provides, Ivy and SDFC own, control and maintain a website for its clinic, https://www.sdfertility.com/ ("Website").

[7] *See* https://www.sdfertility.com/ (last visited Jan. 30, 2024).

[8] *Id*.

10. Defendants actively encourage patients and prospective patients to use the Web Properties, including the Website, to communicate with their healthcare providers; manage medical appointments for fertility services; search medical conditions concerning fertility and treatment options; and much more. The Website invites patients to share and search for personal medical information about their own reproductive health. And patients, trusting that this extremely private and sensitive information will be safeguarded, share intimate and personal medical information with SDFC through the Website.

11. SDFC boldly proclaims to its patients in its "Privacy Policy" that it is "committed to respecting your privacy" and that it does "not share tracking information with unaffiliated companies, and [does] not allow other companies to place cookies on our Site."[9]

12. As described in more detail below, those statements are false.

Defendants Utilized Tracking Technologies to Monetize Users' Private Information.

13. Plaintiffs and Class Members who visited and used SDFC's Website and Defendants' Web Properties (collectively, the "Users") reasonably believed that they were communicating only with their trusted healthcare providers.

14. At no point have Defendants, despite intentionally incorporating invisible tracking codes from unauthorized third parties into their Web Properties and servers, informed Users that their personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "PII/PHI" or "Private Information") communicated via their

[9] *Disclaimer and Privacy Policy*, https://www.sdfertility.com/resources/disclaimer (last visited Jan. 30, 2024).

Web Properties was intentionally disclosed to a third party—let alone Facebook,[10] which has a sordid history of privacy violations.[11]

15. However, unbeknownst to Plaintiffs and Class Members, Defendants installed tracking technologies on their Web Properties to collect and disclose their Private Information to unauthorized third parties for its own pecuniary gain.

16. Specifically, Defendants embedded undetectable tracking Facebook pixels (the "Pixels" or "Facebook Pixels") on the Web Properties, including the Website, which transmit an incredible amount of personal and protected data about its Users to Meta Platforms, Inc., d/b/a Meta ("Meta" or "Facebook"). The collection and transmission of this information is instantaneous, invisible and occurs without any notice to—and certainly no consent from—the Users.[12]

17. The Facebook Pixel, installed and configured by Defendants, is a piece of code that "tracks the people and [the] type of actions they take"[13]

---

[10] Meta Platforms, Inc. is doing business as "Meta" and "Facebook." The terms "Meta" and "Facebook" are used interchangeably throughout.

[11] This Court will not have to look far to find evidence of Meta's violations of privacy laws. Just in May of last year, for instance, the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html (last visited Jan. 30, 2024).

[12] Healthcare providers that use analytics tools like the Facebook Pixel or Google Analytics on their websites may also have those tools embedded on a patient portal login page or even inside a patient portal.

[13] *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Jan. 31, 2023).

as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).

18. The pixels—which are configured by the website owners, here, Ivy Fertility and SDFC—collect and transmit information from Users' browsers to unauthorized third parties, including, but not limited to, Facebook (collectively, "Pixel Information Recipients").[14]

19. Together with the patients' Private Information, the data sent to Facebook also discloses Users' unique and persistent Facebook ID ("Facebook ID" or "FID") which allows Facebook and other third parties to personally identify those Users and associates their Private Information with their Facebook profile.[15]

---

[14] The pixel itself is a small snippet of code placed on webpages by the website owner. The process of adding the pixel to a webpage is a multi-step process that, as described in detail in *section E*, must be undertaken by the website owner such as SDFC.

While this Complaint primarily focuses on how Defendants embedded the Facebook Pixel on their Websites to collect and disclose Users' Private Information, other secret tracking technologies embedded by Defendants—such as Google Analytics, Bing and Twitter tracking codes—also collect such Private Information, and the respective tech companies have the capability to link it to specific user profiles.

[15] The Facebook ID is a string of numbers Facebook uses to identify and connect to a User's Facebook profile. Facebook creates a Facebook ID automatically, whether or not you choose to create a username. *See* https://www.facebook.com/help/211813265517027 (last accessed Jan. 30, 2024). Thus, Facebook, which creates and maintains the Facebook ID directly connected to a User's Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it.

Defendants' Disclosure of Private Information Without Consent Violates the Law.

20. In recent months, and in stark contrast to Defendants, several medical providers that used the Facebook Pixel in a similar way have provided their patients with notices of data breaches caused by the Pixel transmitting their information to third parties.[16]

21. Simply put (and as detailed herein), covered entities such as Defendants are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third party without express and informed consent from each patient. Neither Plaintiff nor any other Class Members were provided—much less signed—a written authorization permitting Defendants to disclose their Private Information to Facebook or any other third-party data brokers.

22. As recognized by both the Federal Trade Commission ("FTC") and the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS"), healthcare companies' use of tracking technologies to collect and divulge their patients' sensitive and confidential information is an extremely serious data security and privacy issue:

---

[16] *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Jan. 30, 2024); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), available at https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited Jan. 30, 2024); *Novant Health notifies patients of potential data privacy incident* (Aug. 12, 2022), available at https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx (last visited Jan. 30, 2024).

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***[17]

23. Similarly, the OCR is clear that "[r]egulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the Health Insurance Portability and Accountability Act ("HIPAA") Rules."[18]

24. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

---

[17] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), *available at* https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Jan. 30, 2024).

[18] The OCR Bulletin, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis added) (last visited Jan. 30, 2024).

25. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs, and IP addresses.[19]

Defendants Derive Significant Value from Users' Private Information

26. There is no anonymity in the information disclosed to Facebook for marketing and analytics purposes; that is, the Pixel collects and discloses a substantial "data packet" coupled with the FID so that Defendants can, among other things, send targeted advertisements to Users based on their sensitive and protected Private Information. Defendants also use this impermissibly obtained data for analytics purposes to gain additional insights into how its patients use their Web Properties.[20]

27. Operating as designed and as implemented by Defendants, the Pixel disclosed information that allows a third party (*e.g.*, Facebook) to know when and where a specific patient was seeking confidential medical care, the medical condition(s) that patients inquired about, and the precise care the patient sought or received. Facebook, in turn, sells Plaintiffs' and Class

---

[19] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 11, 2024).

[20] SDFC unquestionably is required to inform its Users if it deploys tracking technologies on its Web Properties so that Users can make informed decisions as to whether they want their information to be collected, disclosed, and used in this manner. The OCR Bulletin is, again, instructive: "disclosures of PHI to tracking technology vendors for marketing purposes, ***without individuals' HIPAA-compliant authorizations,*** would constitute impermissible disclosures." *See* OCR Bulletin, *supra* note 15.

Members' Private Information to third-party marketers who target Plaintiffs' and Class Members' Facebook accounts based on that Private Information.

28. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, the User's first name, last name, email address, phone number, zip code, and city of residence entered on the Website. The data packets also include the buttons a User clicks and the words a User types into a search bar.

29. For instance, when a User uses Defendants' Web Properties where tracking technologies, such as the Facebook Pixel are present, the Pixel transmits the contents of their communications to Facebook, including, but not limited to: (i) medical reproductive and fertility services and treatments sought; (ii) patient status; (iii) scheduling of appointments; (iv) accessing and viewing the bill page; (v) the text of URLs visited by the User; (vi) User's email address and phone number and (vii) other information that qualifies as PII and PHI under federal and state laws. The data in the "data packets" is then linked to a specific internet protocol ("IP") address, which is itself protected information under HIPAA, as well as the Users' Facebook ID.

30. By installing the Facebook Pixel and other tracking technologies, Defendants effectively planted a bug on Plaintiffs' and Class Members' web browsers and caused them to unknowingly disclose their private, sensitive and confidential health-related communications to Facebook (and, upon information and good faith belief, other third-party data brokers).

31. The information intercepted by the Pixels and third-party tracking technologies is used to build incredibly fulsome and robust

marketing profiles for individual Users and create targeted advertisements based on the medical conditions and other Private Information disclosed. Despite the clear and unequivocal prohibition on the disclosure of PHI without consent, Ivy Fertility and SDFC chose to use the Pixel data for marketing purposes to bolster their revenue.

32. Simply put, Defendants put their desire for revenue over their patients' privacy rights.

Defendants' Conduct Caused Concrete & Demonstrable Harm to Users.

33. As healthcare providers, Defendants have certain duties and obligations to their patients. Defendants breached those duties and obligations in one or more of the following ways: (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) failing to obtain the consent of Plaintiffs and Class Members to disclose their PII and PHI to Facebook or other third parties; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' PII and PHI through the Pixels; (v) failing to warn Plaintiffs and Class Members about the tracking technology; and (vi) otherwise failing to design and monitor their Web Properties to maintain the confidentiality and integrity of patient PII and PHI.

34. Plaintiffs and Class Members have suffered injury because of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) compromise and disclosure of Private Information; (iv) diminution of value of their Private Information; (iv)

statutory damages; and (v) the continued and ongoing risk to their Private Information.[21]

35. Plaintiffs seek to remedy these harms for themselves and a class of all others similarly situated and therefore assert causes of action for (1) Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq*., Unauthorized Interception, Use and Disclosure; (2) Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*; (3) Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq*.; (4) Invasion of Privacy under California Constitution; (5) Common Law Intrusion upon Seclusion; (6) Breach of Implied Contract; (7) Violation of California Penal Code § 496, *et seq.*; and (8) Unjust Enrichment.

PARTIES

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

37. As detailed herein, Plaintiff B.W. accessed Defendants' Web Properties, including the SDFC Website, on her computer and mobile devices and used the Website to look for providers of fertility and infertility treatments, review fertility treatments' costs and insurance options, and submit forms with personal medical information. Plaintiff B.W. has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

[21] The exposed Private Information of Plaintiffs and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties often offer the unencrypted, unredacted Private Information for sale to criminals on the dark web for use in fraud and cyber-crimes.

38. Plaintiff Jane Doe is a natural person and resident of the city of San Diego in San Diego County, California.

39. As detailed herein, Plaintiff Jane Doe accessed Defendants' Web Properties, including the SDFC Website, on her mobile device and used the Website to look for providers of fertility treatments, review fertility treatments' costs and insurance options, pay bills and submit forms with personal medical information. Plaintiff has used the same device to maintain and access an active Facebook account throughout the relevant period in this case.

40. Defendant SDFC is a California corporation with its principal place of business and corporate headquarters at 11425 El Camino Real, San Diego, California 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 covered entities under HIPAA.

JURISDICTION & VENUE

43. This Court has "federal question" jurisdiction given the federal claims alleged by Plaintiff. This Court also has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

44. The Court has personal jurisdiction over Defendants Ivy Fertility and SDFC because their principal places of business and headquarters are located in San Diego, County of San Diego, State of California, they

regularly engage in business in the State of California and in County of San Diego, and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this county.

45. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendants governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class Members' Private Information; Defendants principal places of business are located in this District; Defendants collect and redistribute Class Members' Private Information in this District and Defendants caused harm to Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Make Clear that the Use of Tracking Technologies to Collect & Divulge Private Information Without Informed Consent is Illegal.

46. Defendants' surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the FTC and the OCR of HHS have—in recent months—reiterated the importance of and necessity for data security and privacy concerning health information.

47. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Prenom, BetterHelp, GoodRx, and Flo Health* ***make clear that the fact that a consumer is using a***

particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."[22]

48. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information***.[23]

49. The federal government is taking these violations of health data privacy and security seriously, evidenced by recent high-profile FTC settlements against several telehealth companies.

50. For example, the FTC recently imposed a $1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms, including Facebook, Google and Criteo. The FTC also reached a $7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared

---

[22] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Jan. 30, 2024).

[23] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization).

customer health data with Facebook and Snapchat for advertising purposes. Likewise, the FTC reached a settlement with Flo Health, Inc. related to information about fertility and pregnancy that Flo fertility-tracking app was improperly sharing with Facebook, Google, and other third parties. And Easy Healthcare was ordered to pay a $100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app, Premon, shared health data for advertising purposes.[24]

51. Even more recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about using online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the "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," and warned about "[i]mpermissible disclosures of an individual's personal health information

[24] *See* How FTC Enforcement Actions Will Impact Telehealth Data Privacy, https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy (last visited Jan. 30, 2024); *see also* Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), available at www.law360.com/articles/1571369/ftc-targets-goodrx-in1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc (last visited Jan. 30, 2024); https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google (last visited Jan. 30, 2024).

to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch 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."[25]

52. The Office for Civil Rights at HHS has made clear, in a recent bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology 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.***[26]

53. The OCR Bulletin *reminds* healthcare organizations regulated under HIPAA that they may use third-party tracking tools, such as Google Analytics or Pixels *only in a limited way* to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[27]

54. The OCR Bulletin discusses the harms that disclosure may cause patients:

---

[25] *See* OCR Bulletin, *supra* note 15.

[26] *Id*.

[27] *See id*.

> 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.***[28]

55. Moreover, investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on the digital properties of hospitals, health care providers and telehealth companies to monetize their Users' Private Information.

56. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[29]

57. And, in the aptly titled report *"Out of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech*

---

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

[29] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Jan. 30, 2024).

Companies, a joint investigation by STAT and THE MARKUP of 50 direct-to-consumer telehealth companies reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world's largest advertising platforms.[30]

58. Many healthcare sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn, and/or Pinterest—that collected patients' answers to medical intake questions.[31]

B. Tracking Pixels.

59. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting, for example, serving online advertisements to people who have previously engaged with a business's website—and other marketing.

60. Here, a User's web browser executes the Pixels via instructions within each webpage of SDFC's Website and Defendants' appointment forms such as https://app.ivyfertility.com/contact-us/sdfc/scheduleconsultation (and, upon information and good faith belief, within Ivy Fertility's Patient Portal) to communicate certain information (within parameters set by Defendants) directly to the corresponding Pixel

[30] Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools* (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 (last visited Jan. 30, 2024).

[31] *See id.* (noting that "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

Information Recipients, including Facebook—at the same time as the User's browser is sending this information to Defendants.

61. The Pixels can also share the Users' identifying information for easy tracking via "cookies"[32] stored on their computer by any of the Pixel Information Recipients with whom they have an account. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser.

62. The Facebook Pixel can access this cookie and send certain identifying information like the User's Facebook ID to Facebook along with the other data relating to the User's Website inputs. The same is true for Facebook and the other Pixel Information Recipients, which also create cookies that are stored in the User's computer and accessed by the Pixels to identify the User.

63. The Pixels are programmable, meaning that Defendants control which of the webpages on the Website contain the Pixels and which events are tracked and transmitted to the Pixel Information Recipients.

64. Defendants used the data they collected from Plaintiffs and Class Members, without their consent, to improve their advertising and bolster their revenue.

C. Conversions API.

65. In addition to the Facebook Pixel, Facebook Conversions API and similar tracking technologies allow businesses to send web events, such

[32] "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." *See* https://www.cloudflare.com/learning/privacy/what-are- cookies/ (last visited Jan. 30, 2024).

as clicks, form submissions, keystroke events and other actions performed by the user on the Website, from their own servers to Facebook and other third parties.[33]

66. Conversions API creates a direct and reliable connection between marketing data (such as website events and offline conversations) from Defendants' servers to Facebook.[34]

67. In doing so, Defendants store Plaintiffs' and Class Members' Private Information on their own servers and then transmit it to unauthorized third parties like Facebook.

68. Conversions API is an alternative method of tracking versus the Meta Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology, whereas pixels are "client-side"—executed on users' computers in their web browsers.

69. Because Conversions API is server-side, it cannot access the Facebook c_user cookie to retrieve the Facebook ID.[35] Therefore, other

---

[33] *See* https://revealbot.com/blog/facebook-conversions-api/ (last visited Jan. 30, 2024).

[34] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 30, 2024).

[35] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited Jan. 30, 2024).

roundabout methods of linking the user to their Facebook account are employed.[36] For example, Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Facebook Pixel and Conversions API are executed.[37]

70. Conversions API tracks the user's website interactions, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API 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 impacts both online and offline results."[38]

71. Defendants installed the Meta Pixel and, upon information and good faith belief, Conversions API, as well as other tracking technologies, on many (if not all) of the webpages within their Web Properties (including webpages for patients to pay their bills or for prospective patients seeking appointments) and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with Facebook (and with other Pixel Information Recipients via their proprietary

---

[36] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited Jan. 30, 2024).

[37] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel- and-server-events (last visited Jan. 30, 2024).

[38] *About Conversions API*, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 30, 2024).

tracking codes)—communications that included Plaintiffs' and Class Members' Private Information.

D. Defendants' Method of Transmitting Plaintiffs' & Class Members' Private Information via Pixels.

72. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (computer, tablet or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome, Mozilla's Firefox, Apple's Safari, and/or Microsoft's Edge browsers).

73. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' devices as their web browsers query the server through the internet.

74. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

1. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF to file a motion to a court.)

2. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when

visiting one website to an entirely different website.

3. **HTTP response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP request. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data.

75. A patient's HTTP request essentially asks Defendants' Web Properties to retrieve certain information (such as a set of health screening questions). The HTTP response sends 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 participants' screens as they navigate Defendants' Web Properties.

76. Every website is comprised of Markup and "Source Code." Source Code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

77. 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.

78. The Pixels are Source Code that do just that—they surreptitiously transmit a Website User's communications and inputs to the corresponding Pixel Information Recipient, much like a traditional wiretap.

79. For example, when individuals visit Defendants' Web Properties, including the Website or Defendants' appointment page, via an HTTP request to Defendants' server, Defendants' server sends an HTTP response (including the Markup) that displays the webpage visible to the User, along with Source Code (including the Pixels).

80. Thus, Defendants are, in essence, handing their patients a tapped website and, once a webpage is loaded into the patient's browser, the

software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications—intended only for Defendants—and instantaneously transmit those communications to Facebook or another corresponding Pixel Information Recipient

81. Third parties like Facebook (and other Pixel Information Recipients) place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third party can identify the specific user associated with the information intercepted (in this case, highly sensitive Private Information).

82. Defendants intentionally configured Pixels installed on their Web Properties to capture both the "characteristics" of individual patients' communications with their Web Properties (their IP addresses, Facebook ID, cookie identifiers, device identifiers, emails and phone numbers) and the "content" of these communications (the buttons, links, pages, and tabs they click and view related to their health conditions and services sought from Defendants).

83. Defendants' appointment software system was also designed to permit licensees to deploy "custom analytics scripts" within the webpage. For example, this would allow the website owner to deploy the Facebook Pixel or Google Analytics to capture the transmission of Private Information, including medical and health-related information and communications to third parties.[39]

[39] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at

84. Upon information and belief, Defendants intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiffs' and Class Members' status as medical patients;

b. Plaintiffs' and Class Members' communications with Defendants through their Web Properties, including medical conditions for which they sought treatments and treatments sought;

c. Plaintiffs' and Class Members' searches for appointments, location of treatments, medical conditions, and treatments sought; and

d. PII, including but not limited to patients' locations, IP addresses, device identifiers, individual's unique Facebook ID and other unique personal identifiers such as email and phone number.

85. Through the Web Properties, Defendants share their patients' identities and online activity, including information and search results related to their private medical treatment.

86. For example, when they visit the SDFC Website, SDFC patients can search fertility treatments by selecting the "Treatments" menu which takes them to a list of services offered by SDFC. Patients are then directed to a variety of sensitive fertility treatments, including, for example SDFC's "Surrogacy Program." On those pages the User can further narrow their search results by the type of surrogacy service SDFC offers, including gestational surrogacy, egg donorship, or surrogacy and IVF.

87. The User's selections and filters are transmitted to Facebook via the Meta Pixels, even if they contain the User's treatment, procedures, medical conditions, or related queries, without alerting the User, and the images below confirm that the communications Defendant SDFC sends to

---

https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Jan. 30, 2024).

Facebook contain the User's Private Information and personal identifiers, including but not limited to their Facebook ID, IP Address, datr and fr cookies, along with the search filters the User selected.

88. Here, the search parameters set by the patient and the patient's FID number are being shared together, thereby allowing Facebook to make the direct connection between the search parameters and each individual patient's FID. Even without the FID, other identifying information like IP address or device identifier is captured by the Pixel and transmitted to Facebook.

89. Facebook categorizes this event as a "PageView," which indicates that the patient viewed the webpage.

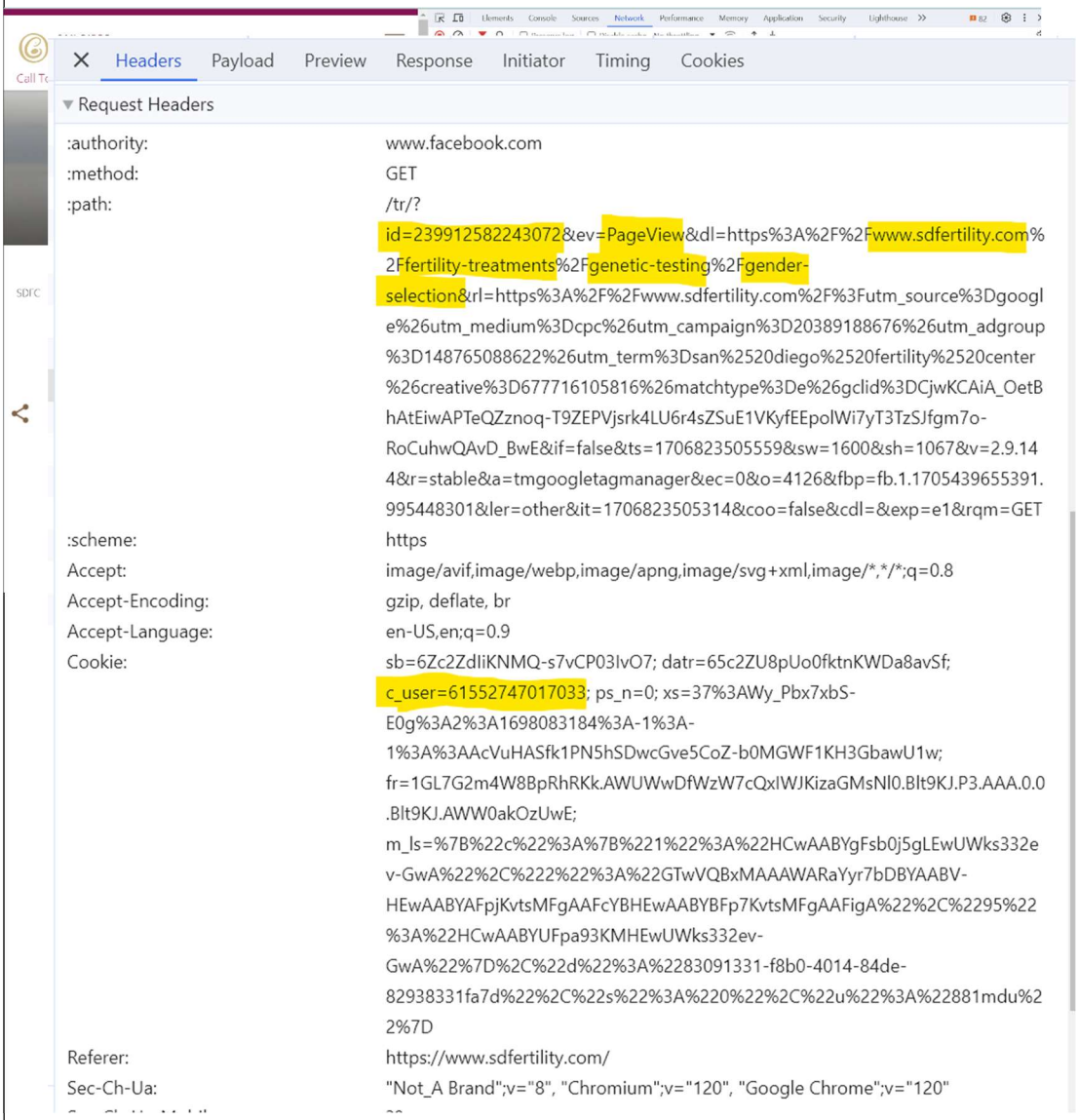
90. Every time Defendants send a patient's Website activity data to Facebook, that patient's personally identifiable information is also disclosed, including their FID. An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who knows or has acquired someone's FID. Facebook admits as much on its website. Indeed, ordinary people who come to acquire an FID can connect to the corresponding Facebook profile.

91. A user who accesses Defendants' Web Properties while logged into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted Facebook ID. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies embedded on SDFC's website to link to FIDs and corresponding Facebook profiles.

92. For example, a fertility patient who searches for "genetic testing

options" can search for various services, including "gender selection."[40]

Figures 1-2: Defendant's transmission to Facebook of User's navigating SDFC's Genetic Testing "Gender Selection":



93. The fourth line of highlighted text, "id: 239912582243072," refers to Defendants' Pixel ID for the Website and confirms that Defendants have downloaded the Pixel into its Source Code on this particular web

[40] See *Genetic Testing*, https://www.sdfertility.com/fertility-treatments/genetic-testing/gender-selection.

page.[41]

94. In that same line of text, "ev:" is an abbreviation for event, and "PageView" is the type of event. Here, this event means that Defendants' Pixel is sending information about the webpage being viewed, which can include information like page title, URL and page description.

95. The remaining lines of text identify the User as a patient: (i) seeking medical care from Defendant SDFC via www.sdfertility.com who is searching for "fertility treatments," (ii) including "genetic testing," and more specifically, (iii) testing for "gender selection."

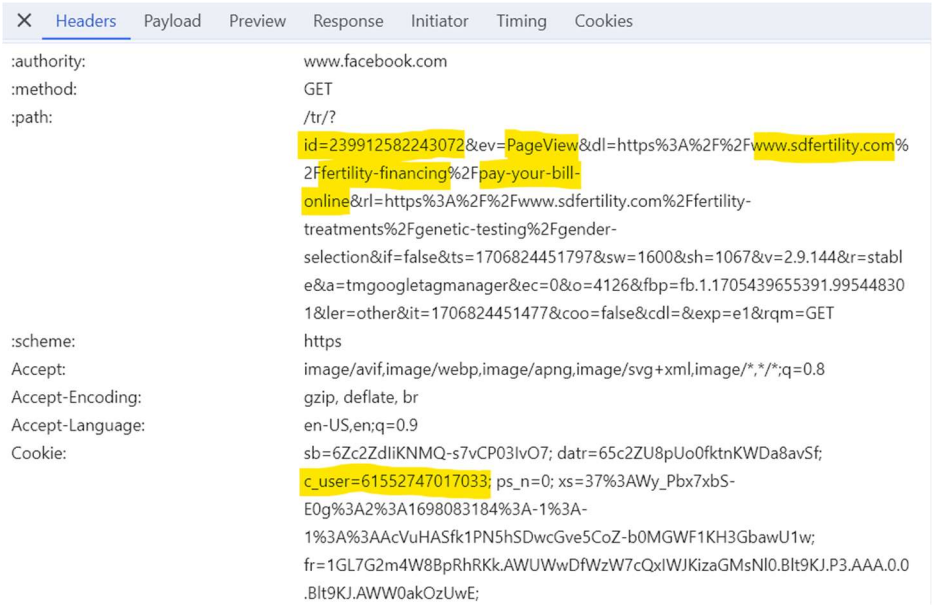
96. Finally, the second line of highlighted text ("GET"), demonstrates that Defendants' Pixel sent the User's communications, and the Private Information contained therein, alongside the User's personal identifiers, including Facebook ID and other cookies.

97. As Users move further into SDFC's Website, Defendants continue to disclose user details through PageView and SubscribedButtonClick events. Defendants disclosed users': (i) appointment booking activities; (ii) browsing medical conditions and treatments; (iii) bill payment activities; (iv) submission of forms containing personal medical information and, upon information and good faith belief, (v) patient portal activities.

98. For example, Defendants also share details about Users' bill payment activities. When a User navigates to the Online Bill Payment page,

[41] Defendants have embedded at least six Meta Pixels on their Web Properties, including those with ID numbers 1024940958846869, 1666143710464689, 239912582243072, 305890348536996, 6707064245994307 and 951372101648912. For example, Pixel 239912582243072, installed on the SDFC Website and identified in Figure 2, is installed in each of the websites that make up Defendants' Web Properties.

Defendants send PageView events revealing that the user was on the page for "fertility financing."[42] Defendants inform Facebook that the User was on the page for patients to "pay your bill online," *see* **Figure 3**:[43]



99. When a User searches for a specific doctor, Defendants also send that information to Facebook through PageView events, *see* **Figure 4**:[44]

//////

//////

//////

//////

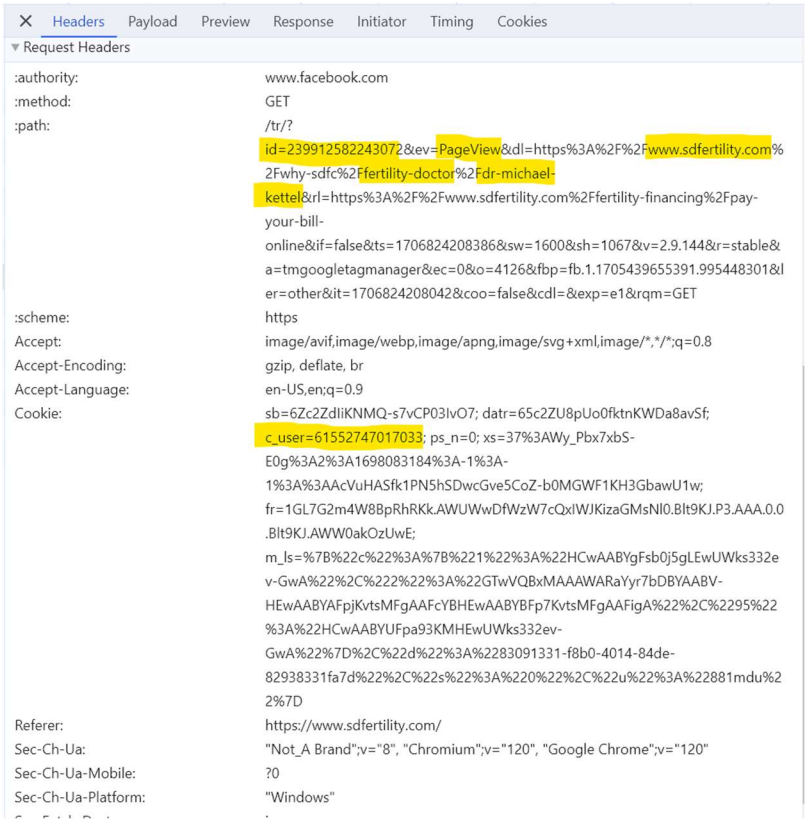
//////

[42] As mentioned previously, Defendants have several Pixels embedded in the web pages Source Code, which all capture PageView events (as well as "SubscribedButtonClick" events on pages where Users engage with the Web Properties by clicking buttons).

[43] *See* https://www.sdfertility.com/fertility-financing/pay-your-bill-online (last visited February 1, 2024).

[44] *See* https://www.sdfertility.com/why-sdfc/fertility-doctor/dr-michael-kettel (last visited February 1, 2024).

//////



100. Defendants also disclose the specific location the User searches for. In the figure below, Defendants disclose that the User is seeking to contact a medical provider at the "Temecula Valley" location, *see* **Figure 5**:[45]

//////

//////

//////

//////

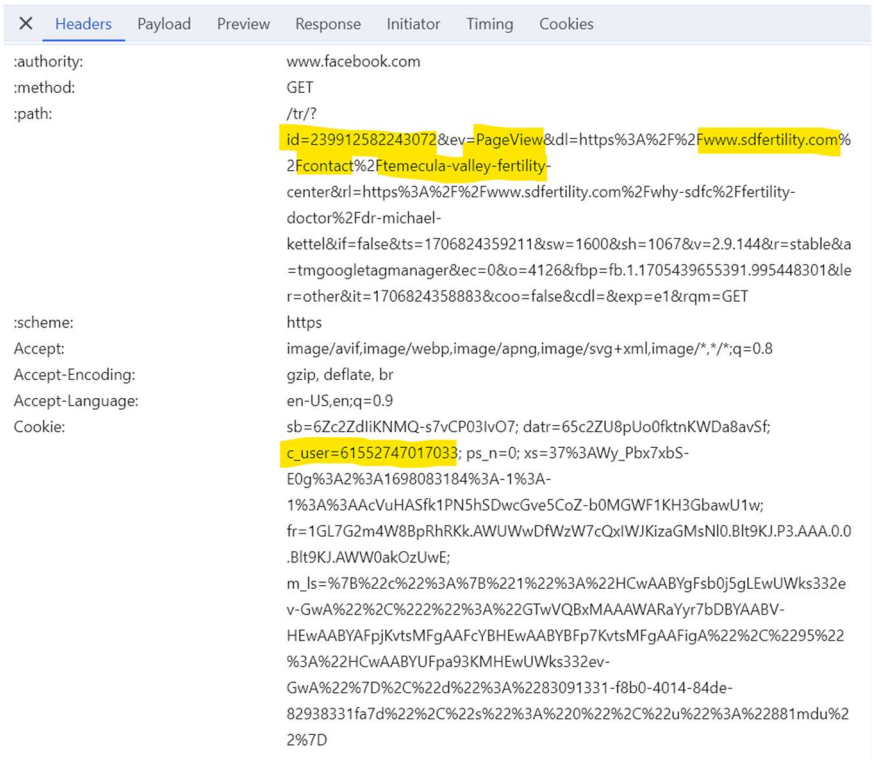
//////

//////

//////

//////

[45] *See* https://www.sdfertility.com/contact/temecula-valley-fertility-center (last visited February 1, 2024).



Headers Payload Preview Response Initiator Timing Cookies

:authority:	www.facebook.com
:method:	GET
:path:	/tr/?id=239912582243072&ev=PageView&dl=https%3A%2F%2Fwww.sdfertility.com%2Fcontact%2Ftemecula-valley-fertility-center&rl=https%3A%2F%2Fwww.sdfertility.com%2Fwhy-sdfc%2Ffertility-doctor%2Fdr-michael-kettel&if=false&ts=1706824359211&sw=1600&sh=1067&v=2.9.144&r=stable&a=tmgoogletagmanager&ec=0&o=4126&fbp=fb.1.1705439655391.995448301&ler=other&it=1706824358883&coo=false&cdl=&exp=e1&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9
Cookie:	sb=6Zc2ZdliKNMQ-s7vCP03lvO7; datr=65c2ZU8pUo0fktnKWDa8avSf; c_user=61552747017033; ps_n=0; xs=37%3AWy_Pbx7xbS-E0g%3A2%3A1698083184%3A-1%3A-1%3A%3AAcVuHASfk1PN5hSDwcGve5CoZ-b0MGWF1KH3GbawU1w; fr=1GL7G2m4W8BpRhRKk.AWUWwDfWzW7cQxlWJKizaGMsNl0.Blt9KJ.P3.AAA.0.0.Blt9KJ.AWW0akOzUwE; m_ls=%7B%22c%22%3A%7B%221%22%3A%22HCwAABYgFsb0j5gLEwUWks332ev-GwA%22%2C%222%22%3A%22GTwVQBxMAAAWARaYyr7bDBYAABV-HEwAABYAFpjKvtsMFgAAFcYBHEwAABYBFp7KvtsMFgAAFigA%22%2C%2295%22%3A%22HCwAABYUFpa93KMHEwUWks332ev-GwA%22%7D%2C%22d%22%3A%2283091331-f8b0-4014-84de-82938331fa7d%22%2C%22s%22%3A%220%22%2C%22u%22%3A%22881mdu%22%7D

101. Defendants also disclose when users try to contact them to make an appointment – and where. When a User clicks the button "Appointments," the User lands on the app.ivyfertility.com "Contact Us" page and Defendants disclose that by sending PageView events to Facebook, *see* **Figure 6**:

//////

//////

//////

//////

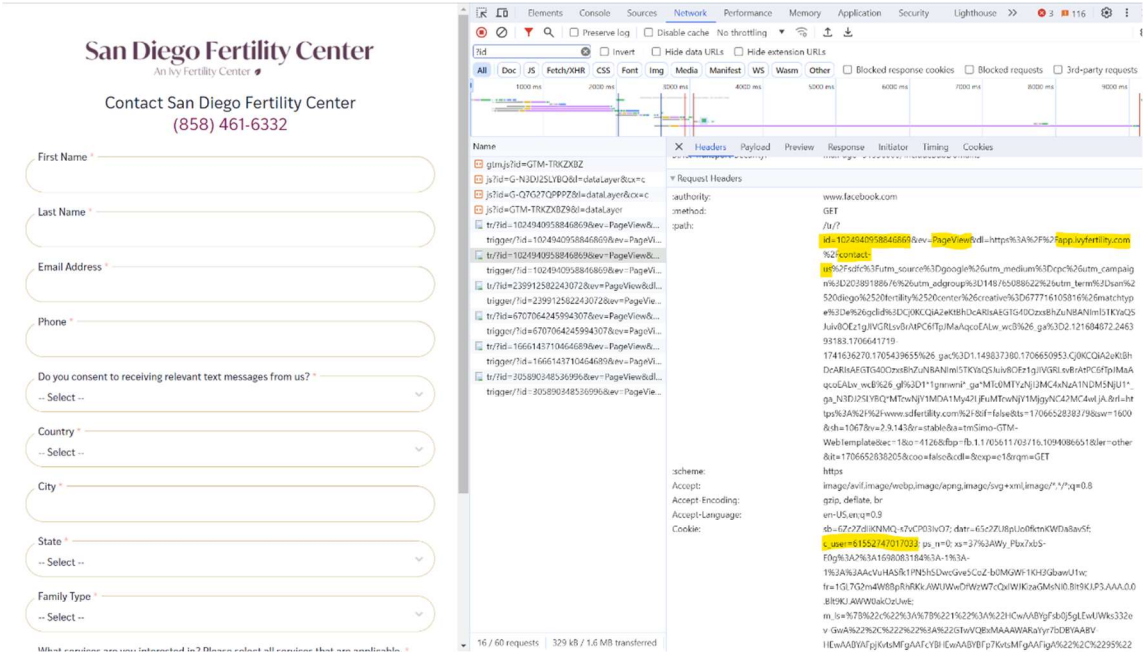
//////

//////

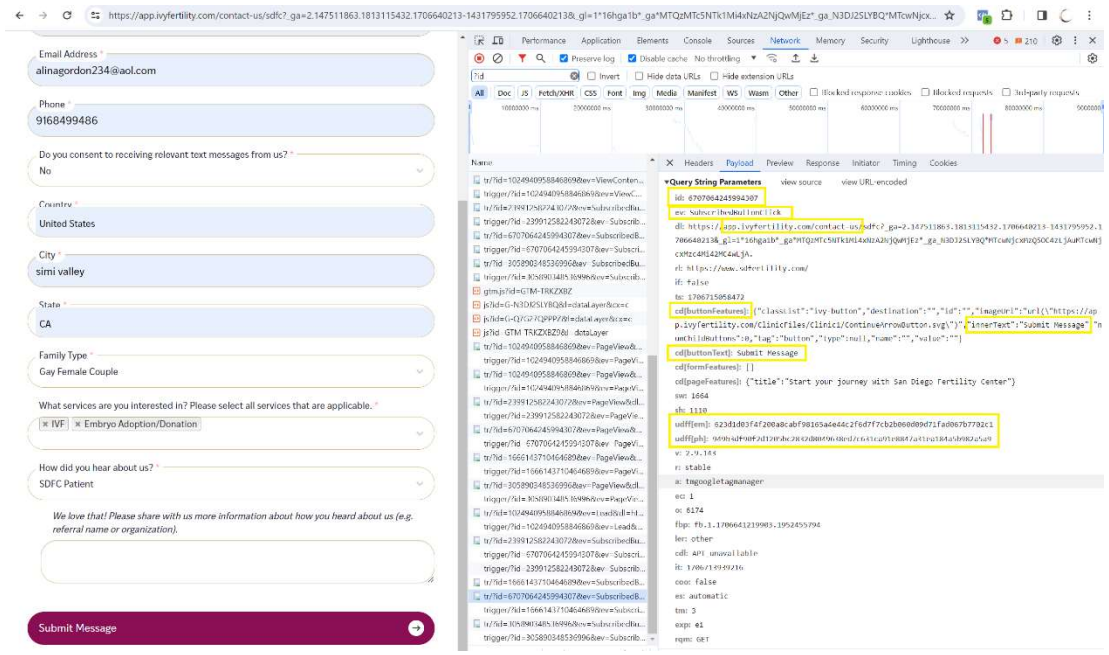
//////

//////

//////

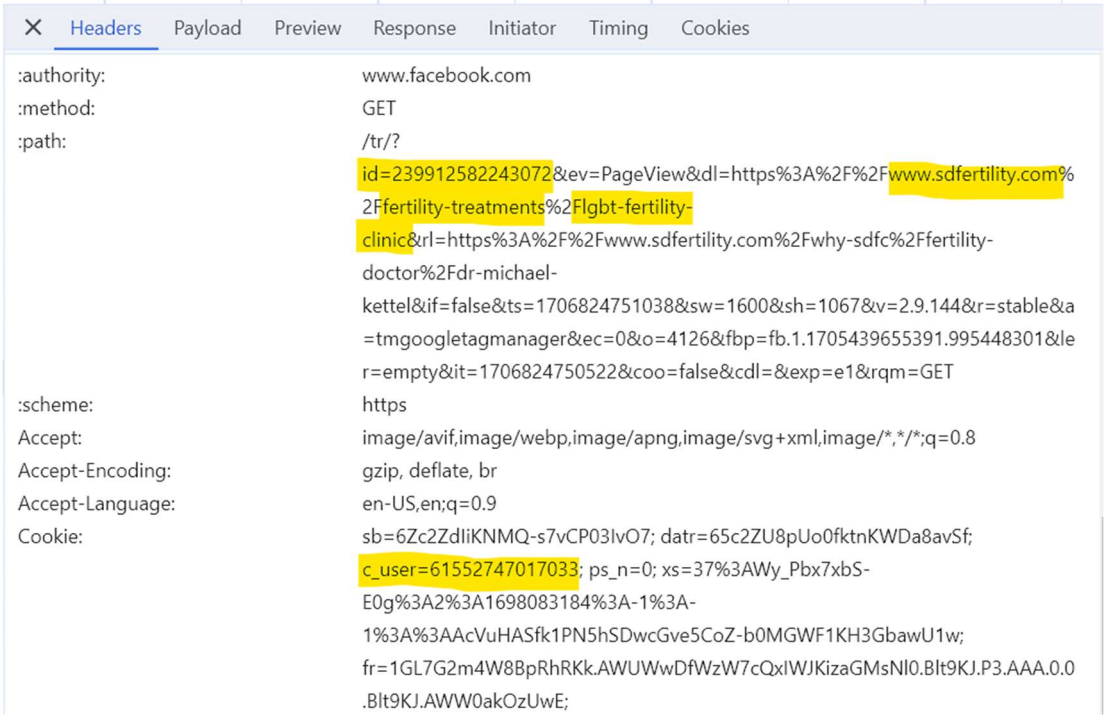


102. After a user fills out the appointment form, Defendants disclose that the user is contacting them, via a "SubscribedButtonClick" event – along with the user's email and phone number, as evidenced by the "udff" values in **Figure 7** below:



103. In addition to users' search for doctors, searches for fertility conditions and treatments, appointments and financial information, Defendants also disclose sensitive information about the sexual orientation of the User.

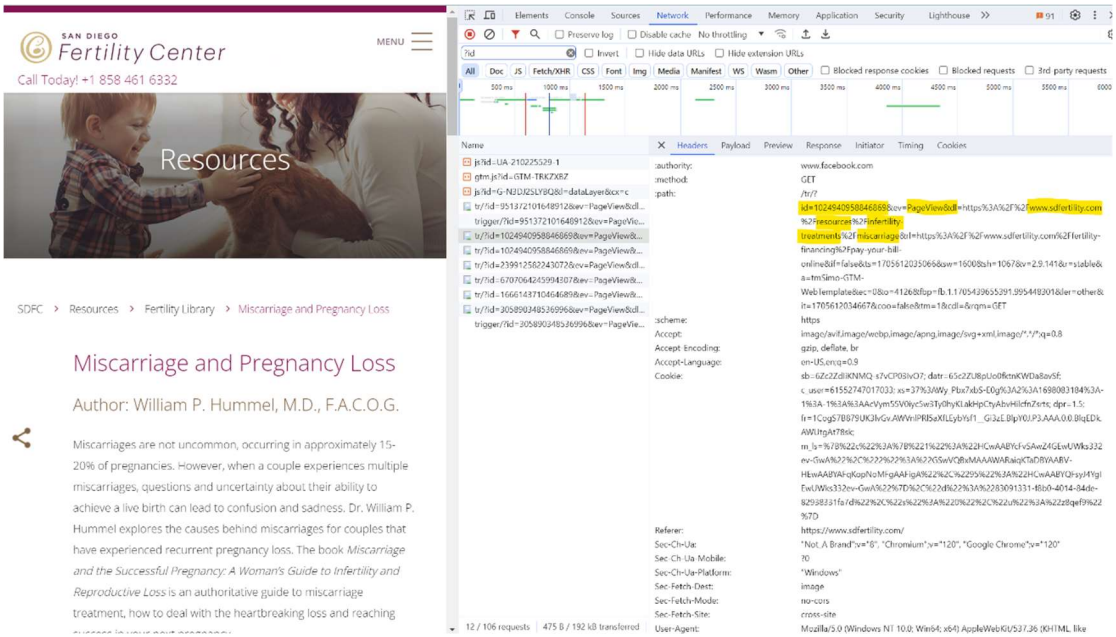
104. For example, when a user navigates to view SDFC's fertility treatments, the user can select "LGBT Family Building." When the User clicks on that option, SDFC sends PageView event to Facebook revealing that the user was on the page "lgbt-fertility-clinic." *See* **Figure 8**:[46]



105. Defendants also inform Facebook when Users view pages concerning a patients' researching resources for miscarriage and pregnancy loss. Upon a User loading the page to access the resource page for miscarriage, Defendants send PageView events. The PageView events

[46] *See* https://www.sdfertility.com/fertility-treatments/lgbt-fertility-clinic (last visited February 1, 2024).

inform Facebook that the User was on the page for "resources/infertility-treatments/miscarriage." *See* **Figure 9**:[47]



106. Defendants did not seek and did not have Plaintiffs' and Class Members' consent for sharing any of the sensitive Private Information described above.

E. Facebook's Platform & its Business Tools.

107. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021.[48] Roughly 97% of that came from selling advertising space.[49]

---

[47] *See* https://www.sdfertility.com/resources/infertility-treatments/miscarriage (last visited February 1, 2024).

[48] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Jan. 30, 2024).

[49] *Id.*

108. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendants, to utilize its "Business Tools" to gather, identify, target, and market products and services to individuals.

109. Facebook's Business Tools, including the Meta Pixel, 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.

110. In particular, the Meta Pixel "tracks the people and type of actions they take."[50]

111. The User's web browser (software applications that allow consumers to exchange electronic communications over the Internet) executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner.

112. The Pixel is thus customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

113. The process of adding the Pixel to webpages is a multi-step process that must be undertaken *by the website owner*.[51]

---

[50] *Retargeting*, *supra* note 10.

[51] *Business Help Center: How to set up and install a Meta Pixel*, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited Jan. 30, 2024); *see* Ivan Mana, *How to Set Up & Install the Facebook Pixel (in 2022)*, https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited Jan. 30, 2024).

114. Facebook guides the website owner through setting up the Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a pixel:

> 1. Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you or you can manually add code to your website.
>
> 2. Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website.[52]

115. Aside from the various steps to embed and activate the Pixel, website owners, like Defendants, must also agree to Facebook's Business Tools Terms by which Facebook requires website owners using the Meta Pixel to "represent and warrant" that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook's Business Tools (including the Pixel and Conversions API)[53] and that websites "will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information . . . ."[54]

---

[52] *Id.*

[53] *Meta Business Tools Terms*, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfbOvnb7E0sZ-wzgCW6xNLFKEOEVH_fr6JjkMINTJNqN7i1R-3MPh5caFgmdgAOxbL8&_rdr (last visited Jan. 30, 2024) ("When you use any of the Meta Business Tools to send us or otherwise enable the collection of Business Tool Data . . ., these Business Tools Terms govern the use of that data").

[54] *Id.*; *see also* Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022)

116. Once fully loaded and operational, the Pixel prompts the Users' web browser to transmit specific information based on parameters set by the website owner. This customizable nature of the Meta Pixel allows the website owner to determine which webpages contain the Pixel, which events are tracked and shared with Facebook and whether the tracked events are standard (chosen from the list of 18 provided by Facebook) or custom (defined by the website owner). For example, the Pixel can be set to capture the URLs visited by website visitors via a "PageView" event, or to capture the exact inner text of buttons clicked by a visitor, via a "SubscribedButtonClick" event.

117. The Business Tools are automatically configured to capture "Standard Events," such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[55]

---

https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story (quoting Facebook spokesman Dale Hogan as saying that it is "against [Facebook's] policies for websites and apps to send sensitive health data about people through [its] Business Tools") (last visited Jan. 30, 2024).

[55] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Jan. 30, 2024); *see also* META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Jan. 30, 2024); BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Jan. 30, 2024); APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 30, 2024).

118. Advertisers, such as Defendants, can track other User actions and can create their own tracking parameters by building a "custom event."[56]

119. When a user accesses a webpage that is hosting the Meta Pixel, their communications and interactions with the host webpage are instantaneously and surreptitiously sent to Facebook's servers—traveling from the user's browser to Facebook's server.[57]

120. This simultaneous secret transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendants' Web Properties—Defendants' own code and Facebook's embedded code.

121. In particular, Defendants tracked Users and disclosed Users' Private Information including at least the following:

- What care and treatment options Users viewed and/or sought;
- When Users clicked to request an appointment;
- Users' unique personal identifiers when they requested an appointment including their FID, email address, phone number and IP address; and
- When Users clicked to access and view the bill page,

122. Accordingly, during the same transmissions, the Web Properties routinely provide Facebook with Defendants' patients' Facebook IDs, IP addresses and/or device IDs, and the other information they input into

---

[56] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Jan. 30, 2024).

[57] Plaintiffs unequivocally and in good faith plead that Defendants' Pixel transmissions to Facebook occur simultaneously as Users navigate and use Defendants' Websites.

Defendants' Web Properties, including not only their medical searches, treatment requests, and the webpages they view, but, for those making appointments online, also their email address and phone number.

123. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[58] Plaintiffs' and Class Members' identities can be easily determined based on the Facebook ID, IP address, and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

124. Instead of taking proactive steps to verify that businesses using the Pixel obtain the required consent, Meta uses an "honor system" under which Meta assumes these businesses have "provided robust and sufficient prominent notice to users regarding the Business Tool Data collection, sharing, and usage."[59]

125. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. When the Website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the User's Facebook ID that identifies their name and Facebook profile—their real-world identity.

126. The Pixel collects data regardless of whether the visitor has an account. Facebook maintains "shadow profiles" on Users without Facebook

[58] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 30, 2024).

[59] *See* Facebook Business Tools Terms, https://www.facebook.com/legal/terms/businesstools.

accounts and links the information collected via the Meta Pixel to the User's real-world identity using their shadow profile.[60]

127. A User's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access and view the User's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

128. The Private Information disclosed via the Pixel allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to sell advertising to Defendants and other advertisers and/or sells that information to marketers who use it to online target Plaintiffs and Class Members.

129. Facebook (and other Pixel Information Recipients) track user data and communications for their own marketing purposes and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

130. Thus, without any knowledge, authorization or action by a user, website owners like Defendants use source code to commandeer the user's

[60] *See* Russell Brandom, *Shadow Profiles Are the Biggest Flaw In Facebook's Privacy Defense*, (Apr 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Jan. 30, 2024).

computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

131. In this case, Defendants employed the Pixels, among other tracking technologies, to intercept Plaintiffs' and Class Members' Private Information to Facebook and the other Pixel Information Recipients.

132. In sum, the Pixels and other tracking technologies on the Web Properties permitted Facebook and any other Pixel Information Recipient to intercept the content of Plaintiffs' and Class Members' highly sensitive communications and Private Information , which communications contained private and confidential medical information.

133. These interceptions of Plaintiffs' and Class Members' communications content were performed without Plaintiffs' or Class Members' knowledge, consent, or express written authorization.

F. Meta Encourages Healthcare Partners, Including Ivy Fertility & SDFC, to Upload Patient Lists for Ad Targeting.

134. Meta operates the world's largest social media company. Meta's revenue is derived almost entirely from selling targeted advertising. Meta's Health division is dedicated to marketing to and servicing Meta's healthcare partners. Meta defines its Partners to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

135. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

136. Meta offers an ad targeting option called "Custom Audiences."

137. When a patient takes an action on a Meta healthcare partner's website embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta matches to its users.

138. A web developer can then create a "Custom Audience" based on Events to target ads to those patients.

139. The Pixel can then be used to measure the effectiveness of an advertising campaign.[61]

140. Meta also allows healthcare partners to create a Custom Audience uploading a patient list to Meta. As Meta describes it:[62]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

---

[61] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa.

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

141. Meta provides detailed instructions for healthcare partners to send their patients' Private Information to Meta through the customer list upload. For example:[63]

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

142. Meta healthcare partners can then use the Custom Audiences derived from their patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

G. SDFC's Use of the Pixels Violated Its Own Privacy Policies.

143. Defendants publish several privacy policies that represent to patients and visitors to their Web Properties that they will keep their PHI private and secure and that they will only disclose PHI provided to them under certain circumstances, ***none of which apply here***.[64]

144. With respect to tracking technologies and analytics, although Defendants admit to using these tools to collect information about browsing activity, it does not disclose to Users that it collects their PHI.

---

[63] Create a customer list custom audience, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Jan. 30, 2024).

[64] There is a privacy policy for each of the Web Properties and while Plaintiffs cite to Defendant SDFC's policy, the allegations regarding that policy are applicable to each of the Web Properties.

145. For example, Defendant SDFC's Policy highlights that it is "committed to respecting your privacy."[65]

146. Defendant SDFC acknowledges that it collects IP addresses, cookies, and similar technologies but it claims that "[t]he IP address does not identify you personally," and the cookie technology "is not personally identifying information[.]"[66]

147. Patients and other Users of the Web Properties are not informed about, and have not consented to, the collection of their PHI and Website activity or to providing that information to a third party.

148. This is precisely the type of information for which HIPAA requires healthcare providers to utilize de-identification techniques to protect the privacy of patients.[67]

149. Despite a lack of disclosure, Defendants allow Facebook to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information that they promise to keep private.

150. Defendants breached their own privacy policies by unlawfully permitting Facebook and likely other third parties to intercept Users' Private Information without obtaining patients' consent or authorization. Facebook then read, understood, and used that Private Information for its own business purposes—i.e., selling targeted advertising to Defendants (and other

---

[65] *See* https://www.sdfertility.com/resources/disclaimer#privacy-policy (last visited January 31, 2024).

[66] *Id*.

[67] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Feb. 2, 2024).

companies) which specifically targeted those Users based on their reproductive health conditions.

H. Defendants Violated HIPAA.

151. Defendants' disclosure of Plaintiffs' and Class Members' Private Information to entities like Facebook also violated HIPAA.

152. Under federal law, a healthcare provider may not disclose PII, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[68]

153. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

154. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

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

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

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

A. Names;
…
H. Medical record numbers;
…
J. Account numbers;
…
M. Device identifiers and serial numbers;
N. Web Universal Resource Locators (URLs);
O. Internet Protocol (IP) address numbers; … and
P. Any other unique identifying number, characteristic, or code… and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."[69]

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

158. Even the fact that an individual is receiving a medical service, i.e., is a patient of a particular entity, can be PHI.

159. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source

[69] *See* 45 C.F.R. § 160.514.

such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[70]

160. Consistent with this restriction, HHS has issued marketing guidance that provides, "With limited exceptions, the [Privacy] 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 or enrollees to third parties without obtaining authorization from each person on the list."[71]

161. Here, as described *supra*, Defendants provided patient information to third parties in violation of the Privacy Rule—and its own Privacy Policy. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."

162. The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information … if the

---

[70] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, (last visited Jan. 30, 2024).

[71] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited Jan. 30, 2024).

information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

163. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually identifiable health information relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both." 42 U.S.C. § 1320(d)(6)(b)(1).

164. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306I, and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights," 45 C.F.R. § 164.312(a)(1)—which Defendants failed to do.

165. Under HIPAA, Defendants may not disclose PII about a patient, potential patient or household member of a patient for marketing purposes without the patient's express written authorization. See HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

166. Defendants further failed to comply with other HIPAA safeguard regulations as follows:

a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants created, received, maintained and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendants in violation of 45 C.F.R. section 164.308(a)(6)(ii);

d) Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e) Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3); and

f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

167. In disclosing the content of Plaintiffs' and Class Members' communications, Defendants had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions, that is, to illegally disclose Plaintiffs' and Class Members' Private Information to Facebook (and other Pixel Information Recipients) in violation of HIPAA, including 42 U.S.C. § 1320d-6(a)(3), as well as the torts alleged below.

168. Defendants intercepted the content of Plaintiffs' and Class Members' communications, including their Private Information, for a criminal and tortious purpose. Defendants would not have been able to obtain the Private Information or the marketing services they did if they had complied with the law.

169. Commenting on a June 2022 report discussing the use of Meta Pixels by hospitals and medical centers, David Holtzman, a health privacy

consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."72

170. Defendants' placing third-party tracking codes on their Web Properties is a violation of Plaintiffs' and Class Members' privacy rights under federal law. While Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates Defendants' wrongdoing relevant to other claims and establishes their duty to maintain patient privacy.

I. Defendants' Use of the Pixel Violates OCR Guidance.

171. The government has issued guidance warning that tracking technologies like the Pixel may come up against federal privacy law when installed on healthcare websites.

172. Healthcare organizations regulated under the HIPAA may use third-party tracking tools, such as Google Analytics or Pixels only in a limited way to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[73]

173. According to the Bulletin, Defendants have violated HIPAA rules by implementing the Pixel and other tracking technologies.[74]

---

[72] ADVISORY BOARD, '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited Jan. 30, 2024).

[73] *See* OCR Bulletin, *supra* note 15.

[74] *See id*. ("disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures").

174. Defendants have shared Plaintiffs' and Class Members' Private Information, including health conditions for which they seek treatments, treatments and/or medications sought, the frequency with whom they take steps to obtain healthcare for certain conditions, and their unique identifiers. This information is, as described in the OCR Bulletin, "highly sensitive."

175. The OCR Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code***.[75]

176. Defendants' sharing of Private Information with Facebook and other Pixel Information Recipients violated Plaintiffs' and Class Members' rights.

J. Defendants Violated Industry Standards.

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

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

179. 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)[.][76]

---

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

[76] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (last visited Jan. 30, 2024).

180. 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 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.[77]

181. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping with ethics guidelines for confidentiality.[78]

182. Defendants' use of the Pixels also violates FTC data security guidelines. The FTC has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

183. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[79] established cyber-security guidelines for businesses. These guidelines state that businesses should protect the personal

---

[77] *Id*.

[78] *Id*.

[79] *See* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 30, 2024).

patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network vulnerabilities, and implement policies to correct any security problems.

184. In fact, the FTC has recently brought enforcement actions against several healthcare companies, including Premom, BetterHelp, GoodRx, and Flow Health for conveying information—or enabling an inference—about their consumers' health to unauthorized third parties without the consumers' consent.

185. Like the health care companies fined by the FTC in recent years, Defendants failed to implement these basic, industry-wide data security practices.

K. Users' Reasonable Expectation of Privacy.

186. Plaintiffs and Class Members were aware of Defendants' duty of confidentiality when they sought medical services from Defendants.

187. Indeed, when Plaintiffs and Class Members provided their PII/PHI to Defendants, they each 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 purpose unrelated to patient care.

188. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

189. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the

same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[80]

190. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class Members.

191. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendants' status as healthcare providers, Defendants' common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendants' express and implied promises of confidentiality.

L. Unique Personal Identifiers are Protected Health Information.

192. While not all health data is covered under HIPAA, the law specifically applies to healthcare providers, health insurance providers, and healthcare data clearinghouses.[81]

---

[80] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Jan. 30, 2024).

[81] *See* Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook* (June 21, 2022), https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other

193. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

194. These HIPAA Identifiers, as relevant here, include names, dates related to an individual, email addresses, device identifiers, web URLs and IP addresses.[82]

195. Defendants improperly disclosed Plaintiffs' and Class Members' HIPAA identifiers, including their emails, phone numbers, dates they sought treatments, computer IP addresses, device identifiers, and web URLs visited to Facebook through their use of the Pixel *in addition to* services selected, patient statuses, medical conditions, treatments, provider information, and appointment information.

196. An IP address is a number that identifies the address of a device connected to the Internet. IP addresses are used to identify and route communications on the Internet. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

---

identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations") (last visited Jan. 30, 2024).

[82] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 30, 2024).

197. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

198. Facebook, Google, and other third-party marketing companies track IP addresses to target individual homes and their occupants with advertising.

199. Under HIPAA, an IP address is considered personally identifiable information, which is defined as including "any unique identifying number, characteristic or code," specifically listing IP addresses among examples. See 45 C.F.R. § 164.514 (2).

200. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

201. Consequently, Defendants' disclosure of Plaintiffs' and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

M. Defendants were Enriched by & Benefitted from the Use of the Pixel & Other Tracking Technologies.

202. Defendants decided to embed the Pixel and other tracking technologies on their Web Properties with the purpose of disclosing Plaintiffs' and Class Members's communications to Facebook and other Pixel Recipients in order to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to Defendants and boost their revenue.

203. After receiving individually identifiable patient health information communicated on Defendants' Web Properties, Facebook analyzes this data, improves its own technology and business (including machine learning), and then forwards this data and analysis of this data, to Defendants.

204. Defendants then use this data and analysis for its own commercial purposes that include understanding how Users utilize their Web Properties.

205. Facebook, as well, uses this data and analysis for its own commercial purposes, including to improve its platform and better understand the individuals that make up the audiences that its clients (advertisers) pay Facebook to target with ads.

206. Defendants also receive an additional commercial benefit from using Facebook's tracking tools, such as the Facebook Pixel, in being able to serve more targeted advertisements to existing and prospective patients on their Meta accounts such as Facebook and Instagram.

207. Facebook advertises its Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting."[83]

208. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a

[83] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited Jan. 30, 2024).

website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[84]

209. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Defendants' Web Properties.

210. For example, when a User searches for doctors or medical conditions or treatment on SDFC's Website, that information is sent to Facebook. Facebook can then use its data on the User to find more users to click on a SDFC ad and ensure that the targeted Users are more likely to convert.[85]

211. Through this process, the Facebook Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[86]

212. Plaintiffs' and Class Members' Private Information has considerable value as highly monetizable data, especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

---

[84] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Jan. 30, 2024).

[85] *See, e.g.*, *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking (last visited Jan. 30, 2024).

[86] *Id.*

213. In exchange for disclosing the Private Information of their account holders and patients, Defendants are compensated by Facebook (and other Pixel Information Recipients) in the form of enhanced advertising services and more cost-efficient marketing on their platforms.

214. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[87]

215. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[88]

216. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[89]

217. Whether a user has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court

---

[87] *See The guide to HIPAA compliance in analytics,* https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Jan. 30, 2024).

[88] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra* note 90.

[89] *The complex world of healthcare retargeting, supra* note 89.

has recognized that the pixels' ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).

218. Upon information and good faith belief, Defendants retargeted patients and potential patients, including Plaintiffs and Class Members.

219. Thus, utilizing the Pixels directly benefits Defendants by, among other things, reducing the cost of advertising and retargeting.

N. Plaintiffs' Private Information is Extremely Valuable.

220. Plaintiffs' and Class Members' Private Information has value, and Defendants' disclosure and interception harmed Plaintiffs and the Class by not compensating them for the value of their Private Information and, in turn, decreasing the value of their Private Information.

221. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

222. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

223. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[90] A 2015 article from TechCrunch accurately

[90] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Jan. 30, 2024).

noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."[91] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

224. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).92 That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

225. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[93]

226. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize

---

[91] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Jan. 30, 2024).

[92] *See What Your Data is Really Worth to Facebook* (July 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ (last visited Jan. 30, 2024).

[93] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[94]

227. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

228. Courts recognize the value of personal information and the harm when it is disclosed without consent.[95]

229. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

230. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

231. The value of health data is well-known and various reports have been conducted to identify its value.

232. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers,

---

[94] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last visited Jan. 30, 2024).

[95] *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[96]

233. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[97]

234. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[98]

235. 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."[99]

---

[96] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Jan. 30, 2024).

[97] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Jan. 30, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[98] *See* https://time.com/4588104/medical-data-industry/ (last visited Jan. 30, 2024).

[99] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Jan. 30, 2024).

236. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

237. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

238. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

239. Defendants shared Plaintiffs' and Class Members' communications and transactions on their Web Properties without permission.

240. The unauthorized access to Plaintiffs' and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Web Properties Users, including Plaintiffs and Class Members.

241. Plaintiffs have a continuing interest in ensuring that her future communications with Defendants are protected and safeguarded from future unauthorized disclosure.

REPRESENTATIVE PLAINTIFF B.W.'S EXPERIENCES

242. 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.

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

244. 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.

245. 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).

246. 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.

247. 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).

248. 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.

249. 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.

250. 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.

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

252. 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.

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

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

255. 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.

256. 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.

REPRESENTATIVE PLAINTIFF JANE DOE'S EXPERIENCES

257. Plaintiff Jane Doe accessed and used the SDFC Website using her personal phone while located in California to seek medical treatment for infertility starting in September 2017.

258. Jane Doe has been a patient of SDFC since September 2017. She set appointments and was treated for fertility issues, including infertility diagnosis and testing.

259. Jane Doe 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.

260. Information that Jane Doe 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.

261. Jane Doe 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.

262. After she provided information to Defendants and looked for egg freezing and other fertility treatments on the SDFC Website, Jane Doe began receiving ads for fertility treatments on her Meta accounts (Facebook and Instagram).

263. The amount of ads targeting Plaintiff Jane Doe was excessive and overwhelming, causing her extreme emotional distress.

264. Furthermore, Jane Doe 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.

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

266. Plaintiff Jane Doe 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.

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

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

269. Defendants willfully facilitated these interceptions without Plaintiff Jane Doe's knowledge, consent, or express written authorization.

270. Within the State of California, Defendants transmitted Plaintiff Jane Doe'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.

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

272. Defendants did not inform Plaintiff Jane Doe that they shared her Private Information with Facebook.

273. Plaintiff Jane Doe 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.

274. Plaintiff Jane Doe has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure. Plaintiff Jane Doe 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.

TOLLING

275. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that their Private Information was intercepted and unlawfully disclosed because Defendants kept this information secret. Plaintiffs only discovered that their Private Information had been disclosed by Defendants, in January 2024.

CLASS ACTION ALLEGATIONS

276. **Class Definition:** Plaintiffs bring this action on behalf of themselves and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

277. The **Nationwide Class** that Plaintiffs seek to represent is defined as:

> All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the third-party tracking technologies on Defendants Web Properties.

278. The California Sub-Class that Plaintiffs seek to represent is defined as:

> All individuals residing in California whose Private Information was disclosed to a third party without authorization or consent through the third-party tracking technologies on Defendants Web Properties.

279. Plaintiffs reserve the right to modify the class definition or add sub-classes as necessary prior to filing a motion for class certification.

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

281. The Nationwide Class, and the California Sub-Class are referred to collectively as the "Classes." Excluded from the Class are Defendants; any affiliate, parent, or subsidiary of Defendants; any entity in which Defendants have a controlling interest; any officer director, or employee of Defendants; any successor or assign of Defendants; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

282. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiffs at

this time. However, it is estimated that there are at least thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendants' records and non-party Facebook's records.

283. Typicality. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs used the Web Properties and had their personally identifiable information and protected health information disclosed to Facebook without her express written authorization or knowledge. Plaintiffs' claims are based on the same legal theories as the claims of other Class Members.

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

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

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 Plaintiffs' and Class Members' Private

Information to unauthorized third parties;

c. Whether Defendants violated their privacy policies by disclosing Plaintiffs' and Class Members' Private Information to Facebook, Meta, or other third parties;

d. Whether Defendants adequately, promptly and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

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

f. Whether Defendants adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information;

h. Whether Defendants violated the consumer protection statutes invoked herein;

i. Whether Defendants knowingly made false representations or omitted material representations as to their data security and/or privacy policy practices;

j. Whether Defendants knowingly omitted material representations with respect to their data security

and/or privacy policy practices;

k. Whether Defendants' acts and practices violated Plaintiffs' and Class Members' privacy rights;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential or nominal damages as a result of Defendants' wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendants' disclosure of their Private Information;

n. Whether Plaintiffs and Class Members are entitled to damages under CIPA, the CMIA, or any other relevant statute; and

o. Whether Defendants' actions violate Plaintiffs' and Class Members' privacy rights as provided by the California Constitution.

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

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

CLAIMS FOR RELIEF

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq.*
(On behalf of Plaintiffs & the Nationwide Class)

287. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

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

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

290. 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.

291. 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).

292. 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).

293. 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).

294. 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).

295. 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).

296. 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 patients' sensitive communications.

297. Plaintiffs and Class Members' interactions with Defendants' Web Properties are electronic communications under the ECPA.

298. 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).

299. 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.

300. 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.

301. 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).

302. 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).

303. 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.

304. 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.[100]

305. Plaintiffs' information that Defendants disclosed to third parties qualifies as IIHI, and Defendants violated Plaintiffs' expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6).

306. 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.

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

308. 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.

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

310. 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

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

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.

311. 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.

312. 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.

313. 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.

314. 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.

315. 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.

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

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

318. 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 II
VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code §§ 630, *et. seq.*
(On behalf of Plaintiffs & the California Class)

319. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

320. The California Invasion of Privacy Act ("CIPA") is codified at California Penal Code §§ 630 to 638.

321. CIPA begins with its statement of purpose.

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

CAL. PENAL CODE § 630.

> California Penal Code § 631(a) provides, in pertinent part: Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500)[.]

322. A defendant must show it had the consent of *all* parties to a communication.

323. At all relevant times, Defendants aided, employed, agreed with, and conspired with Facebook and other third parties to track and intercept Plaintiffs' and Class Members' internet communications while using the Website, specifically by installing and configuring the Pixel to permit Facebook to eavesdrop on and intercept in real-time the content of Plaintiffs' and Class Members' private communications with Defendants.

324. The content of those conversations included Private Information, such as highly sensitive PHI. Through Defendants' installation and configuration of the Pixels on their Web Properties, these communications were intercepted by Facebook during the communications and without the knowledge, authorization, or consent of Plaintiffs and Class Members.

325. Defendants intentionally inserted an electronic device into their Web Properties that, without the knowledge and consent of Plaintiffs and

Class Members, transmitted the substance of their confidential communications with Defendants to a third party.

326. Defendants willingly facilitated Facebook's and other third parties' interception and collection of Plaintiffs' and Class Members' private medical information by embedding the Pixel(s) on the Website, thereby assisting Facebook's eavesdropping.

327. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Pixel falls under the broad catch-all category of "any other manner":

p. The computer codes and programs Facebook and other third parties used to track Plaintiffs' and Class Members' communications while they were navigating the Website;
q. Plaintiffs' and Class Members' browsers;
r. Plaintiffs' and Class Members' computing and mobile devices;
s. Facebook's web and ad servers;
t. The web and ad servers from which Facebook and other third parties tracked and intercepted Plaintiffs' and Class Members' communications while they were using a web browser to access or navigate the Website;
u. The computer codes and programs used by Facebook and other third parties to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a browser to visit the Website; and
v. The plan Facebook and other third parties carried out to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a web browser or mobile application to visit the Website.

328. Defendants fail to disclose that they are using the Pixels to track and automatically and simultaneously transmit highly sensitive personal communications to a third party. Defendants are necessarily aware that these communications are confidential as their Website Privacy Notices acknowledge the confidential nature of PHI and disclaims that it is being

shared with unidentified third parties without Plaintiffs' and Class Members' express authorization.

329. The patient communication information that Defendants transmit while using the Pixel and tracking technologies constitutes protected health information.

330. As demonstrated hereinabove, Defendants violate CIPA by aiding and permitting third parties, including Facebook and its agents, employees, and contractors to receive its patients' online communications in real time through their Web Properties without their consent. Facebook specifically receives the content of these communications and understands it, as the FID is assigned by Facebook and Facebook must understand the content in order to process it and link it to individual Users so that Facebook may target advertising to those persons based on their healthcare choices.

331. By disclosing Plaintiffs' and Class Members' private health information, Defendants violated Plaintiffs' and Class Members statutorily protected right to privacy.

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

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

COUNT III

VIOLATIONS OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code §§ 56, *et seq*.
(On behalf of Plaintiffs & the California Class)

317. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

318. The California Confidentiality of Medical Information Act, California Civil Code §§ 56, *et seq.* ("CMIA") prohibits health care providers from disclosing medical information relating to their patients without patient authorization. "Medical information" refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual[.]" CAL. CIV. CODE § 56.05.

319. Defendants are "provider[s] of health care" as defined by California Civil Code § 56.06(b).

320. Plaintiffs and Class Members are patients, and, as health care providers, Defendants had an ongoing obligation to comply with the CMIA's requirements. As set forth above, device identifiers, web URLs, Internet Protocol (IP) addresses, and other characteristics that can uniquely identify Plaintiffs and Class Members are transmitted from within the State of California to Defendants in combination with patient medical conditions, medical concerns, treatment(s) sought by the patients, and doctors viewed along with the medical specialty of the doctor(s) searched for and viewed by

patients. This is protected health information under the CMIA.

321. This private medical information is intercepted and transmitted within the State of California to third parties including Facebook and its agents, employees, and contactors via Defendants' knowing and intentional decision to embed enabling software into their Web Properties.

322. Facebook ID is also an identifier sufficient to allow identification of an individual. Along with patients' Facebook ID, Defendants disclose to third parties including Facebook and its agents, employees, and contactors several pieces of information regarding patient use of their Web Properties including but not limited to the following: patient medical conditions, medical concerns, treatment(s) sought by the patients, and medical specialty of the doctor(s) searched for by patients.

323. The information described above constitutes medical information pursuant to the CMIA because it is patient information derived from a provider of health care regarding patients' medical treatment and physical condition, and this medical information is linked with individually identifying information. CAL. CIV. CODE § 56.05(i).

324. As demonstrated hereinabove, Defendants fail to obtain their patients' authorization for the disclosure of medical information and fails to disclose in their Website Privacy Notice that it shares protected health information with Facebook or other third parties for marketing purposes.

325. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must be: (1) "Clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization;" (2) signed and dated by the patient or his representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date

after which the authorization expires. Accordingly, the information set forth in Defendants' Website Privacy Notice does not qualify as a valid authorization.

326. As described above, Defendants are violating the CMIA by disclosing its patients' medical information to third parties, including Facebook and its agents, employees, and contractors along with the patients' individually identifying information. Accordingly, Plaintiffs and Class Members seek all relief available for Defendants' CMIA violations.

327. Plaintiffs and Class Members seek nominal damages, compensatory damages, punitive damages, attorney fees, and costs of litigation for Defendants' violation(s) of the CMIA.

COUNT IV
INVASION OF PRIVACY—CALIFORNIA CONSTITUION ART. 1 § 1
(On behalf of Plaintiffs & the California Class)

328. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

329. 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.

330. 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.

331. 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.

332. 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.

333. 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.

334. 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.

335. 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.

336. 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.

337. 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.

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

COUNT V
COMMON LAW INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On behalf of Plaintiffs & the Nationwide Class)

339. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

340. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendants via their Web Properties and the communication platforms and services therein.

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

342. 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.

343. Plaintiffs and Class Members had a reasonable expectation of privacy because Defendants' Website Privacy Notice states that they can expect such privacy. 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 private medical information coupled with individually identifying information is highly offensive to the reasonable person.

344. 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.

345. 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.

346. Plaintiffs and Class Members seek appropriate relief for these 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.

347. 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.

COUNT VI

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiffs & the Nationwide Class)

348. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

349. Defendants solicited and invited Plaintiffs and Class Members to

provide their Private Information through Defendants' Web Properties as part of its regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendant.

350. Defendants required Plaintiffs and Class Members to provide their Private Information, including email addresses, phone numbers, computer IP addresses, appointment information, medical insurance information, medical provider information, medical histories, and other content submitted on Defendants' Web Properties as a condition of their receiving healthcare services.

351. As a condition of utilizing Defendants' Web Properties and receiving services from Defendants, Plaintiffs and Class Members provided their Private Information and compensation for their medical care. In so doing, Plaintiffs and Class Members entered into contracts with Defendants by which Defendants agreed to safeguard and protect such information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

352. Implicit in the agreement between Defendants and their patients was the obligation that both parties would maintain the Private Information confidentially and securely.

353. Defendants had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in their possession was used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Defendants.

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

355. Additionally, Defendants implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

356. Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

357. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendants. 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 and would have instead retained the opportunity to control their Private Information for uses other than medical treatment, billing, and benefits from Defendants.

358. Consumers of medical services value their privacy and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected, nor would Plaintiffs and Class Members have entrusted their Private Information to Defendants in the absence of Defendants' implied promise to monitor their Website, computer systems, and networks to ensure that reasonable data security measures were adopted and maintained.

359. Defendants breached the implied contracts with Plaintiffs and Class Members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties, failing to properly safeguard and protect Plaintiffs' and Class Members' Private Information; and violating

industry standards as well as legal obligations that are necessarily incorporated into implied contract between Plaintiffs, Class Members, and Defendants.

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

361. As a result of Defendants' failure to fulfill the promises in these implied contracts, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of diminished value.

362. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiffs and Class Members have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities, the loss of control of their Private Information, disruption of their medical care and treatment, and the loss of the benefit of the bargain they had struck with Defendants.

363. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

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

364. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

365. Internet users have a property interest in their personal

information and data.

366. 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.

367. 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.

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

369. 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.

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.

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.

372. 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).

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

COUNT VIII

UNJUST ENRICHMENT

(On behalf of Plaintiffs & the Nationwide Class)

374. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and bring this count on behalf of themselves and the proposed Class.

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

376. 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 their own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiffs and Class Members conferred a benefit on Defendants in the form of monetary compensation.

377. 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 this information to third parties.

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

379. 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 and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

380. The benefits that Defendants derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles for Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

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

RELIEF REQUESTED

382. Plaintiffs, on behalf of themselves and the proposed Classes, respectfully requests that the Court grant the following relief:

a. Certification of this action as a class action and appointment of Plaintiffs and Plaintiffs' counsel to represent the Class;

b. A declaratory judgment that Defendants violated: (1) the California Invasion of Privacy

Act; (2) the California Confidentiality of Medical Information Act; and (3) Plaintiffs' and Class Members' privacy rights as provided at common law and pursuant to the California Constitution;

c. An order enjoining Defendants from engaging in the unlawful practices and illegal acts described herein; and

d. An order awarding Plaintiffs and the Class: (1) actual or statutory damages; (2) punitive damages in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorney fees and expenses and costs of suit pursuant to California Code of Civil Procedure § 1021.5 and/or other applicable law; and (6) Such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Classes, demand a trial by jury for all claims asserted herein and so triable.

DATED: February 3, 2024

/s/ Daniel Srourian

Daniel Srourian, California Bar No. 285678
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd. Suite 1710
Los Angeles, CA 90010
daniel@slfla.com

John R. Parker, Jr. (SBN 257761)
ALMEIDA LAW GROUP LLC
jrparker@almeidalawgroup.com
3550 Watt Avenue, Suite 140
Sacramento, California 95608
Tel: (916) 616-2936

David S. Almeida (*pro hac vice forthcoming*)
Matthew J. Langley, California Bar No. 342846
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
t: 312-576-3024
david@almeidalawgroup.com
matt@almeidalawgroup.com

Attorneys for Plaintiff & the Classes

ClassAction.org