IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

N.B. and A.E., individually and on behalf of all others similarly situated, Plaintiffs, v. PLANNED PARENTHOOD FEDERATION OF AMERICA INC. d/b/a PLANNED PARENTHOOD Defendant.	**Case No. 1:25-cv-10279-MKV** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs N.B. and A.E. (collectively, "Plaintiffs") bring this action individually and on behalf of all others similarly situated (the "Class Members"), against Defendant Planned Parenthood Federation of America Inc. ("Planned Parenthood" or "Defendant"). Plaintiffs bring this action based upon personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all Planned Parenthood patients who accessed www.plannedparenthood.org (the "Website") to schedule an appointment for medical and health related services.

2. As a healthcare provider, Defendant provides a variety of services, including access to abortion, birth control, emergency contraception, HIV services, mental health services, pregnancy testing and planning, prenatal and postpartum services, sexual and reproductive health

concerns, STD testing and treatment, gender-affirming care, vaccines, wellness care and preventative care services.[1]

3. When patients disclose health information and schedule medical appointments online, patient privacy is crucial. Patients expect, as they should, that their information will be held in confidence and not shared with third parties without their knowledge or consent. The sensitive nature of information related to medical procedures, such as those offered by Defendant, amplifies the need for privacy during online bookings.

4. Moreover, information concerning an individual's healthcare, including health information and medical appointments, is protected by state and federal law. Despite these protections, and unbeknownst to Plaintiffs and Class Members, Defendant aided, employed, agreed, and conspired with Google, LLC ("Google") to intercept sensitive and confidential communications sent and received by Plaintiffs and Class Members, including sensitive and confidential medical and health information. Plaintiffs bring this action for legal and equitable remedies resulting from these illegal actions.

PARTIES

Plaintiffs

5. Plaintiff N.B. is an adult citizen of the state of California, domiciled in Chico, California.

6. On or around August 2025, Plaintiff N.B. visited the Website to book an appointment at Defendant's Chico, California location for medical services. Plaintiff N.B. attended her scheduled medical appointment and received treatment for the services she selected. Unbeknownst to Plaintiff N.B., Defendant intercepted and/or assisted Google with intercepting

[1] PLANNED PARENTHOOD, *Our Services*, https://www.plannedparenthood.org/get-care/our-services.

her communications, including those that contained personally identifiable information ("PII") and protected health information ("PHI").

7. Plaintiff A.E. is an adult citizen of the state of California, domiciled in Los Angeles, California.

8. Between 2021 and 2024, Plaintiff A.E. visited the Website to book appointments for various medical services (including: contraceptives, STI/STD screenings, and elective termination of a pregnancy) at Defendant's Antelope Valley Center, California location. To schedule these appointments, Defendant required Plaintiff A.E. to disclose additional information, including the date of her last menstrual period. Plaintiff A.E. provided her PHI, attended her scheduled medical appointment, and received treatment for the services she selected. Unbeknownst to Plaintiff A.E., Defendant intercepted and/or assisted Google with intercepting her communications, including those that contained her PII and PHI.

9. At all relevant times, Plaintiffs have maintained active Google accounts. When creating their Google accounts, Plaintiffs were required to provide their PII, including their full legal name, date of birth, phone number, email, and gender. Additionally, every time Plaintiffs access their accounts, Google collects information related to their IP address and electronic device (e.g. browser, operating system, screen resolution, etc.) and stores it in a profile maintained by Google for targeted advertising purposes. Plaintiffs used the same devices to access the Website that they did to access their Google accounts. Plaintiffs were in California when they visited the Website and entered their protected health information to schedule medical appointments.

Defendant

10. Defendant Planned Parenthood is a New York corporation with its principal place of business in New York, New York. Defendant owns and operates the Website which patients use to book appointments at one of Defendant or its affiliate's national network of sexual and reproductive health clinics. Defendant maintains hundreds of clinic locations in multiple states throughout the United States. Defendant owns and operates the Website, whereby consumers seeking to procure medical procedures can schedule both in-person and telehealth appointments various medical services and procedures, including at clinics located within California.

11. Defendant disclosed Plaintiffs' and Class Members' confidential and protected medical information without their knowledge, consent, or express written authorization. As a consequence of these interceptions, Plaintiffs have received advertisements marketing various medical procedures, specifically targeted at Plaintiffs as a result of Defendant's disclosure of their medical booking information to Google. However, Plaintiffs did not know why they were receiving such advertisements until contacting undersigned counsel. Defendant breached its duty of confidentiality by unlawfully disclosing Plaintiffs' PII and PHI third parties, including Google, LLC.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiffs allege that at least 100 people comprise the proposed class, that the combined claims of the

proposed Class Members exceed $5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from at least one defendant.

13. This Court has personal jurisdiction over the parties because Defendant is a New York corporation, with its principal place of business within this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because Defendant has its principal place of business is in this District.

FACTUAL ALLEGATIONS

A. Background of the California Invasion of Privacy Act and the Federal Wiretap Act

15. The California Invasion of Privacy Act ("CIPA"), California Penal Code § 630, *et seq.*, prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

16. To establish liability under California Penal Code § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*

> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> 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.

17. Section 631(a)'s applicability is not limited to phone lines, but also applies to "new technologies" including computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

18. Similarly, Section 632 makes it unlawful for:

> A person [to] ***intentionally and without the consent of all parties*** to a confidential communication, use[] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio . . . .

19. Under California Penal Code § 637.2, Plaintiffs may seek injunctive relief and statutory damages of $5,000 per violation.

20. In a manner similar to CIPA, the Federal Wiretap Act (i.e. the ECPA) creates "a comprehensive scheme for the regulation of wiretapping and electronic surveillance."[2]

21. Although the ECPA usually applies "where one part[y] to the communication has given consent[,]" the ECPA eliminates the one-party consent exception when the conduct was

[2] *People v. Roberts*, 184 Cal. App. 4th 1149, 1167 (2010).

for the "the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[3]

B. Warning on Tracking Codes on Health Care Websites

22. The federal government has issued guidance warning that tracking codes like Google tracking technologies violate federal privacy law when installed on healthcare websites such as Defendant's. The statement titled, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" (the "Bulletin"), was issued by the Department of Health and Human Services' Office for Civil Rights ("OCR") in December 2022.[4]

23. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act (HIPAA) may only use third-party tracking tools, such as Google's tracking technologies, in a very 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. The Bulletin explains:

> 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***.[5]

24. The bulletin discusses the types of harm that disclosure may cause to the patient:

> 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***

[3] 18 U.S.C. § 2511(d)

[4] HHS.gov, 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.

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

> ***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.***[6]

25. Plaintiffs and Class Members face the risks about which the government expresses concern. Defendant disclosed the fact that Plaintiffs and Class Members booked medical appointments on Defendant's Website, which in turn also discloses the health conditions for which they sought a health care provider; the frequency with which they take steps relating to medical health; and where they seek medical treatment. This information is, as described by the OCR in its bulletin, "highly sensitive."

26. The Bulletin goes on to make clear how broad the government's view of protected information is. 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***.[7]

27. Crucially, that paragraph in the government's Bulletin continues:

> All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or

[6] *Id.* (Emphasis added).

[7] *Id*. (Emphasis added).

> benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[8]

28. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.
>
> "When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."
>
> "Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."
>
> The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about 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. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.
>
> In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency

[8] *Id*. (Emphasis added).

> of visits to health care professionals, and where an individual seeks medical treatment.
>
> . . . Through its recent enforcement actions against BetterHelp, GoodRx and Premom, as well as recent guidance from the FTC's Office of Technology, the FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC's Health Breach Notification Rule . . . .[9]

29. The FTC is unequivocal in its stance. The FTC has specifically informed healthcare companies, like Defendant, that they should not use tracking technologies to collect sensitive health information and disclose it to third party advertising platforms without informed consent:

> The FTC Act prohibits companies and individuals from engaging in unfair or deceptive acts or practices in or affecting commerce. This means you must ensure your health data practices aren't substantially injuring consumers, including by invading their privacy.
>
> For instance, *BetterHelp*, *GoodRx*, and *Premom* make clear that disclosing consumers' health information for advertising without their affirmative express consent may be an unfair practice.
>
> [I]f you use behind-the-scenes tracking technologies that share consumers' sensitive health data in contradiction of your privacy promises, that's a violation of the FTC Act.[10]

30. Thus, Defendant's conduct as alleged herein, is directly contrary to clear pronouncements by the FTC and HHS.

---

[9] FEDERAL TRADE COMMISSION, FTC AND HHS WARN HOSPITAL SYSTEMS AND TELEHEALTH PROVIDERS ABOUT PRIVACY AND SECURITY RISKS FROM ONLINE TRACKING TECHNOLOGIES, July 20, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

[10] https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach.

31. In light of, and in addition to, the federal government's own issued guidance above, news sources also warn that tracking code—such as Google's tracking technologies—pose risks of violating federal privacy law and HIPAA:

> Federal regulators are warning [regulated entities] hospital systems and telehealth providers about the data privacy risks of using third-party tracking technologies. These services, like…Google Analytics, could violate the Health Insurance Portability and Accountability Act (HIPAA) or Federal Trade Commission (FTC) data security rules, officials said.
>
> The FTC and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued a rare joint release announcing that 130 [regulated entities] hospital systems and telehealth providers received a letter warning them about the data privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps … "The compliance buck still stops with you. Furthermore, your company is legally responsible even if you don't use the data obtained through tracking technologies for marketing purposes."[11]

32. Fierce Healthcare also spoke up in an April 3, 2023 article:

> Nearly all nonfederal acute care hospitals' [regulated entities'] websites track and transfer data to a third party, potentially fueling the unwanted disclosures of patients' sensitive health information and opening up that [regulated entity] hospital to legal liability, according to a recently published University of Pennsylvania analysis.[12] The census of more than 3,700 hospital [regulated entity] homepages found at least one third-party data transfer among 98.6% of the websites as well as at least one third-party cookie on 94.3%, researchers wrote in Health Affairs.
>
> The hospitals' [regulated entities'] homepages had a median of 16 third-party transfers, more of which were found among medium-sized (100 to 499 beds) hospitals, nonprofit hospitals, urban hospitals, health system-affiliated hospitals and those that weren't serving the largest portion of patients in poverty, they wrote . . . Many of these complaints cite Facebook parent company Meta's Pixel tracker, which a June 2022 investigation from The Markup[13] detected on about a third of

[11] Heather Landi, *Regulators warn hospitals and telehealth companies about privacy risks of Meta, Google tracking tech*, FIERCE HEALTHCARE, July 21, 2023, https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google.

[12] https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2022.01205.

[13] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

> large hospitals' websites. That report found evidence that, in some instances, the sensitive data transferred to third parties met the criteria for a HIPAA violation.[14]

33. Health Affairs also published an article in April 2023, stating in relevant part:

> By including third-party tracking code on their websites, hospitals [regulated entities] are facilitating the profiling of their patients by third parties. These practices can lead to dignitary harms, which occur when third parties gain access to sensitive health information that a person would not wish to share. These practices may also lead to increased health-related advertising that targets patients, as well as to legal liability for hospitals [regulated entities].[15]

34. This is further evidence that the data that Defendant chose to share is protected PHI and PII. The sharing of that information was a violation of Plaintiffs' and Class Members' privacy rights.

C. Defendant's Conduct Violates HIPAA

35. Under HIPAA, a healthcare provider may not disclose personally identifiable information ("PII") or protected health information ("PHI") without the patient's express written authorization.[16]

36. The United States Department of Health and Human Services ("HHS") has established a national standard, known as the HIPAA Privacy Rule ("Privacy Rule"), to explain the duties healthcare providers owe to their patients. "The Rule requires appropriate safeguards

---

[14] Dave Muoio, *Almost every hospital's homepage is sending visitors' data to third parties, study finds*, FIERCE HEALTHCARE, Apr. 3, 2023, https://www.fiercehealthcare.com/providers/almost-every-hospital-homepage-sending-visitors-data-third-parties-study-finds.

[15] Ari B. Friedman, et al., *Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals*, HEALTH AFFAIRS, Vol. 42, No. 24, April 2023, https://www.healthaffairs.org/doi/10.1377/hlthaff.2022.01205.

[16] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

to protect the privacy of [PHI] and sets limits and conditions on the uses and disclosure that may be made of such information without an individual's authorization."[17]

37. In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), making business associates of HIPAA covered entities directly liable for compliance with certain requirements of the Privacy Rule.[18] Those requirements include the impermissible uses and disclosures of PHI.[19]

38. A healthcare provider or business associate violates the Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-d9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[20]

39. The statute states that an entity "shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization." *Id.*

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

---

[17] U.S. DEPT. OF HEALTH & HUM. SERVS., THE HIPAA PRIVACY RULE, https:/www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[18] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat 115; *see also* 42 U.S.C. § 17931(b) (applying civil and criminal penalties to business associates for violations of 42 U.S.C. § 1320d-6).

[19] U.S. DEPT. OF HEALTH & HUM. SERVS., DIRECT LIABILITY OF BUSINESS ASSOCIATES, https://hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html.

[20] 42 U.S.C. § 1320d-6.

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

41. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to their patients.

42. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant 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 Defendant 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 306(a)(2); and

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

43. Moreover, HIPAA requires a heightened "authorization" requirement to disclose protected health information and personally identifiable information. While consent may allow certain uses or disclosures of PHI for treatment, payment, or healthcare operations, it is not sufficient for uses or disclosures that require an authorization under 45 C.F.R. § 164.508, which encompasses most uses, including marketing. *Compare* 45 C.F.R. § 164.506 (consent); *with* 45 C.F.R. § 164.508 (authorizations).

44. The HIPAA de-identification rule reaffirms the positions of the HHS and the FTC. The pertinent provisions of 45 C.F.R. § 164.514 state information is not individually identifiable only if:

> (b) Implementation specifications: Requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:
>
> . . .
>
> (2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
>
> (A) Names;
>
> (B) All geographic subdivisions smaller than a State . . . .;
>
> (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
>
> (D) Telephone numbers;
>
> (E) Fax numbers;
>
> (F) Electronic mail addresses;
>
> (G) Social security numbers;
>
> (H) Medical record numbers;
>
> (I) Health plan beneficiary numbers;
>
> (J) Account numbers;
>
> (K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

45. The HHS has further instructed that patient status alone is protected:

- "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);
- "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which would include disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);
- It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and
- The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

46. Therefore, Defendant's conduct, as described herein, is directly contrary to federal privacy laws.

D. Google's Tracking Technologies

47. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each device (such

as a computer, tablet, laptop, or smartphone) accesses web content through a web browser (e.g. Chrome, Safari, Edge, etc.).

48. Every website is hosted by a computer server that holds the website's contents and through which the entity in charge of the website exchanges communications with the consumer's device via web browsers.

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

(a) HTTP Request: an electronic communication sent from a 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.

(b) Cookies: a small text file that can be used to store information on the device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from 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.

(c) HTTP Response: an electronic communication that is sent as a reply to the device's web browser from the host server in response to a HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

50. A consumers' HTTP Request essentially asks the Website to retrieve certain information (such as appointment booking information), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the consumer's screen as they navigate the Website).

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

52. 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. The tracking technologies embedded on the Website by Defendant constitute Source Code and function is a substantially similar way.

53. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over $1 trillion dollars. Google fancies itself a "tech" company, but at its core, Google is an advertising company.

54. Google "make[s] money" from "advertising products [that] deliver relevant ads at just the right time," generating "revenues primarily by delivering both performance advertising and brand advertising."[21] In 2020, Google generated $146.9 billion in advertising revenue, which amounted to more than 80 percent of Google's total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

Table 1:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$257.6 billion	$209.5	81.33%
2020	$182.5 billion	$146.9 billion	80.49%
2019	$161.9 billion	$134.8 billion	83.29%
2018	$136.8 billion	$116.5 billion	85.12%

55. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google's SDK and pixel integrate with Google's advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google's ad network and products increasing Google's overall ad revenue. Products like Google's SDK and its tracking pixel also improve

[21] ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm.

the company's advertising network and capabilities by providing more wholesome profiles and data points on individuals.

56. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

57. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth information about user behavior. Also, Universal Analytics enabled tracking the same user across multiple devices through its addition of the User-ID feature, which "associate[s] a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices."

58. In 2020, Google launched Google Analytics 4, a platform combining Google Analytics with Firebase to analyze both app and web activity.

59. Since launching Google Analytics, Google has become one of the most popular web analytics platforms on the internet. Indeed, Google had a $62.6 billion increase in advertising revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

60. Google touts Google Analytics as a marketing platform that offers "a complete understanding of your customers across devices and platforms."[22] It allows companies and advertisers that utilize it to "understand how your customers interact across your sites and apps, throughout their entire lifestyle," "uncover new insights and anticipate future customer actions with Google's machine learning to get more value out of your data," "take action to optimize marketing performance with integrations across Google's advertising and publisher tools," and "quickly analyze your data and collaborate with an easy-to-use interface and shareable reports."[23]

61. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site. This code immediately intercepts a user's interaction with the webpage every time the user visits it, including what pages they visit and what they click on. The code also collects PII, such as IP addresses and device information related to the specific computing device a consumer (or patient) is using to access a website. The device information intercepted by Google includes the patient's operating system, operating system version, browser, language, and screen resolution.

62. In other words, when interacting with the Website, an HTTP Request is sent to Planned Parenthood's server, and that server sends an HTTP Response including the Markup that displays the website visible to the patient and Source Code, including Google's tracking technologies.

63. Thus, Defendant is essentially handing patients a tapped device, and once the webpage is loaded onto the patient's browser, the software-based wiretap is quietly waiting for

[22] *Analytics*, GOOGLE, https://marketingplatform.google.com/about/analytics/ (last visited Jan. 10, 2023).

[23] *Id.*

private communications on the Website to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third parties like Google.

64. Once Google's software code collects the data intercepted from the Website, it packages the information and sends it to Google Analytics for processing. Google Analytics enables the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google Analytics database and cannot be changed.

65. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on acquisition (e.g., information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (e.g., classify your users by age, location, language, and gender, along with interests they express through their online browsing and purchase activities).

66. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

67. The Website utilizes Google's pixel and SDK. As a result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least "Custom Events" and URLs that disclosed the medical treatment being received by the patient.

Google also received additional PII, including the patients' IP address, device information, and User-IDs.

68. For example, the Website utilizes Google's "cid" or "Client ID" function to identify users as they navigate the Planned Parenthood Website.[24]

69. The Website also utilizes Google Ad's "auid" or "Advertiser User ID" function to identify users as they navigate the Planned Parenthood Website.[25]

70. In addition to user-IDs, upon receiving information from the Website, Google also utilizes a "browser-fingerprint" to personally identify consumers. A browser-fingerprint is information collected about a computing device that is used to identify the specific device.

71. These browser-fingerprints are used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data.

72. As Google explained, "[w]ith fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[26]

73. The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it

[24] https://www.owox.com/blog/use-cases/google-analytics-client-id#:~:text=The%20Client%20ID%20(cid)%20or,unique%20users%20using%20this%20parameter.

[25]

[26] https://www.blog.google/products/chrome/building-a-more-private-web/

employs much more subtle techniques.[27] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.

74. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[28]

75. Browser-fingerprints are personal identifiers. Tracking technologies, like the ones developed by Google and utilized on the Website, can collect browser-fingerprints from website visitors.

76. As enabled by Defendant, Google collects vast quantities of consumer data through its tracking technology.

77. Due to the vast network of consumer information held by Google, it is able to match the IP addresses, device information, and user-IDs it intercepts and link such information to an individual's specific identity.

78. Google then utilizes such information for its own purposes, such as targeted advertising.

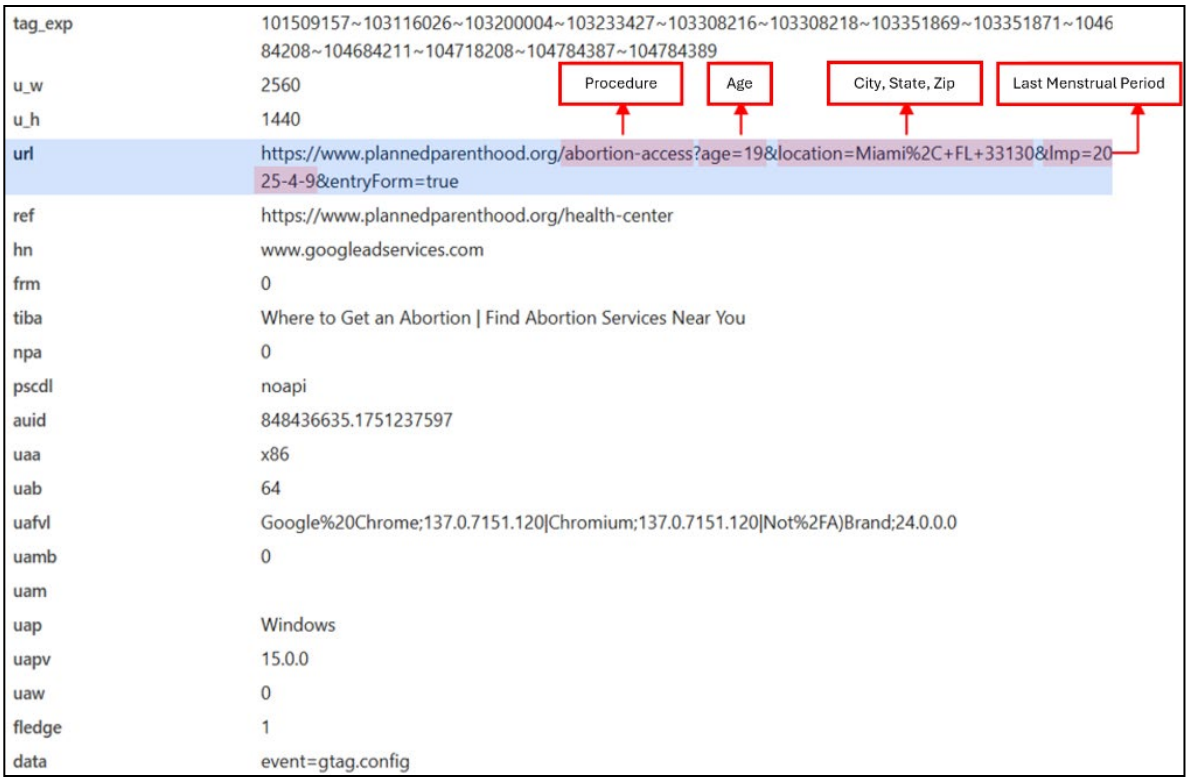
E. Defendant Disclosed Plaintiffs' and Class Members' Protected Health Information

79. Defendant's patients—including Plaintiffs—access the Website to book appointments for various medical procedures.

[27] https://www.pixelprivacy.com/resources/browser-fingerprinting/

[28] https://ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

80. An example illustrates the point. Take, for example, a patient who navigates to the Website to book an abortion. During the appointment booking process, Defendant discloses its patients' PII and PHI to Google, as shown below:



tag_exp	101509157~103116026~103200004~103233427~103308216~103308218~103351869~103351871~104684208~104684211~104718208~104784387~104784389
u_w	2560
u_h	1440
url	https://www.plannedparenthood.org/abortion-access?age=19&location=Miami%2C+FL+33130&lmp=2025-4-9&entryForm=true
ref	https://www.plannedparenthood.org/health-center
hn	www.googleadservices.com
frm	0
tiba	Where to Get an Abortion | Find Abortion Services Near You
npa	0
pscdl	noapi
auid	848436635.1751237597
uaa	x86
uab	64
uafvl	Google%20Chrome;137.0.7151.120|Chromium;137.0.7151.120|Not%2FA)Brand;24.0.0.0
uamb	0
uam	
uap	Windows
uapv	15.0.0
uaw	0
fledge	1
data	event=gtag.config

Figure 1

81. When patients book their appointments on Defendant's Website, Defendant intercepts information related to their patients' appointments through Google's tracking technologies, including the their age, the procedure, their location, and sensitive details such as their last missed period.

82. Defendant further discloses to Google the PII of its patients' sufficient for Google to uncover their identities. In the HTTP communications shown above, the patients' IP address is inherently included in every network request. In addition to its patients' IP address, Defendant, through Google's tracking technologies, disclosed information about each patient's

specific devices and user-IDs, allowing Google to link such information to an individual's specific identity.

83. As shown and described above, Plaintiffs' communications with Defendant were disclosed by Defendant to Google and/or intercepted in transit, in real time, via detailed URLs, which contain the medically sensitive information entered into the Website.

84. Such interceptions included the use of Google's "DSID cookie," which is "used to identify a signed-in user on non-Google sites."[29]

85. Defendant also uses and causes the disclosure of data sufficient for Google to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning individual medical appointments.

86. Defendant sent out these identifiers (e.g. auid, IP address, and device information) with each patient's "event" data.

87. Plaintiffs never consented, agreed, authorized, or otherwise permitted Google to intercept their confidential health information.

88. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to share their confidential health information. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violate federal and state law.

89. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications. Defendant deprived Plaintiffs of their privacy rights when it implemented a system that surreptitiously tracked and recorded Plaintiffs' and other online consumers' confidential communications, personally identifiable information, and protected health information.

[29] https://policies.google.com/technologies/cookies?hl=en-US

F. Defendant Did Not Anonymize Consumer Data By Disclosing "Hashed" Values

90. The Federal Trade Commission routinely evaluates privacy representations by companies. When it comes to hashing the FTC has said the following:

> Companies often claim and act as if data that lacks clearly identifying information is anonymous, but data is only anonymous when it can never be associated back to a person. If data can be used to uniquely identify or target a user, it can still cause that person harm.
> One way that companies obscure personal data is through "hashing." Hashing involves taking a piece of data—like an email address, a phone number, or a user ID—and using math to turn it into a number (called a hash) in a consistent way: the same input data will always create the same hash.
> . . .
> This logic is as old as it is flawed – hashes aren't "anonymous" and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized. FTC staff will remain vigilant to ensure companies are following the law and take action when the privacy claims they make are deceptive.

91. Thus, Defendant intercepted and disclosed Plaintiffs and Class Members personally identifiable information regardless of whether it was hashed or plain text.

G. Tolling

92. Any applicable statutes of limitations have been tolled by Defendant's knowing and active concealment of its incorporation of the Google's tracking technologies onto the Planned Parenthood Website.

93. Google's tracking technologies are entirely invisible to a website visitor.

94. Through no fault or lack of diligence, Plaintiffs and members of the putative classes were deceived and could not reasonably discover Defendant's deceptive and unlawful conduct.

95. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

96. Defendant had exclusive knowledge that the Planned Parenthood Website incorporated Google's tracking technologies and yet failed to disclose to its patients, including Plaintiffs, that by booking appointments through the Website, their PII and PHI would be disclosed to Google.

97. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its users PII and PHI. In fact, to the present, Defendant has not conceded, acknowledged, or otherwise indicated to its users that it has disclosed or released their PII and PHI to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

98. Moreover, all applicable statutes of limitations have also been tolled pursuant to the discovery rule.

99. The earliest that Plaintiffs, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of the initial complaint in this matter.

CLASS ACTION ALLEGATIONS

100. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of a class defined as all natural persons in the United States who, during the class period, navigated the Website to book an appointment (the "Class" or the "Nationwide Class").

101. Plaintiffs also bring this action on behalf of a subclass defined as all natural persons in California who, during the class period, navigated the Website to book an appointment (the "California Subclass").

102. Subject to additional information obtained through further investigation and discovery, the above-described Classes may be modified or narrowed as appropriate, including through the use of subclasses.

103. The "Class Period" is the time 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.

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

105. **Numerosity**. Members of the Classes are so numerous that joinder of all members is impracticable. 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 Classes. The identity of such membership is readily ascertainable from Defendant's records.

106. **Typicality**. Plaintiffs' claims are typical of the claims of the Classes because Plaintiffs used the Website to schedule a medical appointment and had their personally identifiable information and protected health information disclosed to Google without their express written authorization or knowledge. Plaintiffs' claims are based on the same legal theories as the claims of other Class Members.

107. **Adequacy**. Plaintiffs are 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 members of the Classes. 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 members of the Classes.

108. **Commonality**. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members of the Classes because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

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

(b) Whether the Website surreptitiously recorded personally identifiable information, protected health information, and related communications and subsequently, or simultaneously, disclosed that information to Google;

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

(d) Whether Defendant's disclosures of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;

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

(f) Whether Defendant violated Plaintiffs' and Class Members' privacy rights by using Google's tracking technologies to record and communicate patients' confidential medical communications;

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

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

109. **Superiority**. Class action treatment is the superior method for the fair and efficient adjudication of this controversy. Such treatment permits 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 or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweigh any potential difficulties in the management of this class action. Plaintiffs know of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

COUNT I
Violation of the Electronic Communications Privacy Act,
18 U.S.C. § 2511(1), *et seq.*
(On Behalf of the Nationwide Class)

110. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Nationwide Class.

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

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

113. 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.

114. The transmission of Plaintiffs' private and confidential information to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

115. The transmission of the private and confidential information between Plaintiffs and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

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

117. 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." 18 U.S.C. § 2510(4).

118. 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).

119. The following instruments constitute "devices" within the meaning of the ECPA:

(a) The computer codes and programs Google used to track Plaintiffs and

Class Members communications while they were navigating the Website;

(b) Plaintiffs' and Class Members' browsers;

(c) Plaintiffs' and Class Members' mobile devices;

(d) Defendant's and Google's web and ad servers;

(e) The plan Defendant and Google carried out to effectuate the tracking and interception of Plaintiffs' and Class Members' communications while they were using a web browser to navigate the Website.

120. Plaintiffs' and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

121. By utilizing and embedding Google's tracking technologies on its Website, Defendant 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).

122. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications through Google's tracking technologies, which tracked, stored and unlawfully disclosed Plaintiffs' and Class Members' private and confidential information to third parties, including Google.

123. Defendant also procured Google to intercept Plaintiffs' and Class Members' electronic communications through Google's tracking technologies, which tracked, stored and unlawfully disclosed Plaintiffs' and Class Members' private and confidential information to third parties, including Google.

124. Defendant intercepted or assisted in the interception of communications that include, but are not necessarily limited to, communications to/from Plaintiffs and Class Members

regarding private and confidential information, including their treatment information. This confidential information was then monetized for targeted advertising purposes.

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

126. 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), Defendant violated 18 U.S.C. § 2511(1)(d).

127. Defendant intentionally intercepted or intentionally assisted in the interception of 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 any state, namely, HIPAA and invasion of privacy, among others.

128. The party exception in 18 U.S.C. § 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, Defendant violated provisions of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3), 45 CFR 164.501, 164.508(a)(3), as well as the FTC Act. 42 U.S.C. § 1320d-6(a)(3) 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.[30]

129. Plaintiffs' information that Defendant disclosed to Google qualifies as IIHI, and Defendant violated Plaintiffs' and Class Members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the wire or electronic communications to increase their profit margins. Defendant specifically used Google's tracking technologies to track and utilize Plaintiffs' and Class Members' private and confidential information for financial gain.

130. Defendant was not acting under the color of law to intercept Plaintiffs' and Class Members' wire or electronic communications.

131. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy through Google's tracking technologies. Plaintiffs and Class Members had a reasonable expectation that Defendant would not intercept or assist in the interception of their private and confidential information without their knowledge or consent.

132. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq.*

133. As a result of each and every violation thereof, Plaintiffs seek statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, *et seq.* under 18 U.S.C. § 2520.

[30] 42 U.S.C. § 1320d-6.

COUNT II
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 631
(On Behalf of the California Subclass)

134. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the California Subclass.

135. The California Invasion of Privacy Act ("CIPA") is codified at California Penal Code sections 630 to 638. CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . ." Cal. Penal Code § 630.

136. A person violates California Penal Code § 631(a), if:

> by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] 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 [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

137. Further, a person violates Section 631(a) if s/he "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" in the preceding paragraph. *Id.*

138. To avoid liability under Section 631(a), a defendant must show it had the consent of **all** parties to a communication.

139. At all relevant times, Defendant aided, agreed with, and conspired Google to track and intercept Plaintiffs' and Class Members' internet communications while accessing the Website. These communications were intercepted without the authorization and consent of Plaintiffs and Class Members.

140. Defendant, when aiding and assisting Google's wiretapping and eavesdropping, intended to help Google learn some meaning of the content in the URLs and the content the visitor requested.

141. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Google's tracking technologies fall under the broad catch-all category of "any other manner":

a. The computer codes and programs Google used to track Plaintiffs' and Class Members' communications while they were navigating the Website;

b. Plaintiffs' and Class Members' browsers;

c. Plaintiffs' and Class Members' computing and mobile devices;

d. Google's web and ad servers;

e. The web and ad-servers from which Google tracked and intercepted Plaintiffs' and Class Members' communications while they were using a web browser to access or navigate the Website;

f. The computer codes and programs used by Google to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a browser to visit the Website; and

g. The plan Google carried out to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a web browser or mobile device to visit the Website.

142. The information that Defendant transmitted using Google's tracking technologies, including the type of procedure a patient is interested in constituted sensitive and confidential personally identifiable information.

143. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting Google to receive its patients' sensitive and confidential online communications through the Website without their consent.

144. As a result of the above violations, Defendant is liable to Plaintiffs and other members of the California Subclass in the amount of, the greater of, $5,000 dollars per violation or three times the amount of actual damages. Additionally, California Penal Code section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

145. Under the statute, Defendant is also liable for reasonable attorney's fees, other 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 Defendant in the future.

COUNT III
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632
(On Behalf of the California Subclass)

146. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

147. Plaintiffs bring this claim against Defendant individually and on behalf of the California Subclass.

148. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication.

149. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

150. The data collected on Defendant's Website constitutes "confidential communications," as that term is used in Section 632, because Class Members had an objectively reasonable expectation of private with respect to their personally identifiable information and protected health information.

151. Plaintiffs and Class Members expected their communications to Defendant to be confined to Defendant in part, because of Defendant's consistent representations that these communications would remain confidential. Plaintiffs and Class Members did not expect third parties, specifically Google, to secretly eavesdrop upon or record this information and their communications.

152. The tracking technologies from Google, are all electronic amplifying or recording devices for purposes of § 632.

153. By contemporaneously intercepting and recording Plaintiffs' and Class Members' confidential communications to Defendant through this technology, Google eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

154. At no time did Plaintiffs or Class Members consent to Defendant's or Google's conduct, nor could they reasonably expect that their communications to Defendant would be overheard or recorded by Third Parties.

155. Google utilized Plaintiffs' and Class Members' personally identifiable information for its own purposes, including advertising and analytics.

156. Defendant is liable for aiding and abetting violations of Section 632 by Google.

157. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and Members of the California Subclass have been injured by the violations of Cal. Penal Code § 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT IV
Invasion of Privacy Under California's Constitution
(On Behalf of the California Subclass)

158. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed California Subclass.

159. Plaintiffs and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential online 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.

160. At all relevant times, by using Google's tracking technologies to record and communicate patients' sensitive and confidential online medical communications, Defendant intentionally invaded Plaintiffs' and Class Members' privacy rights under the California Constitution.

161. Plaintiffs and Class Members had a reasonable expectation that their sensitive and confidential online communications, identities, health information, and other data would remain confidential, and that Defendant would not install wiretaps on the Website.

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

163. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private medical communications. Moreover, it constituted an egregious breach of societal norms underlying the right of privacy.

164. Accordingly, Plaintiffs and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For a determination that this action is a proper class action;

(b) For an order certifying the Classes, naming Plaintiffs as representatives of the Classes, and naming Plaintiffs' attorneys as Class Counsel to represent the Classes;

(c) For an order declaring that Defendant's conduct violates the statutes referenced herein;

(d) For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

(e) An award of statutory damages to the extent available;

(f) For punitive damages, as warranted, in an amount to be determined at trial;

(g) For prejudgment interest on all amounts awarded;

(h) For injunctive relief as pleaded or as the Court may deem proper; and

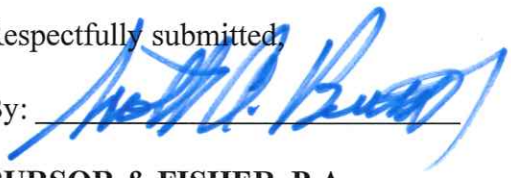
(i) For an order awarding Plaintiffs and the Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Plaintiffs, individually and on behalf of the proposed Classes, demand a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: December 11, 2025

Respectfully submitted,

By: 

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 2806487)
Sarah N. Westcot (*pro hac vice* forthcoming)
Stephen A. Beck (*pro hac vice* forthcoming)
701 Brickell Ave., Suite 2100
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 676-9006
E-Mail: scott@bursor.com
swestcot@bursor.com
sbeck@bursor.com

Counsel for Plaintiffs