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

Attorney for Plaintiff and the Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SAN DIEGO

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

Plaintiff,

v.

DAVITA, INC.

Defendant.

Case No. 37-2023-00025611-CU-PO-CTL

CLASS ACTION COMPLAINT FOR:

1. **VIOLATIONS OF CAL. PENAL CODE § 630, *et seq.*;**
2. **VIOLATIONS OF CAL. CIV. CODE § 56, *et seq.*;**
3. **VIOLATIONS OF CAL. BUS. & PROF. CODE § 17200, *et seq.*;**
4. **VIOLATIONS OF CAL. CONST. ART. 1 § 1;**
5. **INTRUSION UPON SECLUSION;**
6. **PUBLICATION OF PRIVATE FACTS; AND**
7. **BREACH OF CONFIDENCE.**

JURY TRIAL DEMANDED

1. Plaintiff Jane Doe ("Plaintiff") bring this class action complaint on behalf of herself, and all others similarly situated (the "Class Members") against DaVita Inc., (DaVita) which operates 412 facilities in California and offers kidney dialysis services for patients suffering from chronic kidney failure. The allegations contained in this class action complaint are based on Plaintiff's personal knowledge of facts pertaining to herself and upon information and belief, including further investigation conducted by Plaintiff's counsel.

NATURE OF THE ACTION

2. Plaintiff brings this class action lawsuit on behalf of all similarly situated persons to address Defendant's failure to protect information specially entrusted to them—sensitive personal and immensely private information no reasonable person would wish to see exposed.

3. To make matters worse, Defendant's exposure of Plaintiff's and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook"), was not accidental. This was not the work of a third-party hacker. Rather, Defendant actively chose to share patients' communications, and the Private Information within those communications, when it installed and implemented online tracking technologies.

4. Information about a person's physical and mental health conditions and concerns is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

5. Recognizing these facts, and to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

6. Defendant owns and controls https://www.davita.com/ ("Defendant's Website" or the "Website"), which provides kidney care information, kidney health education, diet and nutrition recommendations, care support such as insurance and financial management and emergency services, information for various treatment options, scheduling and location tools to aid patients in finding a facility in their area that offers the particular treatment they require, and much more.

7. Plaintiff and other Class Members who used Defendant's Website thought that they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiff and Class Members, however, Defendant's Website contains the Facebook Tracking Pixel (the "Pixel" or "Facebook Pixel"), which surreptitiously and simultaneously transmits Website visitors' communications and online activity to Facebook, including which buttons they click, the text they have entered or typed into search boxes and text fields, and intimate details about their medical conditions, symptoms, medical treatment, and healthcare providers.

8. Operating as designed and as implemented by Defendant, the Pixel allows the Private Information that Plaintiff and Class Members submit to Defendant to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID") and IP address.[1]

9. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[2] 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), among other things.

10. The user's web browser executes the Pixel based on the instructions it receives from the website's owner, thereby causing the web browser to communicate certain information based on the website owner's chosen parameters. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel, which events are tracked and transmitted to Facebook, and whether the events are categorized as standard events or custom events. By installing the Facebook Pixel on its Website, Defendant effectively planted a bug on Plaintiff and Class Members' web browsers, which disclosed their communications to Facebook in real time as they are transmitted to Defendant.

11. Alarmed at the use of pixels and similar technology by healthcare entities, the Office for Civil Rights (OCR) at HHS issued a Bulletin in December of 2022 to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking

---

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

[2] *Retargeting*, FACEBOOK, https://www.facebook.com/business/goals/retargeting (last visited April 25, 2023).

technologies").[3] The Bulletin expressly provides (in bold type) that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**" In other words, and as described in more detail therein, HHS has expressly stated that entities who use the Facebook Pixel, such as Defendant, have violated HIPAA Rules.

12. In addition to the Facebook Pixel, Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its website servers.[4]

13. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook via the user's web browser, CAPI does not transmit any information via the web browser. Instead, CAPI tracks the user's website interactions and communications, records and stores that information on the website owner's servers, and then transmits the data to Facebook directly from the website owner's servers.[5, 6] Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[7]

---

[3] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited April 5, 2023).

[4] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited April 25, 2023).

[5] https://revealbot.com/blog/facebook-conversions-api/ (last visited April 25, 2023).

[6] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as ottheir connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited April 25, 2023).

[7] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited April 25, 2023).

14. Because CAPI is located on the website owner's servers and is not the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

15. Defendant utilized the Pixel and CAPI data for marketing purposes to bolster its profits. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

16. The information that Defendant's Tracking Pixel and CAPI sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including for example, the type of medical treatment sought, the individual's particular health condition or concern, and the fact that the individual attempted to or did book a medical appointment.

17. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as kidney failure.

18. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients' consent. Neither Plaintiff nor any other Class

Member signed a written authorization permitting Defendant to send their Private Information to Facebook.

19. In response to the use of Pixel tracking by HIPAA-covered entities, the recently issued HHS Bulletin warns that:

> 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. [8]

20. And as recently noted by the Hon. William J. Orrick in a decision concerning the use of the Facebook Pixel by healthcare organizations,

> "[o]ur nation recognizes the importance of privacy in general and health information in particular: the safekeeping of this sensitive information is enshrined under state and federal law. The allegations against Meta are troubling: Plaintiff raise potentially strong claims on the merits and their alleged injury would be irreparable if proven."[9]

21. Consequently, Plaintiff brings this action for legal and equitable remedies to address and rectify the illegal conduct and actions described therein.

---

[8] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERV., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited April 5, 2023).

[9] *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *1 (N.D. Cal. Dec. 22, 2022).

22. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Defendant never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website, or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

23. Defendant breached statutory and common law obligations to Plaintiff and Class Members by, inter alia,: (i) failing to adequately review its marketing programs and web-based technology to ensure the hospital Website was 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 written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

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

25. Plaintiff seeks to remedy these harms and brings causes of action for (1) violations of Cal. Penal Code § 630, *et seq*.; (2) violations of Cal. Civ. Code § 56, *et seq*.; (3) violations of Cal. Bus. & Prof. Code § 17200, *et seq*.; (4) violations of Cal. Const. Art. 1 § 1; and (5) intrusion upon seclusion.

JURISDICTION AND VENUE

26. The Court has personal jurisdiction over Defendant because DaVita, has 412 facilities in the state of California and does business in the state of California through those facilities.

27. This is a class action lawsuit brought pursuant to Code of Civil Procedure § 382, and this Court has jurisdiction over Plaintiff's claims because the amount in controversy exceeds this Court's jurisdictional minimum.

28. Venue is proper under Code of Civil Procedure §395(a), §395.5, and Civil Code §1780(c) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this county and the significant transactions giving rise to Plaintiff's claims occurred in this county.

THE PARTIES

29. Plaintiff [redacted] ("Plaintiff") is and adult citizen of the State of California and is domiciled in San Diego County, California.

30. DaVita, Inc. ("DaVita" or "Defendant") is a Colorado-based dialysis treatment center with 412 facilities located throughout California, including within San Diego county. According to its website, DaVita is a kidney dialysis specialist health care organization that develops solutions that will transform healthcare for patients with kidney disease, provides integrated care to help people better manage their kidney disease, and conducts clinical trial services across the spectrum of pharmaceutical and medical device development.[10]

FACTUAL ALLEGATIONS

A. Statutory Background

i. Background of California Invasion of Privacy Act

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

[10] https://www.davita.com/about (last visited April 25, 2023).

32. To establish liability under CIPA, Plaintiff need only establish that Defendant 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.

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

34. CIPA affords a private right of action to any person who has been subjected to a violation of the statute to seek injunctive relief and statutory damages of $5,000 per violation, regardless as to whether they suffered actual damages. Cal. Penal Code § 637.2.

ii. Background of the Confidentiality of Medical Information Act

35. Pursuant to the California Confidentiality of Medical Information Act ("CMIA"), "A provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in subdivision (b) or (c)." § 56.10(a).[11] "An authorization for the release of medical information . . . shall be valid if it:

> (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
>
> (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
>
> (c) Is signed and dated . . .
>
> (d) States the specific uses and limitations on the types of medical information to be disclosed.
>
> (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
>
> (f) States the name or functions of the persons or entities authorized to receive the medical information.
>
> (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
>
> (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.

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

(i) Advises the person signing the authorization of the right to receive a copy of the authorization.

Cal. Civ. Code § 56.11.

36. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as implementing a system that records and discloses online patients' personally identifiable information and protected health information. Cal. Civ. Code § 56.36(c).[12] Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

37. "In addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning them in violation of this part, for either or both of the following: [¶] (1) ... nominal damages of one thousand dollars ($1,000). To recover under this paragraph, it shall not be necessary that the Plaintiff suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient." *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551 (2014) (quoting Cal. Civ. Code § 56.36(b)).

B. Defendant's Website and Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiff's and Class Members' Private Information to Facebook.

38. Defendant's Website is accessible on mobile devices and desktop computers and allows patients to communicate with Defendant regarding the patients' past, present, and future health or medical care, as well as their past, present, and future medical bills and payments.

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

39. The Website gives patients the option to search for a specialist based on specific treatments or conditions, find facility locations, pay medical bills, receive a cost estimation of specific services using a patient's insurance information, and search symptoms, medical treatments, and medical services.

40. Defendant purposely installed the Pixel on its Website and programmed specific webpage(s) to surreptitiously share its patients' private and protected communications with Facebook, including Plaintiff's and Class Members' PHI and PII.

41. The Pixel tracks users as they navigate through the Website and simultaneously transmits to Facebook the users' communications with the Website, including which pages are visited, which buttons are clicked, specific information users enter into search bars and text boxes (e.g., "symptoms of kidney disease"), and other information including a patient's IP address.[13] Included in these communications transmitted to and intercepted by Facebook are Private Information, including, but not limited to, medical treatment sought, medical conditions, information pertaining to medical appointments and the selected physician, specific button/menu selections, and content (such as searches for symptoms or treatment options) typed into free text boxes.

42. As described by the HHS Bulletin, this is protected health information (PHI) even if the visitor has no previous relationship with Defendant because "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 benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care."[14]

[13] https://developers.facebook.com/docs/meta-pixel/ (last visited April 25, 2023)

[14] *See* HHS Bulletin § *How do the HIPAA Rules apply to regulated entities' use of tracking technologies?*

43. If the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their Facebook ID or "c_user id"), which includes other identifying information.

44. Plaintiff and Class Members did not and could not anticipate that Defendant would aid and conspire with Facebook to intercept and transmit their communications with DaVita.

45. To understand Defendant's unlawful data sharing practices, it is important to first understand basic web design, tracking tools, and web functions.

i. Facebook's Business Tools and the Pixel

46. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[15]

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

48. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of website visitors' activity.

49. 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

[15] *Facebook, Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited April 25, 2023).

metadata, button clicks, etc.[16] Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event." [17]

50. One such Business Tool is the Pixel, which "tracks the people and type of actions they take."[18] When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers. Notably, this transmission does not occur unless the webpage contains the Pixel. Stated differently, Plaintiff's and Class Members' Private Information would not have been disclosed to Facebook but for the Defendant's decisions to install the Pixel on its webpage(s).

51. As explained in more detail below, this secret transmission to Facebook is initiated by Defendant's source code concurrently with Plaintiff's and Class Members' communications to their intended recipient, Defendant.

ii. Defendant's Pixel, Source Code, and Interception of HTTP Requests

52. Web browsers are software applications that allow consumers to navigate the internet and exchange electronic communications, and every "client device" (computer, tablet, or smart phone) has a

---

[16] *Specifications for Facebook Pixel Standard Events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited April 25, 2023); *see* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited April 25, 2023).

[17] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBPAGE(S) EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (Last visited April 25, 2023).

[18] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting. (Last visited April 25, 2023).

web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

53. Correspondingly, every website is hosted by a computer "server" which allows the website's owner (Defendant) to display the Website and exchange communications with the website's visitors (Plaintiff and Class Members) via the visitors' web browser.

54. When a patient uses Defendant's website and undertakes various actions, the patient and Defendant are engaged in an ongoing back-and-forth exchange of electronic communications taking place via the patient's web browser and Defendant's computer server.

55. These communications are invisible to ordinary consumers[19] because they consist of HTTP Requests and HTTP Responses, and one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.

- **HTTP Request:** an electronic communication sent from the website visitor's browser to the website's corresponding server. In addition to specifying a particular URL (i.e., web address), "GET" HTTP Requests can also send data to the host server, including cookies. A cookie is a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response:** an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

56. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a "Find a Dialysis Center" page), and the HTTP Response renders or loads the

[19] See HHS Bulletin § *What is a tracking technology?* ("Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user.").

requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Webpage(s)).

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

58. For example, when a patient visits www.davita.com and selects the "Find a Dialysis Center" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that webpage. As depicted below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

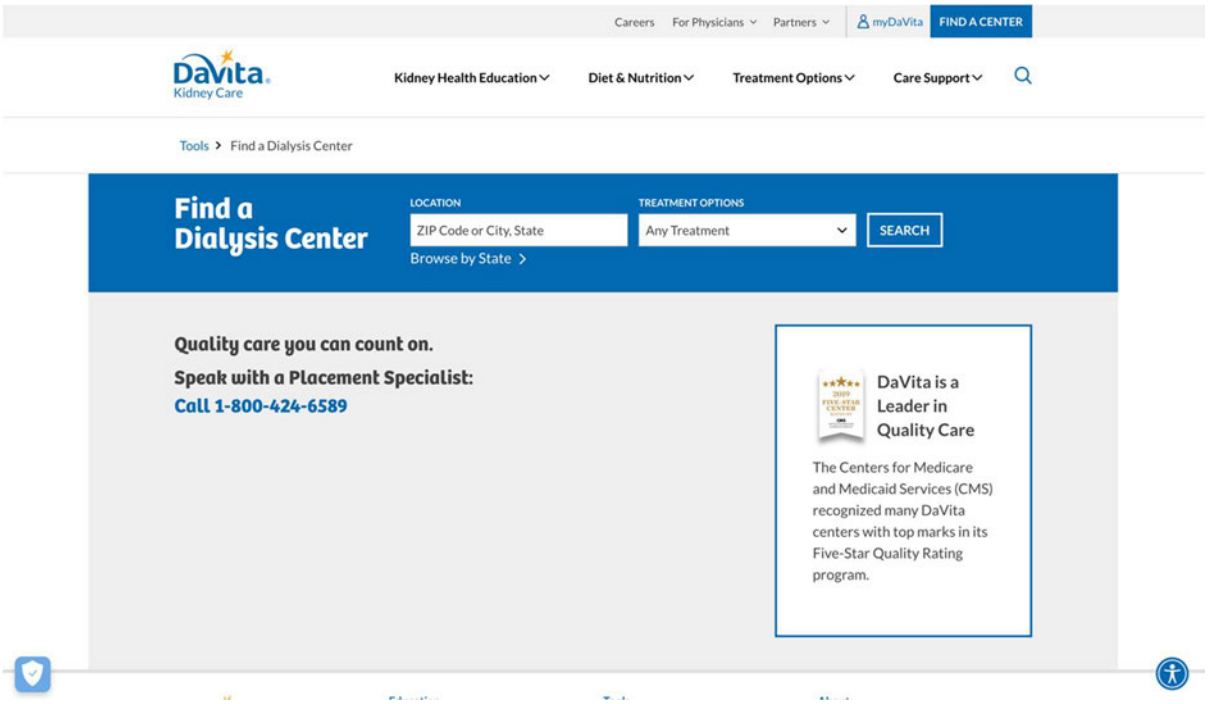


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting https://www.davita.com/ /tools/find-dialysis-center? (Last accessed Apr. 25, 2023).

59. The patient visiting this webpage only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

60. The Facebook Tracking Pixel is embedded in Defendant's Source Code contained in its HTTP Response. The Pixel, programmed to automatically track the patient's communications with Defendant's Website and transmit them to Facebook as they are communicated, executes instructions that effectively open a hidden spying window into the patient's browser through which Facebook can intercept the visitor's data, actions, and communications with Defendant.[20]

61. Looking to the previous example, Defendant's Source Code containing the Pixel manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to also send those communications to Facebook.

62. This communication to Facebook occurs contemporaneously, invisibly, and without the patient's knowledge.

63. Thus, without its patients' consent, Defendant have effectively used its source code to commandeer and "bug" or "tap" patients' computing devices, allowing Facebook to listen in on all their communications with Defendant and thereby intercept those communications, including Private Information.

64. Consequently, when Plaintiff and Class Members visit Defendant's Website and communicate their Private Information, including, but not limited to, medical treatment sought, appointment type, dialysis type desired, specific button/menu selections, content (such as searches for diets, kidney disease education, or treatment options) typed into free text boxes, and demographic information, it is simultaneously intercepted and transmitted to Facebook.

[20] When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. The Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

A. Defendant Disclosed Plaintiff's and Class Members' Private Information to Facebook Using the Pixel and/or Conversions API Tracking Practices.

65. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API on its Website and servers to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties, and obligations.[21]

66. Defendant's Pixel has its own unique identifier (represented as "id=1922159211337179"; "id=802325101033656"; "id=530586864070598 and/or "id=825898851225030") which can be used to identify which of Defendant's webpages contain the Pixel.

67. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences (for future targeting marketing and advertising), and decrease advertising and marketing costs.[22] However, Defendant's Website does not require the Pixel to function.

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

69. Plaintiff and Class Members were not aware that their Private Information would be shared with Facebook as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

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

71. Defendant's Pixel and Conversions API sent non-public Private Information to Facebook, including but not limited to information about Plaintiff's and Class Members' past, present, or future health or health care, such as their: (1) status as medical patients; (2) health conditions; (3) physician

[21] *Id.*

[22] *Id.*

searches; (4) desired locations or facilities where treatment was sought; and (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers) conducted via the general search bar.

72. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.23

73. A user's FID 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 ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

74. If a user accessed Defendant's Website while they were logged into Facebook, such as in the examples above, their c_user cookie—which contains the user's unencrypted FID—was transmitted to Facebook alongside 6 other cookies:

Name	Value	Domain
sb	EviWYHBCNlrLUD…	.facebook.com
c_user	100001028527210	.facebook.com
usida	eyJ2ZXIiOjEsImlkIjo…	.facebook.com
datr	LUNgZOg84ndHb…	.facebook.com
m_ls	%7B%22c%22%3…	.www.facebook.com
xs	21%3Ak8h4z26wK…	.facebook.com
fr	0x8LFPnGedeb4iic…	.facebook.com

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

75. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.[24]

Name	Value	Domain
sb	EviWYHBCNlrLUD…	.facebook.com
usida	eyJ2ZXIiOjEsImlkIjo…	.facebook.com
datr	LUNgZOg84ndHb…	.facebook.com
m_ls	%7B%22c%22%3…	.www.facebook.com
dpr	2	.facebook.com
fr	0ZqcFQtTjwegi5tq…	.facebook.com

76. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.[25] Facebook, at a minimum, uses the fr cookie to identify users.[26]

77. If a visitor has never created an account, an even smaller set of cookies are transmitted.

fr	0ZqcFQtTjwegi5tq…	.facebook.com

78. At each stage, Defendant also utilizes the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.[27]

_fbp	fb.1.168235772…	.davita.com

79. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook. If that happens, the time resets, and another 90 days begins to accrue.

80. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[28] If that happens, the time resets, and another 90 days begins to accrue.

[24] Not pictured here or in the preceding image is the _fbp cookie, which is transmitted as a first-party cookies instead of a third-party cookie.
[25] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.
[26] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.
[27] *Id.*
[28] *Id.*

81. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

82. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to Facebook IDs and corresponding Facebook profiles.

83. As shown in the above figures, based on its configuration of the Facebook Tracking Pixel on its Website, Defendant sends these identifiers to Facebook alongside the event data (i.e., the searches, page views, and button clicks described above).

84. Plaintiff never consented, agreed, authorized, or otherwise permitted DaVita to disclose her personally identifiable information and protected health information and assist third parties with intercepting her communications. Plaintiff was never provided with any written notice that Defendant discloses its Website users' protected health information, nor was she provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's Private Information to Facebook.

85. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications. DaVita deprived Plaintiff of her privacy rights when it: (1) implemented a system that surreptitiously tracked and disclosed Plaintiff's and other online patients' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party eavesdropper; and (3) undertook this pattern of conduct without notifying Plaintiff and without obtaining her express written consent. Plaintiff did not

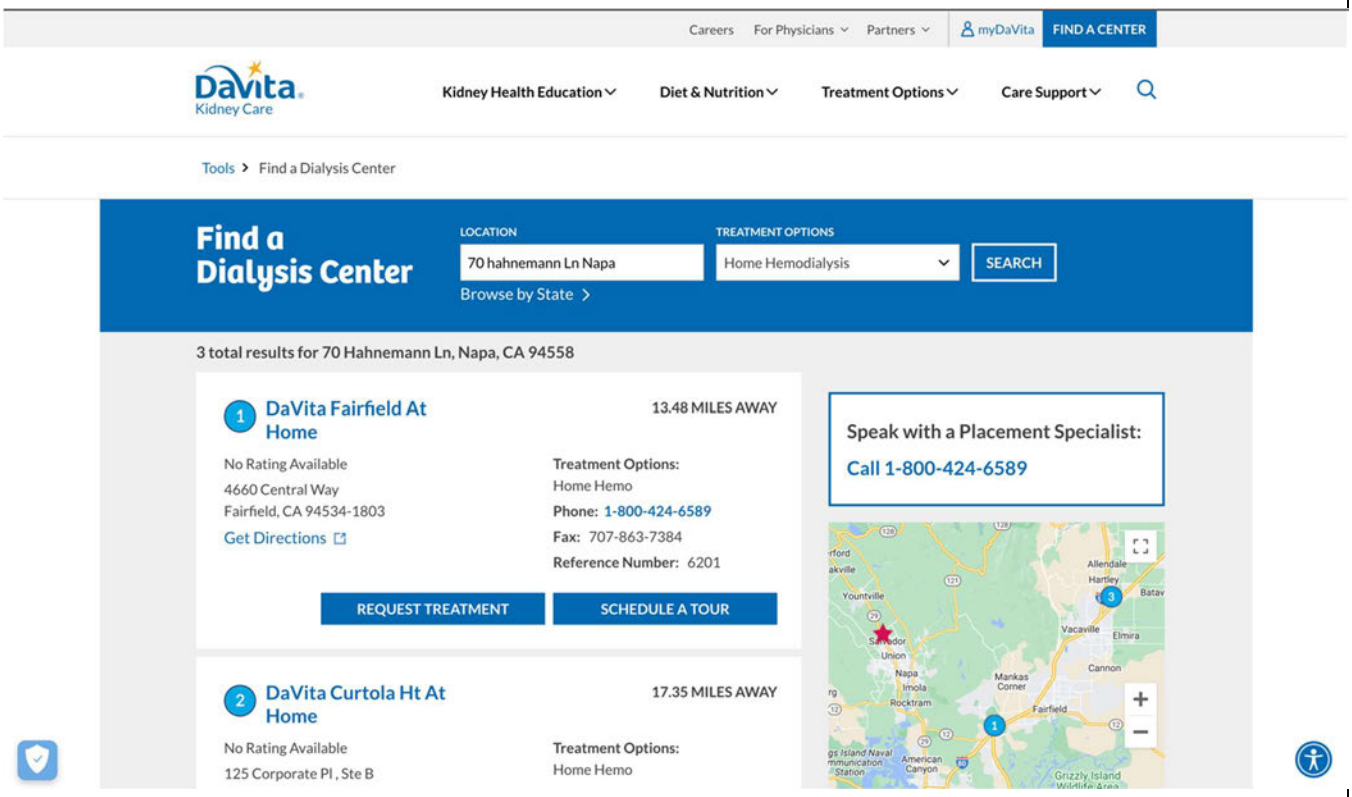
discover that DaVita disclosed her personally identifiable information and protected health information to Facebook, and assisted Facebook with intercepting her communications.

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

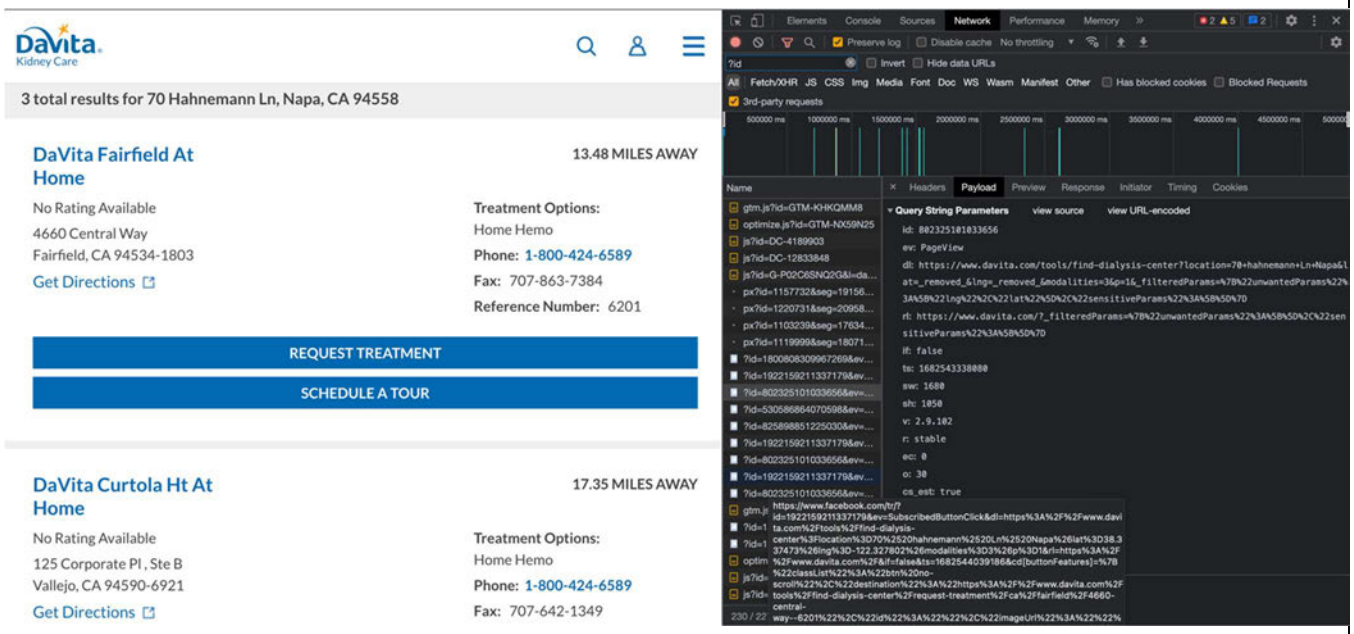
i. Defendant's Pixel Disseminates Patient Information via Its Website

87. An example illustrates the point. If a patient uses www.davita.com to request a dialysis treatment, Defendant's Website directs the patient to communicate Private Information, including their dialysis service, last time they received treatment, treatment frequency, their date of birth, their contact information, their street address, and their insurance provider. Unbeknownst to the patient, every communication is sent to Facebook via Defendant's Pixel, including the medical condition the patient types into the search bar and the filters they select.

88. In the example below, the user searched for a dialysis facility that offers "Home Hemodialysis and is located near their address, of "70 Hahnemann Lane, Napa, CA 94558, USA".

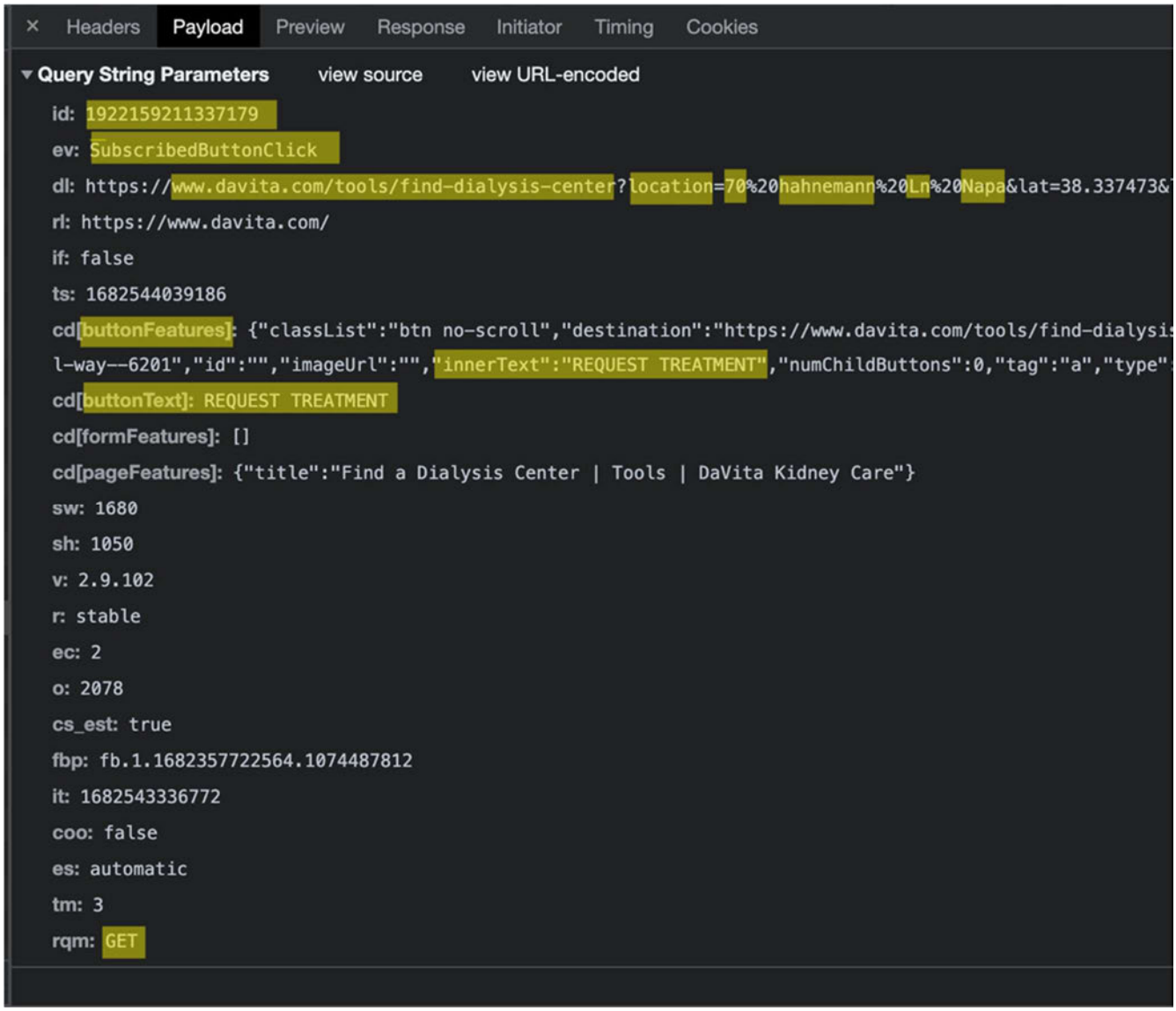


89. Unbeknownst to ordinary patients, this webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant's Pixel. The image below shows the "behind the scenes" portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Pixel sent this user's information to Facebook.



90. Thus, without alerting the user, Defendant's Pixel sends every communication the user made via the webpage to Facebook, and the images below confirm that the communications Defendant send to Facebook contain the user's Private Information.

91. The image below is a screenshot that shows what information is sent to Facebook when the patient clicks request treatment from the closest facility that meets their requested treatment type.



92. The first line of highlighted text, "id: 1922159211337179," refers to Defendant's Pixel ID and confirms that Defendant have downloaded the Pixel into its Source Code for this webpage.

93. The second line of text, "ev: SubscribedButtonClick," identifies and categorizes which actions the user took on the webpage ("ev:" is an abbreviation for event, and "SubscribedButtonClick" is the type of event). Thus, this identifies the user as having viewed the specific webpage after applying their search criteria, and it also identifies them as having clicked the button titled "[innertext]: REQUEST TREATMENT."

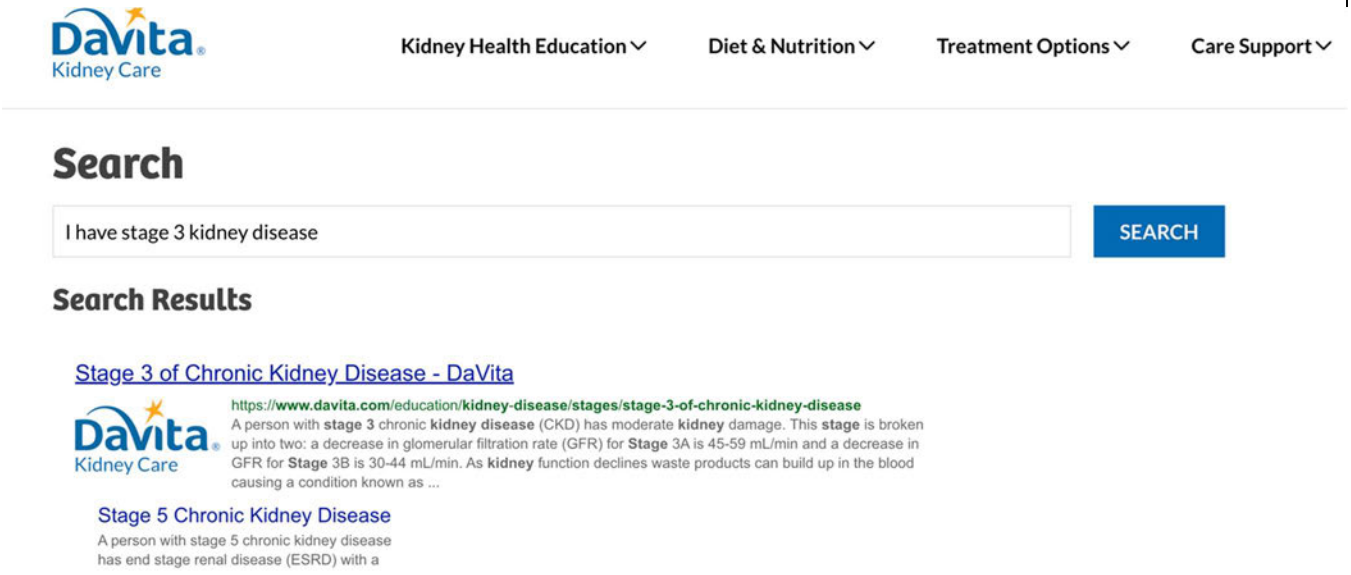
94. The next lines of highlighted text show Defendant disclosed to Facebook: (1) the fact that the user is a patient or prospective patient seeking medical care from Defendant via www.davita.com ("request treatment"); (2) to request treatment; (3) the user's address ("location=70 Hahnemann Ln. Napa"); and (4) the city of the treatment center provided.

95. Finally, the highlighted text ("GET") combined with the user's Facebook ID (highlighted as "c_user=" in the image below) demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID (c_user ID), thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.[29]

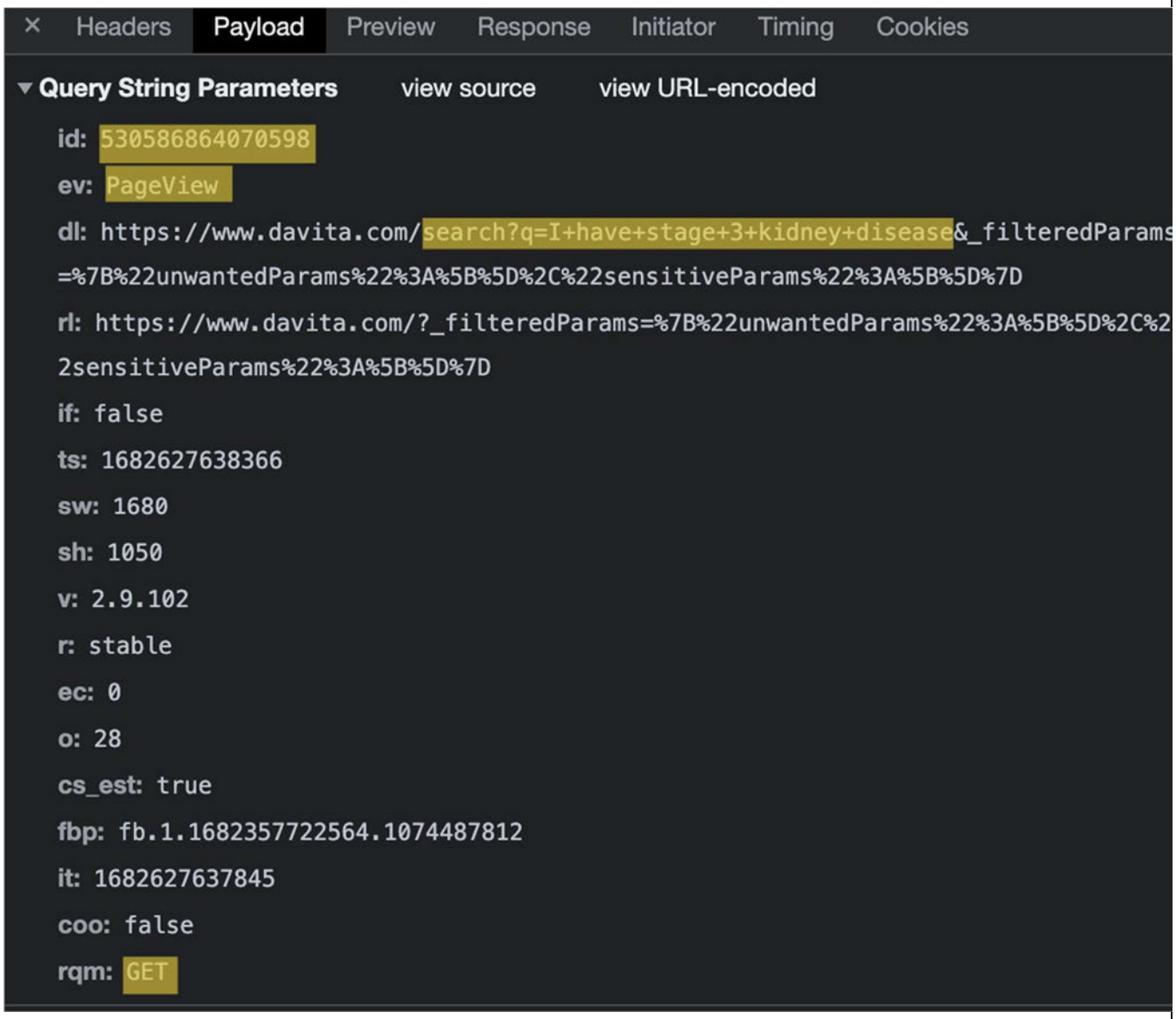
96. As seen in the image below, this information is sent to Facebook four times via four distinct pixel id's, each of which has been installed and incorporated within Defendant's source code.

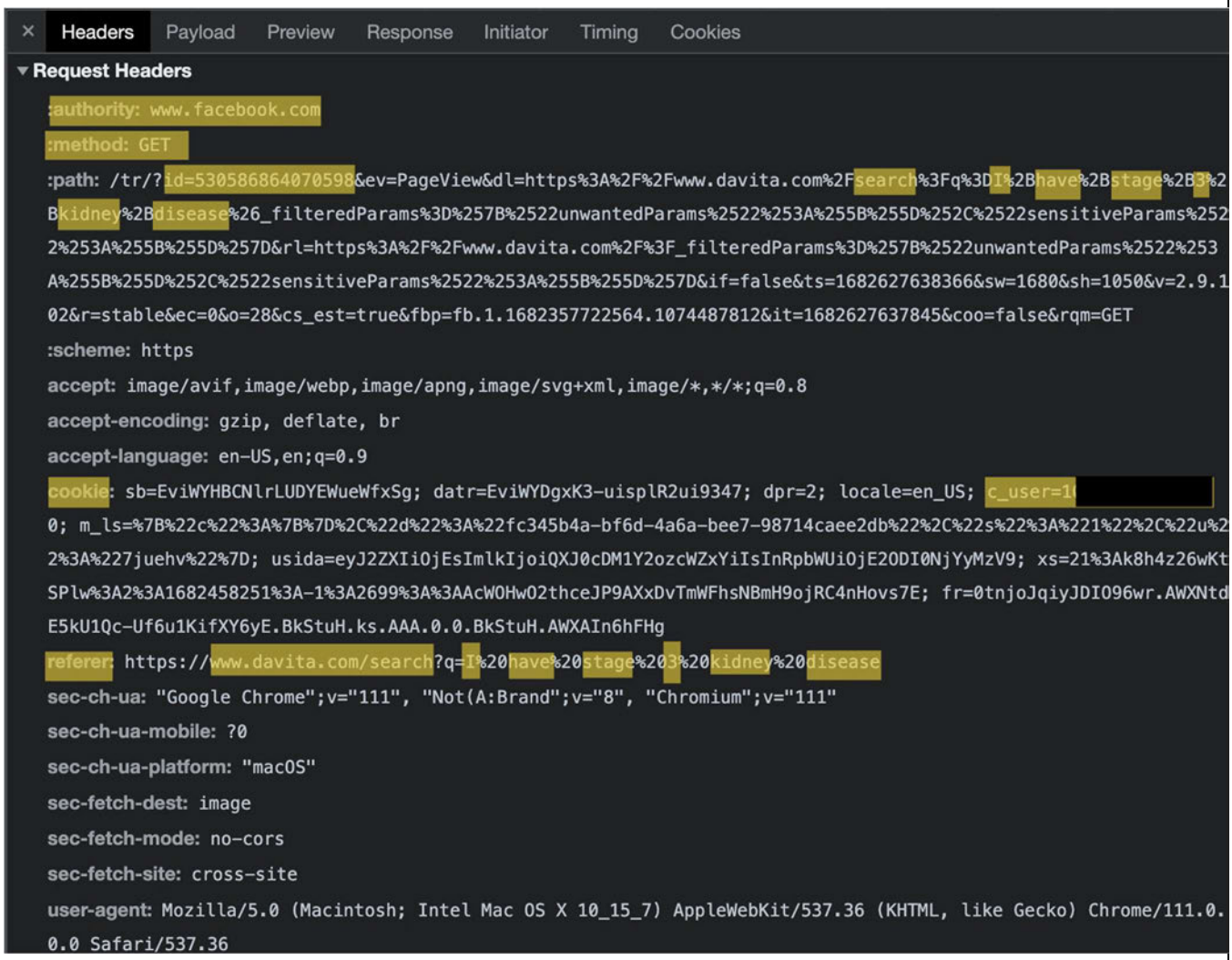
[29] The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiff has redacted the corresponding string of numbers to preserve the user's anonymity.

97. To make matters worse, Defendant's Pixel even tracks and records the exact text and phrases that a user types into the general search bar located on Defendant's homepage. In the example below, the user typed "I have stage 3 kidney disease" into the search bar.

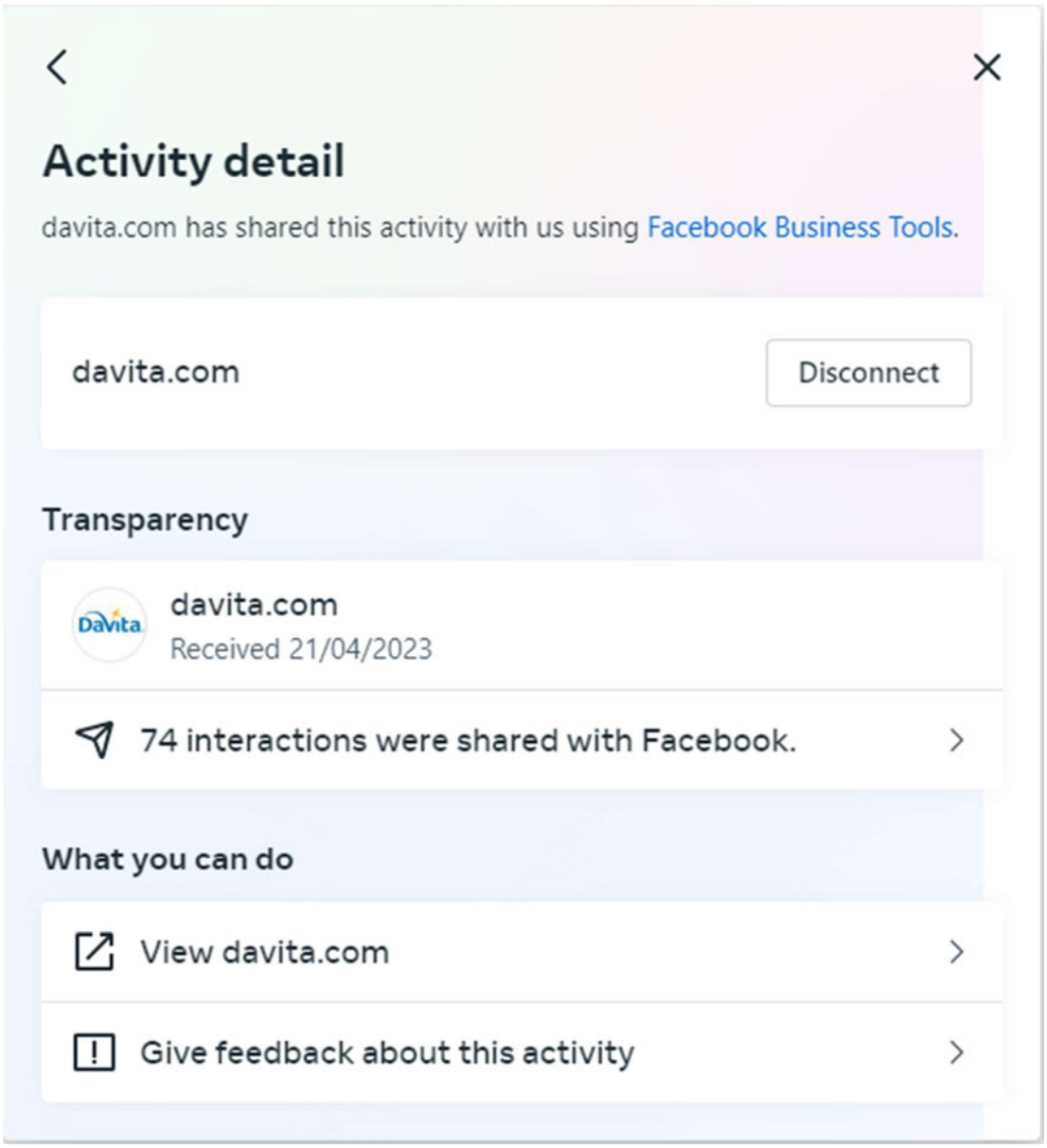


98. That exact phrase is sent to Facebook, allowing the user's medical condition to be linked to their individual Facebook account for future retargeting and exploitation. There is no legitimate reason for sending this information to Facebook.


Headers
Payload
Preview
Response
Initiator
Timing
Cookies
Query String Parameters
view source
view URL-encoded
id: 530586864070598
ev: PageView
dl: https://www.davita.com/search?q=I+have+stage+3+kidney+disease&_filteredParams
=%7B%22unwantedParams%22%3A%5B%5D%2C%22sensitiveParams%22%3A%5B%5D%7D
rl: https://www.davita.com/?_filteredParams=%7B%22unwantedParams%22%3A%5B%5D%2C%2
2sensitiveParams%22%3A%5B%5D%7D
if: false
ts: 1682627638366
sw: 1680
sh: 1050
v: 2.9.102
r: stable
ec: 0
o: 28
cs_est: true
fbp: fb.1.1682357722564.1074487812
it: 1682627637845
coo: false
rqm: GET

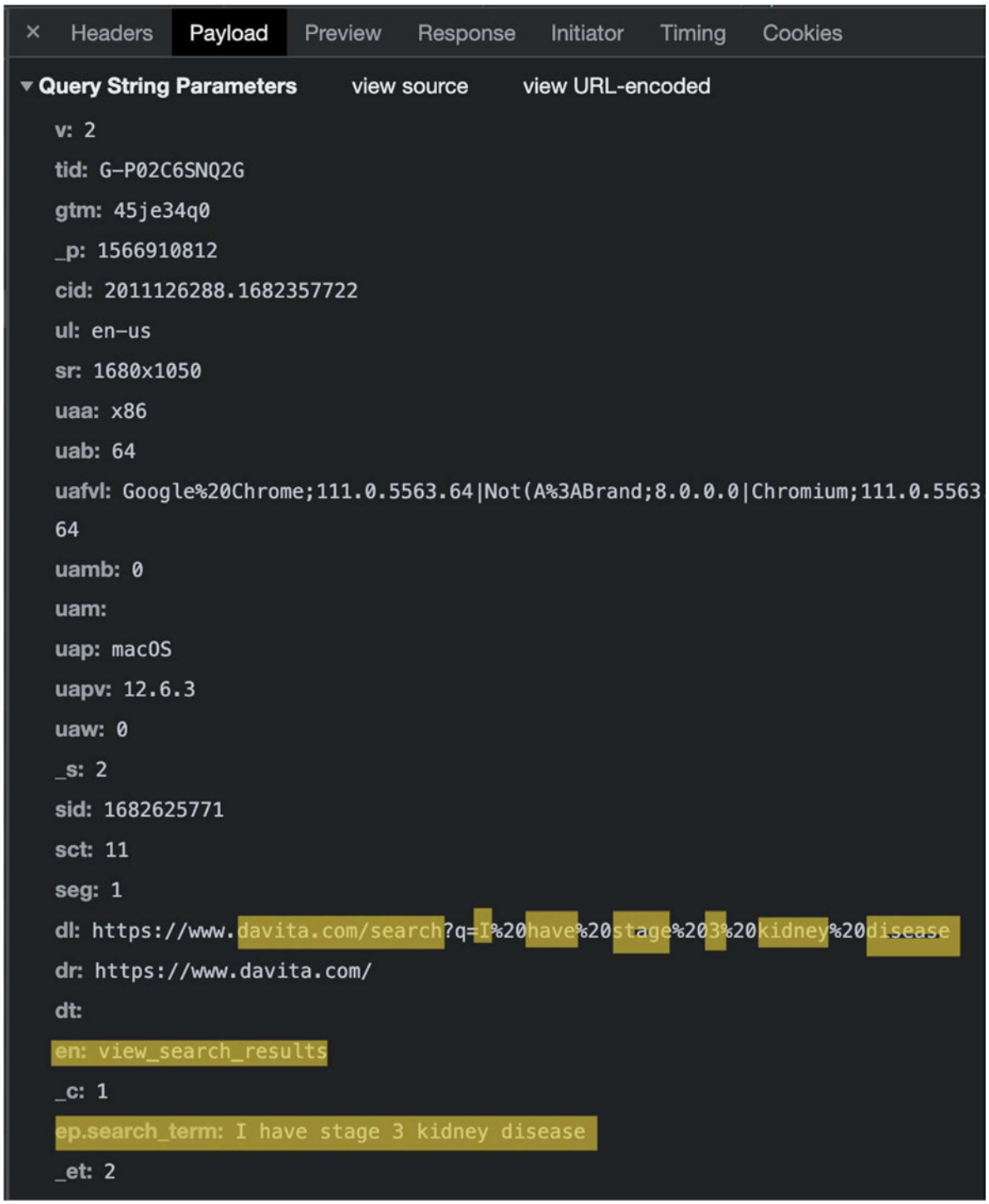


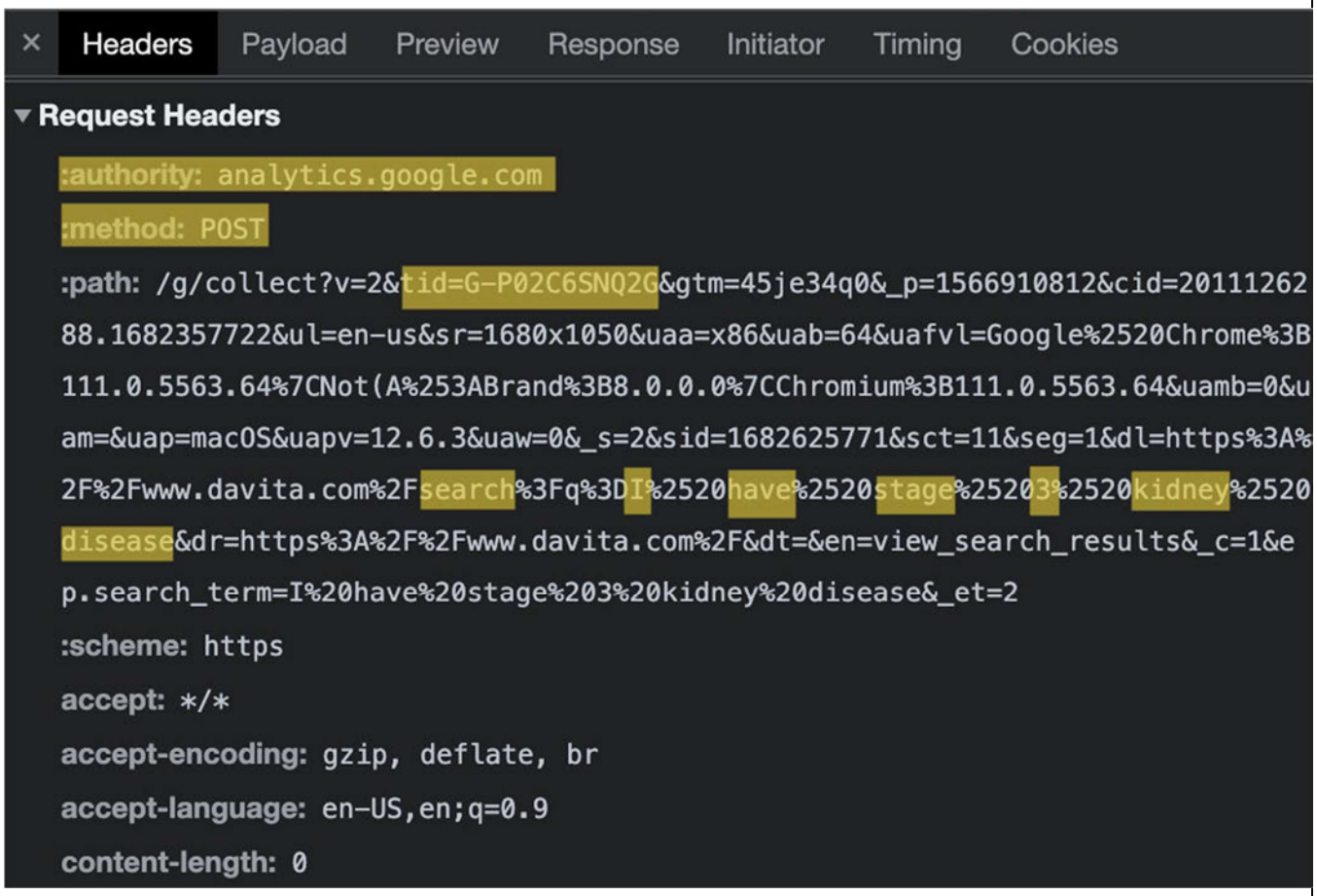
99. The image below, gathered from a website visitor's own Facebook account after the fact, makes it patently clear that Defendant are actively sending patient communications to Facebook, stating, "davita.com has shared this activity with us [74 times] using Facebook Business Tools."



100. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant are using additional tracking pixels and tools to transmit its patients' Private Information to additional third parties. For example, the images below indicate that Defendant is also sending its patients' protected health information to Google via the Google Analytics tool and Google Tag Manager.

101. Both images below contain the user's search phrase ("I have stage 3 kidney disease"), and Defendant do not appear to have enabled the anonymize feature provided by Google Analytics because the text "aip:" does not appear in either image.





102. Accordingly, Google receives patients' communications alongside the patients' IP address, which is also impermissible under HIPAA.

103. In addition, upon information and belief and as described above, Defendant has also installed Conversions API on its servers to record and store its patients' Website interactions and Private Information before transmitting that information direct to Facebook via Defendant's computer server.

104. Defendant did not disclose that the Pixel, Conversions API, Google Analytics, or any other tracking tools embedded in the Website's source code tracks, allows the interception of, records, and transmits Plaintiff's and Class Members' Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiff and Class Members' private communications to Facebook, Google, or any other third party. Defendant never received consent or

written authorization to disclose to Facebook, Google, or other third parties the Private Information entered by Plaintiff and Class Members via the Website.

105. Thus, without its patients' consent, Defendant effectively used its Source Code to commandeer and bug patients' computing devices, thereby re-directing their Private Information to unintended third parties (including Facebook) in real time, including but not limited to, medical treatment sought, medical treatment requested at particular locations and specific dates, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers, home addresses, birth dates, insurance provider information, and emergency contact information. This Private Information relates to the past, present, or future health or health care of Plaintiff and Class Members.

iii. Plaintiff's and Class Members' Private Communications to Defendant were Linked to their Individual Facebook Profiles.

106. The information that Defendant's Pixel sent to Facebook was transmitted alongside other information that reveals a particular patient's identity.

107. Every Facebook user has a unique and persistent Facebook ID ("FID") that is associated with their Facebook profile and individual account, and Facebook places a cookie containing the user's FID ("c_user" cookie) on their device when they log into Facebook.

108. The FID is categorized as a third-party cookie, and it identifies a particular person and their actions or communications with a website, such as www.davita.com, if, and only if, the owner of that Website has installed the Facebook Pixel.

109. When a person visits a website that is hosting the Pixel, the Pixel begins "listening in," much like a traditional wiretap, as soon as the website loads. The Pixel lies hidden within the page, waiting to be triggered.

110. Thus, prior to Defendant's recent removal of the Pixel, the Pixel was triggered each time Plaintiff and Class Members communicated with Defendant via www.davita.com (in the form of HTTP Requests to Defendant's server). Upon triggering of the Pixel, the Website user's communications were intercepted, duplicated, and secretly transmitted to Facebook at the same time the message was dispatched to Defendant. Thus, two simultaneous communications originate from a patient's browser once the patient initiates an action on the webpage: one, as intended, to Defendant, and a second, undetectable to and unknown by the patient, to Facebook.

111. Defendant did not inform Plaintiff and Class Members that Private Information communicated via www.davita.com would be shared with Facebook or other third parties.

112. Non-Facebook users also can be individually identified (by third parties such as Google) via the information they input into Defendant's Website, such as their home address or phone number, or via information they unwittingly share, like an IP address or personal device identifying information. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[30]

113. HIPAA requires that patient consent to disclosure of medical information be complete and conspicuous, and "the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures."[31]

[30] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited April 27, 2023).

[31] HHS Bulletin § *HIPAA compliance obligations for regulated entities when using tracking technologies* (emphasis in original).

C. The Extent of Defendant's Invidious Monitoring Cannot be Known Until the Parties Have Engaged in Discovery.

114. Defendant utilized Facebook's Business Tools and intentionally installed the Pixel on its Website to secretly track and disclose patients' activity and experiences in violation of its common law, contractual, statutory, and regulatory duties, and obligations.

115. The Pixel on Defendant's Website contained a unique identifier which unmistakably demonstrates that the Pixel was installed and embedded by Defendant. Defendant's unique Pixel codes were 1922159211337179; 802325101033656; 530586864070598; and/or 825898851225030.

116. The images and network data shown above, compiled prior to Defendant's removal of the Pixel, show that Defendant's Pixel monitored users' activity on the "Request Treatment" feature of Defendant's Website. Plaintiff cannot be sure at the pleading stage just how widespread and invidious Defendant's monitoring and surreptitious sharing of users' data was, however, because the Pixel is no longer running on Defendant's Website and because Conversions API is only installed on Defendant's servers and is not visible or accessible to Plaintiff.

117. Patients using the Website reasonably expect that their medical concerns, symptoms and medical histories, and the type of medical treatment they are seeking will be shared with Defendant purely to schedule and deliver patient care and treatment. They do not reasonably expect that Private Information will be shared with third parties like Facebook.

118. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information and assist Facebook with intercepting their communications. Despite this, Defendant knowingly aided, agreed, and conspired with Facebook to allow Facebook to do just that.

119. By law, Plaintiff and Class Members are entitled to privacy in their Private Information and confidential communications. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented a system that surreptitiously tracked and disclosed Plaintiff's and Class

Members' confidential communications, personally identifiable information, and protected health information to a third party; (2) disclosed patients' Private Information to Facebook—an unauthorized third-party eavesdropper; and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent. Plaintiff did not discover that Defendant disclosed her Private Information to Facebook, and assisted Facebook with intercepting their communications, until speaking with Counsel.

D. Facebook Exploited and Used Plaintiff's and Class Members' Private Information.

120. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"[32] and Facebook has built its more-than $300 billion market capitalization on mining and using that 'digital' oil. Thus, the large volumes of personal and sensitive health-related data Defendant provide to Facebook are actively viewed, examined, analyzed, curated, and used by the company. Facebook acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Facebook offers the Pixel free of charge[33]and the price that Defendant pay for the Pixel is the data that it allows Facebook to collect.

121. Facebook describes itself as a "real identity platform,"[34] meaning users are allowed only one account and must share "the name they go by in everyday life."[35] To that end, when creating an account, users must provide their first and last name, date of birth, and gender.[36]

[32] https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited April 25, 2023).

[33] https://seodigitalgroup.com/facebook-pixel/ (last visited April 25, 2023).

[34] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[35] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity (last visited April 5, 2023).

[36] FACEBOOK, SIGN UP, https://www.facebook.com/ (last visited April 25, 2023).

122. Facebook sells advertising space by emphasizing its ability to target users.[37] Facebook is especially effective at targeting users because it surveils user activity both on and off its own site (with the help of companies like Defendant).[38] This allows Facebook to make inferences about users beyond what they explicitly disclose, including their "interests," "behavior," and "connections."[39] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[40]

123. Advertisers can also build "Custom Audiences,"[41] which helps them reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[42] With Custom Audiences, advertisers can target existing customers directly. They can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[43] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Facebook. This data can be supplied to Facebook by manually uploading

---

[37] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited April 25, 2023).

[38] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited April 25, 2023).

[39] *Facebook, Ad Targeting: Help your ads find the people who will love your business*, https://www.facebook.com/business/ads/ad-targeting (last visited April 25, 2023).

[40] *Facebook, Easier, More Effective Ways to Reach the Right People on Facebook*, https://www.facebook.com/business/news/Core-Audiences (last visited April 25, 2023).

[41] *Facebook, About Custom Audiences*, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited April 25, 2023).

[42] *Facebook, Ad Targeting, Help your ads Find the People Who Will Love Your Business*, https://www.facebook.com/business/ads/ad-targeting (last visited April 25, 2023).

[43] *Facebook, About Lookalike Audiences*, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited April 5, 2023).

contact information for customers or by utilizing Facebook's "Business Tools" like the Pixel and Conversions API.[44]

124. Facebook does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever viewing or accessing the information. Instead, in accordance with the purpose of the Pixel to allow Facebook to create Core, Custom, and Lookalike Audiences for advertising and marketing purposes, Facebook viewed, processed, and analyzed Plaintiff's and Class Members' confidential Private Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Facebook employees at the direction and behest of Facebook.

125. Facebook receives over 4 petabytes[45] of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data to augment human effort.[46] This process is known as "data ingestion" and allows "businesses to manage and make sense of large amounts of data."[47]

126. By using data ingestion tools, Facebook can rapidly translate the information it receives from the Pixel to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage

---

[44] *Facebook, Create a Customer List Custom Audience*, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited April 5, 2023); *Facebook, Create a Website Custom Audience*, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited April 5, 2023).

[45] A petabyte is equal to one million gigabytes (1,000,000 GB).

[46] https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4. Facebook employees would not be able to view each piece of data individually – millions of them per second – without the aid of technology. Just as a microscope or telescope allows the user to see very small or very distant objects by zooming in, however, Facebook's big data management software allows the company to see all this data at once by zooming out.

[47] https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/. Facebook uses ODS, Scuba, and Hive to manage its massive data stores. These technologies are not traditional databases; they are specialized databases for big data designed to process data specifically for analysis—"such as [viewing] hidden patterns, correlations, market trends and customer preferences."

and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper's Facebook page.[48] This evidences the fact that Facebook views and categorizes data as they are received from the Pixel.

127. Moreover, even if Facebook eventually deletes or anonymizes sensitive information that it receives, it must first view that information to identify it as containing sensitive information suitable for removal. Accordingly, there is a breach of confidentiality the instant the information is disclosed or received without authorization. As described by the HHS Bulletin:

> It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

(emphasis in original).

E. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures and Plaintiff's and Class Members' Data and Private Information Had Financial Value

128. Tracking technologies like the Facebook Pixel serve the sole purpose of bolstering Defendant profits via marketing and advertising.

129. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook, Google, and the like in the form of enhanced advertising services and more cost-efficient marketing on its Website.

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

---

[48] *A Complete Guide to Facebook Tracking for Beginners*, OBERLO, Oct. 5, 2021, https://www.oberlo.com/blog/facebook-pixel.

131. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

132. Defendant's disclosure of Private Information harmed Plaintiff and the Class. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is expected to continue to increase, and estimates for 2022 are as high as $434 per user, constituting over $200 billion industry wide.

133. The value of health data in particular is well-known and has 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.[49]

134. 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."[50] Accordingly, patient data that can be linked to a specific individual is even more valuable.

F. IP Addresses are Personally Identifiable Information.

135. On information and belief, with the Facebook Pixel and Google Analytics tools on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook and Google with intercepting Plaintiff's and Class Members' computer IP addresses.

136. An IP address is a number that identifies the address of a device connected to the Internet, and it is used to identify and route communications on the Internet.

---

[49] *See* https://time.com/4588104/medical-data-industry/ (last visited April 25, 2023).

[50] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited April 25, 2023).

137. Internet service providers, Websites, and third-party tracking companies use individual's IP addresses to facilitate and track Internet communications.

138. Facebook tracks every IP address ever associated with a Facebook user and uses IP addresses to target individual homes and their occupants with advertising. In addition, as noted above, Defendant use Google Analytics tools and Google Tag Manager without anonymizing users' IP addresses.

139. Under HIPAA, an IP address is considered personally identifiable information:

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

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

G. Defendant Violated Industry Standards

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

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

143. 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 few aspects, including, … personal data (informational privacy)

144. 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 provide needed services most effectively. 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.

145. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

H. Plaintiff JANE DOE's Experience with Defendant's Website

146. Plaintiff used Defendant's Website to communicate regarding her past, present, and future health, and medical care, including to identify Dialysis locations, obtain recipes designed to aid kidney function and health, and research different types of dialysis treatments. In doing so, Plaintiff communicated PII and PHI to Defendant. Without her knowledge or permission, Facebook and Google intercepted and received, and Defendant disclosed the contents of those communications.

147. Plaintiff reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

148. Plaintiff has an active Facebook account that she accesses several times a day through her android smartphone and laptop.

149. Plaintiff used Defendant's Website to find dialysis locations and schedule her initial appointments. Because Defendant utilizes the Facebook Pixel, the Website's Source Code sent a secret set of instructions back to Plaintiff's browser—which effectively acted as a wiretap—causing the Pixel to

send Plaintiff's FID, and the webpage's URL, and the contents of her communications to Facebook (including PHI and PII contained within those communications).

150. Stated differently, Defendant's use of the Pixel aided in and allowed Facebook to intercept Plaintiff's Private Information and communications as she used Defendant's Website. Additionally, the information intercepted by Facebook via the Pixel included Plaintiff's Facebook ID, linking her communications with her Facebook profile.

151. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.51 Plaintiff's and Class Members identities can easily be determined based on their Facebook ID, IP address, digital fingerprint, or reverse lookup from the collection of other identifying information that was improperly disclosed.

152. Through the process detailed in this Complaint, Defendant assisted Facebook with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Defendant facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

153. Moreover, Defendant breached Plaintiff's right to privacy and unlawfully disclosed her Private Information to Facebook and other third parties. Likewise, Defendant did not inform Plaintiff that it shared her Private Information with Facebook or other third parties. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

154. Upon information and belief, as a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant also used server-to-

[51]https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited April 5, 2023).

server data transmissions, like Conversions API, to send Plaintiff's Private Information directly to Facebook from electronic storage on Defendant's server.

155. Plaintiff has a continuing interesting in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure. Moreover, Plaintiff cannot take proactive measures to guard her information from future use or harassment because she does not know the identity of every third-party who received their communications, or the information embedded within those communications.

156. Plaintiff suffered damages in the form of (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to her Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff's medical conditions and other confidential information she communicated to Defendant via the Website.

CLASS ACTION ALLEGATIONS

157. **Class Definition:** Pursuant to Section 382 of the Code of Civil Procedure, Plaintiff bring this action on behalf of themselves and other similarly situated individuals (the "Class"), defined as California citizens who, during the Class Period, were patients of Davita and used Davita's Website. Plaintiff reserves the right to modify the class definitions or add sub-classes as necessary prior to filing a motion for class certification.

158. The "Class Period" is the period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement or preliminary approval of a settlement.

159. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant;

any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

160. 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 Plaintiff currently. However, it is estimated that there are thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party Facebook's records.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CLAIMS FOR RELIEF

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

165. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed Class.

166. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

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

Cal. Penal Code § 630.

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

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to

> communicate in any way, any information so obtained, or **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

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

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

170. Defendant intentionally inserted an electronic listening device onto Plaintiff's and Class Members' web browsers that, without the knowledge and consent of Plaintiff and Class Members, tracked and transmitted the substance of their confidential communications with Defendant to a third party.

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

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

173. Defendant failed to disclose its use of the Facebook Pixel, Google Analytics, or other tracking technologies to specifically track and automatically and simultaneously transmit Plaintiff's and Class Members' communications with Defendant to undisclosed third parties.

174. The Private Information that Defendant transmitted via the Facebook Pixel, such as dialysis treatment center locations and scheduling, IP addresses, and home addresses constitutes information about Plaintiff's and Class Members' past, present, or future health or health care, conditions, or concerns and therefore constitutes protected health information.

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

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

177. By disclosing Plaintiff's and Class Members' Private Information, Defendant violated Plaintiff's and Class Members' statutorily protected right to privacy.

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

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

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

180. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

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

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

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

184. As set forth above, names, addresses, telephone numbers, email addresses, device identifiers, web URLs, IP addresses, and other characteristics that can uniquely identify Plaintiff and Class Members are transmitted to Facebook and Google in combination with patient medical conditions, medical concerns, treatment(s) sought by the patients, dialysis appointments, and other patient searches and queries. This protected health information and personally identifiable information constitutes confidential information under the CMIA.

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

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

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

188. Defendant failed to obtain Plaintiff's and Class Members' authorization for the disclosure of medical information.

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

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

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

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

192. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

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

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

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

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

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

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

199. As a result of Defendant's violations of the UCL, Plaintiff and Class Members are entitled to injunctive relief. This is particularly true since the dissemination of Plaintiff's and Class Members information is ongoing.

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

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

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

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

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

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

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

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

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

208. 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.

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

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

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

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

213. Plaintiff also seeks such other relief as the Court may deem just and proper.

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

214. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth therein and brings this claim individually and on behalf of the proposed Class.

215. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communications platforms and services therein.

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

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

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

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

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

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

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

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

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

225. Plaintiff also seeks such other relief as the Court may deem just and proper.

SIXTH CAUSE OF ACTION

Common Law Invasion of Privacy – Publication of Private Facts

226. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

227. Plaintiff's and Class Members' Private Information, including their Internet communications and sensitive data, are private facts that Meta acquired without the knowledge or consent of Plaintiff and Class Members.

228. Defendant gave publicity to Plaintiff's and Class Members' Private Information and the content of their communications by sharing them with unauthorized third parties. Many of those companies have business models predicated on building massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

229. Plaintiff and Class Members had no knowledge that Defendant was using software to track and disclose their Private Information because Defendant provided no information about such tracking and Plaintiff did not otherwise consent to being tracked on third party websites.

230. Defendant's surreptitious tracking and commoditization of Plaintiff's and Class Members' Private Information would be highly offensive to a reasonable person, particularly given that Defendant was their healthcare provider with whom they thought they were communicating confidential facts.

231. In disseminating Plaintiff's and Class Members' personal information without their consent in the manner described above, Defendant acted with oppression, fraud, or malice.

232. Plaintiff and Class Members have been damaged by the publication of their Private Information and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

SEVENTH CAUSE OF ACTION
Common Law– Breach of Confidence

233. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

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

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

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

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

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

239. Defendant disclosed Plaintiff's and Class Members' confidential information for Defendant's own economic benefit in Defendant's own business and disclosing it without Plaintiff's and Class Members' consent.

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

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

242. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's breach of their confidence and are entitled to just compensation, including monetary damages.

243. Plaintiff also seeks such other relief as the Court may deem just and proper.

RELIEF REQUESTED

Plaintiff, on behalf of herself and the proposed Class, respectfully requests that the Court grant the following relief:

(a) Certification of this action as a class action and appointment of Plaintiff and Plaintiff's counsel to represent the Class;

(b) A declaratory judgement that Defendant violated: (1) the California Invasion of Privacy Act; (2) the California Confidentiality of Medical Information Act; (3) the Unfair Competition Law; (4) Plaintiff's and Class Members' privacy rights as provided at common law and pursuant to the California Constitution; and (5) Plaintiff's and Class Members' other rights under common law;

(c) An order enjoining Defendant from engaging in the unlawful practices and illegal acts described therein; and

(d) An order awarding Plaintiff and the Class: (1) actual or statutory damages; (2) punitive damages—as warranted—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 attorneys' fees and expenses and costs of suit pursuant to Cal. 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

Plaintiff, on behalf of themselves and the proposed Class, demand a trial by jury for all the claims asserted in this Complaint so triable.

Date: June 16, 2023

Respectfully submitted,

/s/ John J. Nelson
John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

Counsel for Plaintiff and the Putative Class

ClassAction.org
