UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

JACQ NIENABER, ***on behalf of herself and all others similarly situated*****,** **Plaintiff,** **v.** **OVERLAKE HOSPITAL MEDICAL CENTER,** **Defendant.**	**Judge** **Case No.** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jacq Nienaber brings this action in her individual capacity and on behalf of all others similarly situated against Defendant Overlake Hospital Medical Center ("Overlake" or "Defendant"), and alleges, upon personal knowledge as to her own actions, her counsel's investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this case to address Defendant's illegal and widespread practice of disclosing 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").

2. Defendant owns and controls the website https://www.overlakehospital.org, along with the Overlake Patient Portal which can be accessed from its website (collectively, the "Website"). Through the Website, patients can access information about various conditions and treatments, Overlake's numerous locations and the practitioners at each location, and other general information about Overlake and the services it offers to its patients. The Website also enables

patients to input their real time symptoms and experiences on the Website and receive feedback based on the medical information they supply.[1] Critically, a patient can also access their Patient Account through the Website, which contains other aspects of their Private Information.

3. Defendant installed and implemented the Facebook Tracking Pixel (the "Pixel" or "Facebook Pixel") on its Website, which secretly enables the unauthorized transmission and disclosure of Plaintiff's and Class Members' Private Information as it is communicated to Defendant.

4. Based on Defendant's use of the Pixel, and evidence demonstrating that the information transmitted via the Pixel was indeed linked to Plaintiff's personal Facebook account, Plaintiff asserts Defendant also installed and implemented the Facebook Conversions Application Programming Interface ("Conversions API") on its Website.

5. By implementing Conversions API, Defendant secretly enabled additional unauthorized transmissions and disclosures of Plaintiff's and Class Members' Private Information.[2]

6. More specifically, Defendant's Website directs Plaintiff's and Class Members' communications to automatically and surreptitiously be sent to Facebook's servers. This occurs on every webpage on which Defendant has installed the Tracking Pixel and Conversions API.[3]

---

[1] *MyChart for Overlake Medical Centers and Patients*, https://mychart.overlakehospital.org/MyChart/Authentication/Login? (last visited August 3, 2023)

[2] "Conversions API works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See How to implement Conversions API,* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited: July 19, 2023).

[3] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *Conversions API*, Meta for Developers,https://developers.facebook.com/docs/marketing-api/conversions-api (last visited: July 19, 2023).

7. Thus, 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").

8. Similarly, Conversions API stores Plaintiff's and Class Members' Private Information from visiting Defendant's Website and transmits it to Facebook.

Tracking Pixel

9. A pixel is a piece of code that "tracks the people and the types of actions they take"[4] 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, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), and more.

10. The User's web browser executes the Pixel via instructions within the Defendant's webpage to communicate directly to Facebook certain parameters defined by the Defendant.

11. The pixel can share the user's Facebook User ID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser.[5] Cookies are only transmitted to the owner site from the user's web browser and cannot be accessed by any other site.

12. The Facebook Pixel is programmable, meaning that the Defendant controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

---

[4] *How Does Retargeting on Facebook Help Your Business?*, Meta Retargeting, ttps://www.facebook.com/business/goals/retargeting (last visited July 19, 2023).

[5] "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." *What are Cookies?*, CloudFare, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited: July 19, 2023).

13. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data for marketing purposes in an effort to bolster its profits. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions, symptoms, and treatments, and other information disclosed to Defendant.

Conversions API

14. The Facebook Conversions API allows businesses and companies to send web events from their servers to Facebook.[6]

15. Conversions API is designed to create a direct and reliable connection between marketing data (such as website events and offline conversions) from Defendant's server to Facebook.[7] In doing so, Defendant stores Plaintiff's and Class Members' Private Information on Defendant's own server and then transmits it to Facebook.

16. Conversions API is an alternative method of tracking versus the Pixel because no privacy protections on the user's end can defeat it. This is because it is implemented Server-Side, rather than executed by Users' web browsers.

[6] *What is Facebook Conversions API and How to Use It*, Revealbot (May 20, 2022), https://revealbot.com/blog/facebook-conversions-api/ (last visited: July 19, 2023).
[7] *About Conversions API*, Meta Business Help Center, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited: July 19, 2023).

17. Because Conversions API is Server-Side, it cannot access the Facebook Cookie to retrieve the Facebook User ID.[8] Therefore, other round-about methods of linking the user to their Facebook account must be employed.[9]

18. Facebook has an entire page within their developers' website about how to de-duplicate data received when both a Pixel is executed as well as Conversions API.[10]

19. Conversions API tracks the user's website interaction, including Private Information, and then transmits this data to Facebook. Indeed, Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."

Purpose of this Lawsuit

20. Accordingly, this case arises from Defendant's intentional, reckless, and/or negligent disclosure of Plaintiff's and Class Members' confidential and private medical information to Facebook.

21. The information that Defendant's Tracking Pixel and Conversions API sent to Facebook included Private Information that Plaintiff and Class Members submitted to Defendant's

[8] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only." *Customer Information Parameters*, Meta for Developers, https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited: July 19, 2023).

[9] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." *Send Required and Recommended Parameters*, Meta for Developers, https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req-rec-params (last visited: July 19, 2023).

[10] *Handling Duplicate Pixel and Conversions API Events*, Meta for Developers, https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events (last visited: July 19, 2023).

Website, including for example, the type of medical treatment sought, the particular health condition, and the fact that the individual attempted to or did book a medical appointment. Such Private Information would allow a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, dementia, or HIV.

22. 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 Conversions API.

23. For instance, Plaintiff submitted medical information to Defendant's Website and used the Website to schedule appointments with healthcare professionals, communicate with her doctors and communicate Private Information, complete patient web forms, and review medical healthcare and billing records.

24. Shortly thereafter, this information was communicated from Defendant's Website to Facebook.

25. Defendant regularly encourages Plaintiff and Class Members to use its digital tools, including its Website, to receive healthcare services. Plaintiff and Class Members provided their Private Information through Defendant's Website with the reasonable understanding that Defendant would secure and maintain that Private Information as confidential.

26. At all times Plaintiff and Class Members visited and utilized Defendant's Website, they had a reasonable expectation of privacy in the Private Information collected through Defendant's Website, including that it would remain secure and protected and only utilized for medical purposes.

27. Plaintiff and Class Members provided Private Information to Defendant in order to receive medical services rendered and with the reasonable expectation that Defendant would protect their Private Information. Plaintiff and Class Members relied on Defendant to secure and protect the Private Information and not disclose it to unauthorized third-parties without their knowledge or consent.

28. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

29. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

30. Defendant, however, failed in its obligations and promises by utilizing the Facebook Pixel and Conversions API, described below, on its Website knowing that such technology would transmit and share Plaintiff's and Class Members' Private Information with Facebook.

31. While Defendant willfully and intentionally incorporated the Tracking Pixel and Conversions API into its Website, Defendant never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications via the Website with Facebook. As a result, Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated their healthcare information and other Private Information via the Website.

32. Defendant breached its obligations in one or more of the following ways: (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 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.

33. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (vi) the continued and ongoing risk to their Private Information.

34. Plaintiff seek to remedy these harms and bring causes of action for (i) Negligence; (ii) Invasion of Privacy; (iii) Breach of Confidence; (iv) Breach of Implied Contract; (v) Unjust Enrichment; (vi) Violations of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1)—unauthorized interception, use, and disclosure; (vii) Violations of ECPA, 18 U.S.C. § 2511(3)(a)—unauthorized interception, use, and disclosure; (viii) Violations of Title II of the ECPA, 18 U.S.C. § 2702, *et seq*.—Stored Communications Act; and (ix) Violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq*.

PARTIES

Plaintiff Jacq Nienaber

35. Plaintiff is a natural person and citizen of Washington, where she intends to remain.

On numerous occasions, Plaintiff accessed Defendant's Website. Plaintiff used the Website to find and obtain medical treatment. Pursuant to the systematic process described herein, Plaintiff's Private Information was disclosed to Facebook, and this data included her PII, PHI, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

36. Plaintiff is a current patient of Overlake and Plaintiff has been one of Defendant's patients for many years and has used the Website numerous times since she first engaged Defendant for healthcare services. She has used her account to access the Website and use various digital services provided by Defendant since at least 2019.

37. Plaintiff Nienaber used Defendant's Website to conduct the following activities: request and schedule appointments, communicate with healthcare professionals, complete medical forms, and request and review healthcare and billing records.

38. As Defendant's patient, Plaintiff Nienaber reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted or intercepted by a third party. Plaintiff also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff would not have disclosed her Private Information to Defendant.

39. During her time as a patient, Plaintiff Nienaber never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook and Google, to access or interpret such information.

40. Notwithstanding, through the Tracking Pixel and Conversions API, Defendant transmitted Plaintiff Nienaber's Private Information to third parties, such as Facebook and Google.

41. Plaintiff Nienaber has been a regular Facebook user for more than five years.

42. Shortly after using Defendant's Website Plaintiff has seen numerous targeted advertisements on Facebook related to her medical conditions and treatments sought through Overlake.

Defendant Overlake Hospital Medical Center

43. Defendant Overlake is a nonprofit healthcare organization, headquartered at 1035 116th Ave NE, Bellevue, Washington 98004.

44. Defendant is one of the largest nonprofit hospital systems in the country, operating a 349-bed hospital and over 1,300 affiliated providers on its medical staff, including more than 300 physicians and advanced-practice providers who are employed by the organization.

45. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 "HIPAA").

JURISDICTION & VENUE

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

47. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*, and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq*).

48. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

49. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

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

50. Defendant intentionally placed the Pixel and Conversions API tools on numerous webpages of its Website, for the purpose of transmitting patients' confidential and safeguarded communications to Facebook. This transmission includes communications containing Plaintiff's and Class Member's Private Information.

51. Defendant uses its Website to connect Plaintiff and Class Members to Defendant's digital healthcare platforms with the goal of increasing profitability.

52. In order to fully understand Defendant's unlawful data-sharing practices, it is important to understand basic web design and tracking tools.

Facebook's Business Tools and the Pixel

53. Facebook currently 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.[11]

54. As part of its advertising operations, Facebook actively encourages and supports

[11] *Meta Reports Fourth Quarter and Full Year 2021 Results*, Meta Investor Relations, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited July 19, 2023).

entities and website owners, like Defendant, to employ Facebook's "Business Tools" in order to collect, categorize, target, and promote products and services to individuals who visit the owner's website.

55. 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 user activity on those platforms.

56. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, as well as, for example, webpage's Universal Resource Locator ("URL"), metadata, and button clicks.[12] Advertisers, such as Defendant, can track other user actions and can customize their own tracking parameters by building a "custom event."[13]

57. One such Business Tool is the Pixel which "tracks the people and type of actions they take" on a given webpage.[14] Upon a user visiting a webpage that hosts the Pixel, their interactions with the host webpage are surreptitiously replicated, then transmitted to Facebook's servers. This journey occurs seamlessly, starting from the user's browser and ending at Facebook's server.

58. Notably, this transmission exclusively takes place on webpages that host the

[12] *Specifications for Meta Pixel Standard Events*, Meta Business Help Center, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited July 19, 2023); *see also Best Practices for Meta Pixel Setup,* Meta Business Help Center, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited July 19, 2023); *App Events API*, Meta for Developers, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited July 19, 2023, 2022).

[13] *About Standard and Custom Website Events*, Meta Business Help Center, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited July 19, 2023); *see also App Events API*, Meta for Developers, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited July 19, 2023).

[14] *Supra* Fn. 4

Facebook Pixel. Consequently, Plaintiff's and Class Members' Private Information would not have been shared with Facebook through the Pixel had Defendant chosen not to install the software on its Website.

59. Similarly, Plaintiff's and Class Members' Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decision to install and implement that tool as well.

60. Through its installation and utilization of both tools, Defendant intercepted and transmitted Plaintiff's and Class Members' communications with Facebook via the Pixel. Additionally, Defendant caused a second improper disclosure of Private Information through its use of Conversions API.

61. As detailed below, Defendant's source code initiates these illegal transmissions simultaneously with communications made through specific webpages.

Defendant's Method of Transmitting Plaintiff's and Class Members' Private Information via the Tracking Pixel and/or Conversions API i.e., the Interplay Between HTTP Requests and Responses, Source Code, and the Pixel

62. Web browsers are software applications that enable consumers to browse the web, and view and exchange electronic information and communications over the Internet. Each "client device," (such as a computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, or Microsoft's Edge browser).

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

64. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS

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

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court).
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data from 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.[15]

65. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as "Book an Appointment" page). The HTTP Response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's

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

Website.

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

67. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that.

68. The Pixel acts like a wiretap. When patients visit Defendant's website via an HTTP Request to Overlake's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. In essence, Defendant is handing its patients a "tapped phone." Once the webpage is loaded onto the patients' browser, a covert software-based wiretap is silently activated, waiting for private communications on the webpage to initiate the interception. These intercepted communications, intended solely for Defendant, are then transmitted to third parties, including Facebook and Google.

69. Third parties, such as Facebook and Google, implant third-party cookies into the web browser of users who are logged into their services on the same device. These cookies serve the purpose of uniquely identifying the user and are included with each intercepted communication. By doing so, the third-party can accurately identify the patient associated with interception Personal Information.

70. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Personal Information, like Facebook, implement workarounds that even savvy users cannot evade.

Facebook's workaround is called Conversions API. Conversions API is an effective workaround because it does the transmission from their own servers and does not rely on the user's web browsers. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Hence, the interactions between patients and Defendant, which are essential for using Defendant's Website, are effectively received and stored on Defendant's server. Subsequently, the Conversions API directly retrieves and transmits the Private Information present in those interactions from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

71. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[16] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

72. The third parties to whom a website transmits data via pixels and similar methods do not contribute significant content pertaining to the user's communications. Rather, these third parties are commonly engaged to monitor user data and communications for the website owner's marketing objectives, primarily aimed at enhancing profitability.

73. Thus, without any knowledge, authorization, or action by a user, a website owner

[16] *See Best Practices For Conversions Api*, Meta Business Help Center, https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited July 19, 2023).

like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly transmit the users' communications to third parties.

74. In this case, Defendant employed the Tracking Pixel and Conversions API tools to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook.

75. For example, when a patient visits www.overlakehospital.org and selects the "Book an Appointment" 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 particular webpage. As depicted below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses. Additionally, it is to be noted that upon clicking the "Book an Appointment" button, patients are re-directed to a separate page with a different HTTP address: overlakehospital.org/visit/virtual-care.

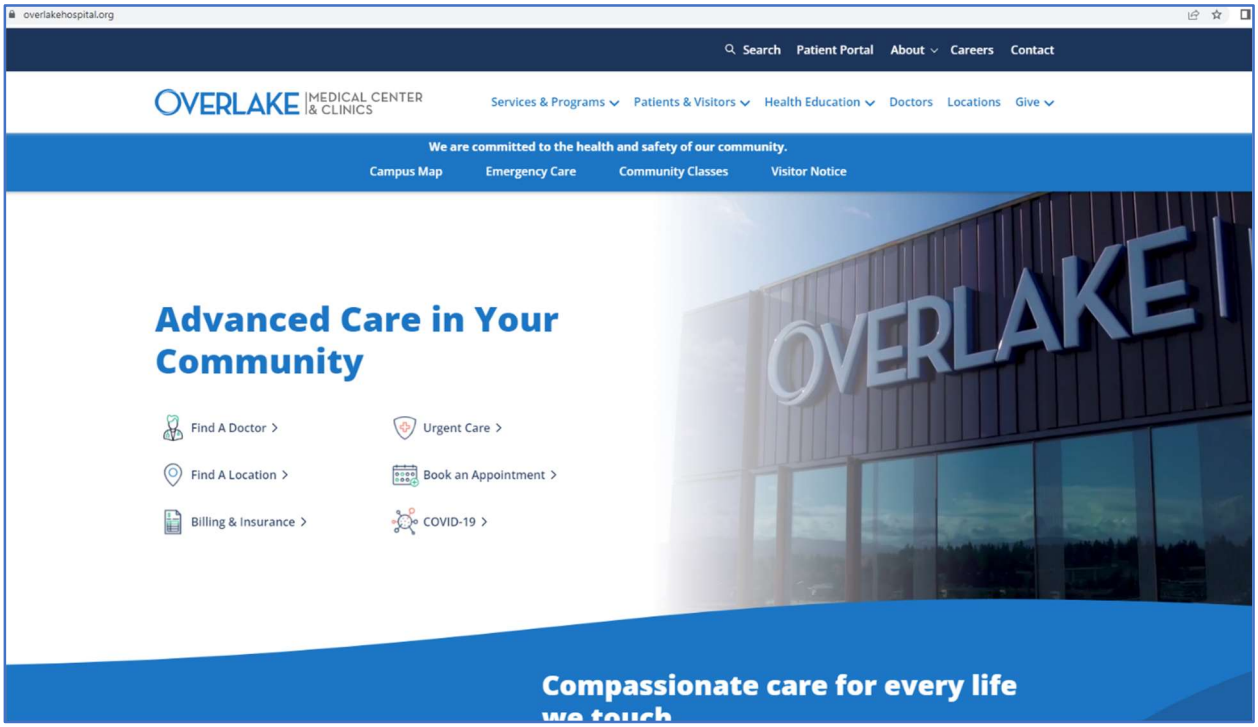


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting overlakehealth.org *(last accessed 18 July 2023).*

76. The Facebook Tracking Pixel is embedded in Defendant's Source Code contained in its HTTP Response. The Pixel, programmed to automatically track and transmit the patient's communications with Defendant's Website to Facebook, 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.[17]

77. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

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

79. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, including, but not limited to, button clicks and selections, and text typed into search bar including conditions, symptoms, and treatments, third parties like Facebook receive the information.

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

80. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API ("First Party cookies") on its Website and servers to secretly track patients

[17] 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.

by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.[18]

81. Defendant's Pixel has its own unique identifier (represented as id=712682029240809), which can be used to identify which of Defendant's webpages contain the Pixel.

82. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.[19] However, Defendant's Website do not rely on the Pixel in order to function.

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

84. Plaintiff and Class Members were not informed that their Private Information would be shared with Facebook when they communicated it to Defendant, primarily due to Defendant's failure to disclose this fact, among other reasons.

85. Plaintiff and Class Members never consented, agreed, or otherwise permitted Defendant to disclose their Private Information to Facebook. Furthermore, they did not have any intention for Facebook to be involved in their communications with Defendant, which often contained highly sensitive and confidential information.

86. Defendant's Pixel and First Party cookies sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (1) health conditions; (2) desired medical treatment or therapies; and (3) phrases and search queries (such as searches for symptoms, treatment options, or types of providers).

---

[18] *Id.*

[19] *Id.*

87. 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.[20]

88. A user's FID is associated with their personal Facebook profile, which typically includes various demographic and personal information about the user. This information can encompass details such as location, photos, personal interests, employment history, relationship status, and other relevant particulars. 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.

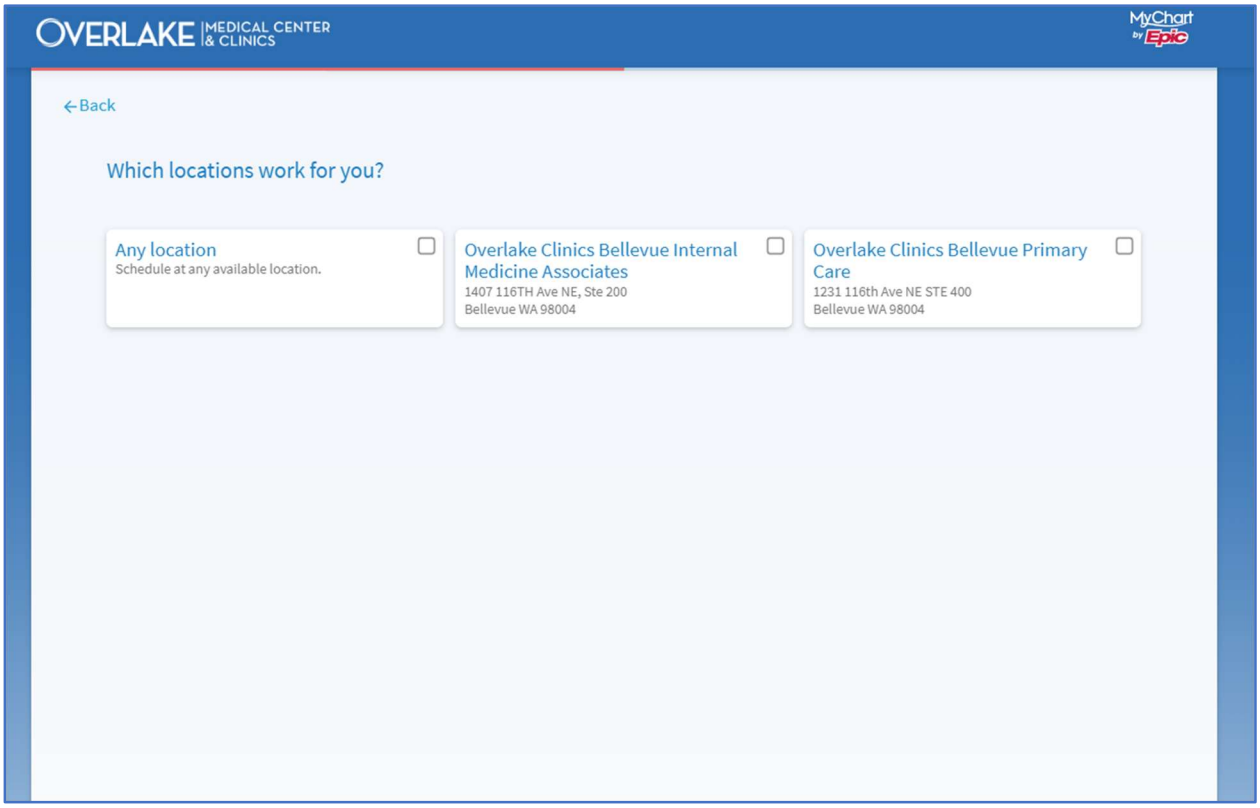
89. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel and First Party cookies) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (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.

Defendant's Pixel Disseminates Patient Information via Its Website

90. An example illustrates the point. If a patient uses the Website to schedule an appointment with an Overlake hospital, Defendant's Website directs them to communicate Private

[20] Defendant's Website track and transmit 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.

Information, including the type of medicine being sought out, the type of appointment being scheduled, and the desired location. Unbeknownst to the patient, each and every communication is sent to Facebook via Defendant's Pixel, including the buttons clicked and the filters they select.

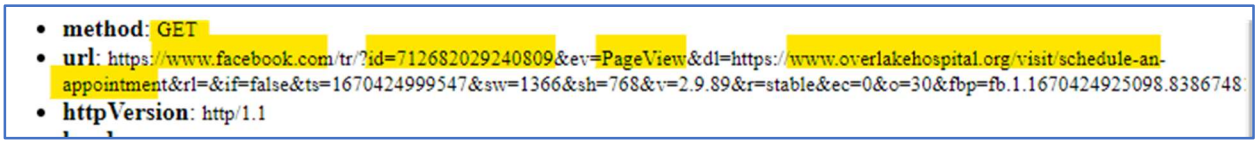


91. In the example above, the user is being prompted to select the Overlake hospital of choice, usually one that is easily accessible to the patient's current location.

92. Next, the user selects the most convenient or preferred location, or has the option to "select all."

93. Unbeknownst to ordinary patients, this particular webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant's Pixel.

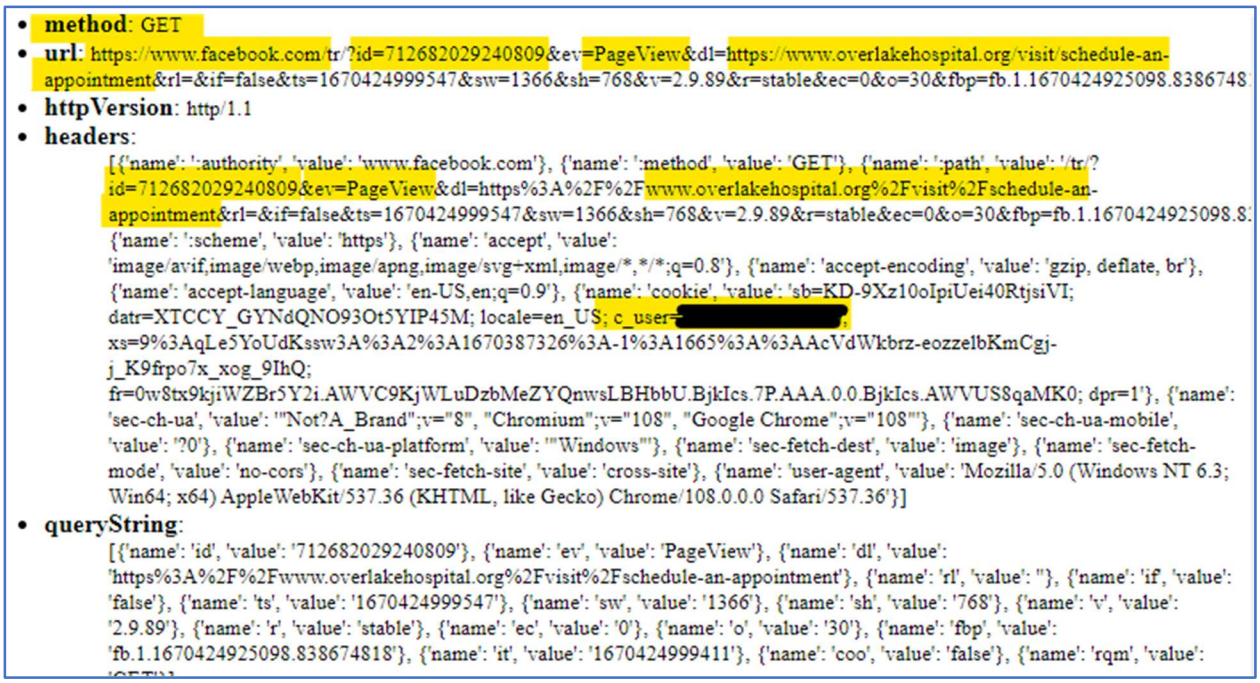
94. Thus, without alerting the user, Defendant's Pixel sends the communications the user made via the webpage to Facebook, and the images below confirm that the communications Defendant sends to Facebook contain the user's Private Information.


- **method**: GET
- **url**: https://www.facebook.com/tr/?id=712682029240809&ev=PageView&dl=https://www.overlakehospital.org/visit/schedule-an-appointment&rl=&if=false&ts=1670424999547&sw=1366&sh=768&v=2.9.89&r=stable&ec=0&o=30&fbp=fb.1.1670424925098.8386748
- **httpVersion**: http/1.1

95. The URL contains, "id=712682029240809" refers to Defendant's Pixel ID and confirms that Defendant has downloaded the Pixel into its Source Code for this particular webpage.

96. On the same line of text, "ev= PageView," identifies and categorizes which actions the user took on the webpage ("ev=" is an abbreviation for event, and "PageView" is the type of event). Thus, this identifies the user as having viewed the "Schedule an Appointment" page on the Overlake Hospital website.

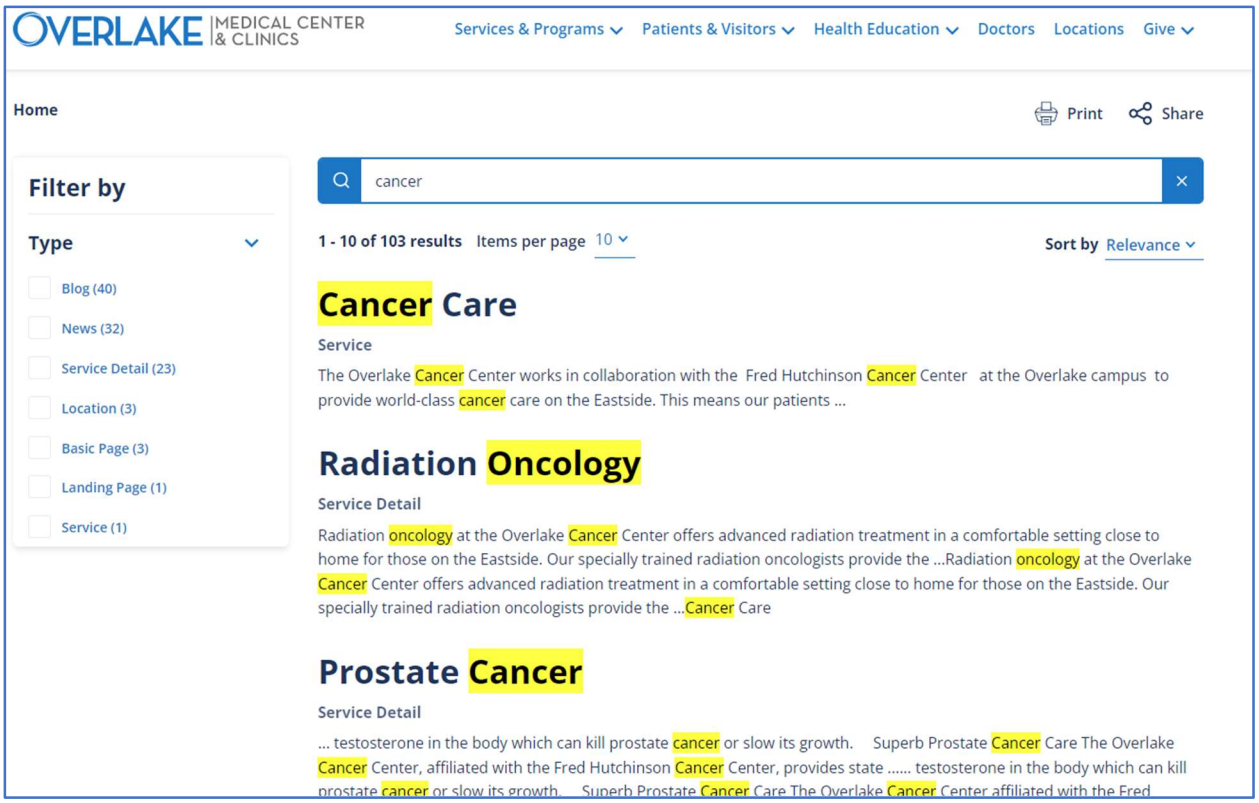
97. Finally, the highlighted text ("GET") demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID (c_user ID), thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.



98. The image demonstrates that the user's Facebook ID (highlighted as "c_user=" in the image above) was sent alongside the other data. [21]

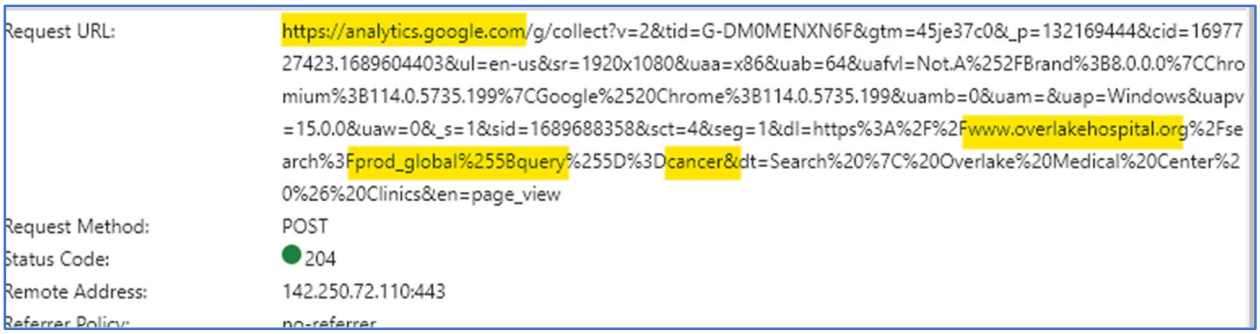
99. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant is using additional tracking pixels and tools to transmit its patients' Private Information to additional third parties. For example, the image below indicates that Defendant is also sending its patients' protected health information to Google via Google Tag Manager., and 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 "Cancer" into the search bar.

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



100. Resultantly, that exact phrase is sent to Google. This is simply unacceptable, and there is no legitimate reason for sending this information to Google.

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



102. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook or Google alongside their personally identifiable information. Several different methods allow marketers and third-parties to identify individual website users, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

103. Defendant does not disclose that the Pixel, First Party cookies, Google Tag Manager, or any other tracking tools embedded in the Website's source code tracks, 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's and Class Members' private communications to Facebook or Google.

Defendant's Conduct Violates its Own Privacy Policies and Promises

104. Defendant's Website contains both a page dedicated to the "Notice of Privacy Practices"[22] as well as a link to Defendant's "Online Privacy Notice."[23]

105. For instance, the Notice of Privacy Practices assures Defendant's patients from the start that:

> Each time you visit a hospital, physician, or other health care provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment and a plan for future care or treatment. This information is often referred to as your health or medical record. We understand

[22] https://www.overlakehospital.org/notice-of-privacy-practices (last visited July 19, 2023).
[23] https://www.overlakehospital.org/online-privacy-notice (last visited July 19, 2023).

> that medical information about you and health is personal and we are committed to protecting medical information about you.[24]

106. Defendant's Online Privacy Notice further provides,

> Any information submitted by users of the Sites is for the exclusive use of Overlake Medical Center and Clinics as well as our contractors that are involved in the operation of Overlake Medical Center and Clinics' activities and website operations. Overlake Medical Center and Clinics is the sole owner of the information collected on the Sites. We only have access to information you voluntarily give us via email, signup forms, contact forms, registration forms, or other direct contact from you. We will not sell or license this information to any third parties. We will not share your information with any third party outside of our organization unless the third party provides services on our behalf (such as email newsletters or class registration) or if it is required by law (such as to comply with a subpoena or legal process).[25]

107. Furthermore, Defendant's Notice of Privacy Practices purports to enumerate "How Will We Use and Disclose Your Medical Information." None of the enumerated uses in Defendant's Privacy Statement cover its conduct of surreptitiously collecting Private Information and disclosing it to third parties for marketing purposes.[26]

108. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shares Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

Defendant Violated HIPAA Standards

109. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a

[24] *Notice of Privacy Practices*, Overlake Medical Center & Clinics (effective March 1, 2021), https://www.overlakehospital.org/notice-of-privacy-practices (last visited July 19, 2023).
[25] *Online Privacy Notice*, Overlake Medical Center & Clinics (effective December 18, 2018), https://www.overlakehospital.org/online-privacy-notice (last visited July 19, 2023).
[26] *Supra* Fn. 24

patient for marketing purposes without the patients' express written authorization.[27]

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

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

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[28]

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

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[29]

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

[27] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[28] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited July 19, 2023)
[29] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited July 19, 2023)

technologies").[30]

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

115. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Facebook Pixel.

Defendant Violated Industry Standards

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

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

118. AMA Code of Ethics Opinion 3.1.1 provides:

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

119. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

[30] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited July 19, 2023).

120. 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.

Plaintiff's and Class Members' Expectation of Privacy

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

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

IP Addresses are Personally Identifiable Information

123. On information and belief, through the use of the Facebook Pixel on the Defendant's Website, Defendant also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' Computer IP addresses.

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

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

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

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

128. Google also tracks IP addresses associated with Internet users.

129. Facebook, Google, and other third-party marketing companies track IP addresses

for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

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

a. 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).

b. 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).

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

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

132. The sole purpose of the use of the Facebook Pixel on Defendant's Website was marketing and profits.

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

134. 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.

135. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby

benefitting Defendant.

TOLLING

136. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that her Private Information was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

137. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

138. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent as a result of using Defendant's Website (the "National Class").**

139. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

140. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

141. Numerosity, Fed R. Civ. P. 23(a)(1). The Nationwide Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose Private Information may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

142. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact

common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing the Private Information of Plaintiff and Class Members to Facebook and/or additional third parties.

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

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

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

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

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

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Private Information.

143. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

144. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

145. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

146. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

147. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

149. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

150. Unless a Class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

151. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

152. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

153. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

COUNT I
Negligence
(On Behalf of Plaintiff and the National Class)

154. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

155. Defendant required patients and users, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of interacting with Defendant's website and seeking to obtain medical care and treatment.

156. By collecting this information from Plaintiff and Class Members in the course of its business, Defendant owed a duty of care to use reasonable means to secure and safeguard said information. This duty of care included a responsibility not only to maintain secure servers and data security protocols, but also to keep information collected confidential. This duty was heightened by the sensitive nature of the Private Information collected from Plaintiff and Class Members.

157. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

158. Defendant owed a duty of reasonable care to Plaintiff and Class Members to maintain the confidentiality of Plaintiff's and Class Members' sensitive Private Information.

159. Defendant's duty of care to exercise reasonable care in protecting the confidentiality of Private Information that it is entrusted with arose from ordinary principles of foreseeability, industry standards, and the special relationship that existed between Defendant and its patients. Defendant was in a superior position to ensure that its systems were sufficient and that its employees and agents were adequately trained to protect against the foreseeable risk of harm to Class Members from the unauthorized disclosure of their Private Information.

160. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

161. Defendant also had a duty to safeguard Private Information under the Arizona Consumer Fraud Act ("ACFA"), A.R.S. §§ 44-1521, *et seq.*, which prohibits "deceptive or unfair" acts or practices. A.R.S. §§ 44-1522(A). In construing the ACFA, the Court should "use as a guide interpretations given by the federal trade commission and the federal courts to 15 United States Code §§ 45, 52 and 55(a)(1)." A.R.S. § 44-1522(C).

162. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Engaging the use of the Facebook Pixel and Conversions API when it knew or should have known that this would track and record the interactions of Plaintiff and Class Members with Defendant's Website;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

c. Failing to adequately program the Pixel and Conversions API to protect the anonymity of Plaintiff and Class Members;

d. Failing to prevent foreseeable access to Class Members' PHI and PII;

e. Negligently and/or recklessly failing to understand or detect the disclosure of Plaintiff's and Class Members' PHI and PII to third parties; and

163. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PHI and PII would result in injury to Class Members. Furthermore, the tracking, recording, and transmission of patients' personal information was foreseeable, as this is what the Pixel is designed to do, and it is widely understood in Defendant's field that third parties often seek to collect data when providing business services, and Defendant's field contains a large quantity of sensitive, confidential information inaccessible from other industries.

164. Plaintiff and Class Members are entitled to nominal, punitive, compensatory and/or consequential damages suffered as a result of the Data Breach.

165. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) immediately stop the use of the Facebook Pixel and Conversions API and (ii) submit to future annual audits of its cyber-security, data collection, and third-party business services systems.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiff and the National Class)

166. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

167. The Private Information of Plaintiff and Class Members consists of private and confidential facts and information that was never intended to be shared beyond private communications.

168. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

169. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

170. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information to Facebook, a third-party social media and marketing giant, is highly offensive to a reasonable person.

171. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

172. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

173. Defendant failed to protect Plaintiff's and Class Members' Private Information and

acted knowingly when it installed the Pixel onto its Website because the purpose of the Pixel is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

174. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

175. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiff and the Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

176. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

177. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

178. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

179. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information and to adhere to its common law, contractual, statutory, and

regulatory duties.

COUNT III
Breach of Confidence
(On behalf of Plaintiff and the National Class)

180. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

181. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

182. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website, which were further buttressed by Defendant's express promises in its privacy policy.

183. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Pixel and Conversions API to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

184. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

185. The third-party recipients included, but were not limited to, Facebook.

186. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

187. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

a. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. General damages for invasion of their rights in an amount to be determined by a jury;

d. Nominal damages for each independent violation;

e. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;

f. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

g. Defendant's actions diminished the value of Plaintiff's and Class Members' Personal Information; and

h. Defendant's actions violated the property rights Plaintiff and Class members have in their Personal Information.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the National Class)

188. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

189. When Plaintiff and Class Members provided their user data to Defendant in

exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

190. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

191. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

192. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to a third party, *i.e.*, Facebook.

193. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

194. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V
Unjust Enrichment
(On behalf of Plaintiff and the National Class)

195. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein, with the exception that this claim is brought in the alternative to breach of contract.

196. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

197. Plaintiff and Class Members conferred a benefit upon Defendant in the form of

Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

198. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

199. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Minnesota and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

200. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VI
Violations of Electronic Communications Privacy Act ("ECPA")
18 U.S.C. § 2511(1) *et seq*.
Unauthorized Interception, Use, and Disclosure
(On Behalf of Plaintiff and the National Class)

201. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

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

203. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter

119.

204. The transmissions of Plaintiff's Private Information to Defendant via Defendant' Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

205. The transmissions of Plaintiff's Private Information to the Webpage and Third Party medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

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

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

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

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

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

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

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

211. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook.

212. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff's and Class Members' regarding Private Information, treatment, medication, and scheduling.

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

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

215. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

216. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel and Conversions API to track and utilize Plaintiff's and Class Members' Private Information for financial gain.

217. Defendant was not acting under color of law to intercept Plaintiff and the Class Member's wire or electronic communication.

218. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

219. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

220. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of Mo. Rev. Stat. § 407.010 *et seq.*

COUNT VII
Violations of the Electronic Communications Privacy Act
Unauthorized Divulgence by Electronic Communications Service
18 U.S.C. § 2511(3)(a)
(On Behalf of Plaintiff and the National Class)

221. Plaintiff repeats and re-alleges each and every allegation contained in the

Complaint as if fully set forth herein.

222. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

223. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

224. Defendant's Website is an electronic communication services that give users the ability to send or receive electronic communications to Defendant and, upon information and belief, medical professionals who contract with, but are not employed by Defendant. In the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiff's and Class Members' Private Information.

225. Defendant's Website is a conduit of communication between Plaintiff and Class Members and their respective medical providers, including third parties who are not employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

226. Defendant's Website is also a conduit between Plaintiff and Class Members and the Webpage.

227. **Intentional Divulgence**. Defendant intentionally designed the Pixel and Conversions API tracking and was or should have been aware that it could divulge Plaintiff's and Class Members' Private Information.

228. **While in Transmission**. Upon information and belief, Defendant's divulgence of

the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Website and/or MyChart Portal, to which they directed their communications.

229. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiff's and Class Members' communications to Facebook without Plaintiff's and Class Members' consent and/or authorization.

230. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication":

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

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

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

U.S.C. § 2511(3)(b).

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

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic

> communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

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

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

234. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel and Conversions API code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiff and Class Members were exchanging information.

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

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

237. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may

assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VIII
Violations of Title II of the Electronic Communications Privacy Act
Stored Communications
18 U.S.C. § 2702, *et seq*.
(On Behalf of Plaintiff and the National Class)

238. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

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

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

241. Defendant's Website is a conduit of communication between Plaintiff and Class Members and their respective medical providers, including third parties who are not employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

242. Defendant's Website is also a conduit between Plaintiff and Class Members and the Webpage.

243. Defendant intentionally procures and embeds various pieces of Plaintiff's Private Information through the Pixel Code and Conversions API used on Defendant's Website, which qualifies as an Electronic Communication Service.

244. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary,

intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

245. Defendant stores the content of Plaintiff's and Class Members' communications with Defendant's Website and files associated with it via the Tracking Pixel or Conversions API. As explained above, via Conversions API, Defendant stores Plaintiff's and Class Members' Private Information on its servers and then transmit that Private Information to Facebook.

246. By way of another example, Defendant stores data pertaining to scheduling appointments, IP addresses, and communications regarding medical treatment.

247. When Plaintiff or Class Member communicates with the Website, the content of that communication is immediately placed into storage.

248. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through its Website' source code.

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

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

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

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

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

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

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

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

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

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

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

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

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

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

253. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. §

2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

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

255. Defendant's divulgence of the contents of user communications on Defendant's Website and/or MyChart Portal was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiff and Class Members were exchanging information.

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

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

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

COUNT IX
Violations of the Computer Fraud and Abuse Act (CFAA)
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiff and the National Class)

259. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

260. The Plaintiff's and the Class's computers and/or mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

261. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

262. For example, Defendant exceeded its unauthorized access because Defendant accessed Plaintiff's and Class Members' Private Information under false pretenses, *i.e.*, Defendant did not disclose it was transmitting Private Information to Facebook.

263. Moreover, Defendant exceeded its unauthorized access because Defendant violated its *own* Privacy Policies in disclosing Plaintiff's and Class Members' Private Information to Facebook.

264. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class's private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications") which were never intended for public consumption.

265. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiff and the Class being made

available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

266. Accordingly, Plaintiff and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

COUNT X
Violations of the Washington Consumer Protection Act,
Wash. Rev. Code Ann. §§ 19.86.020, *et seq*.
(On Behalf of Plaintiff and the Washington Subclass)

267. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

268. Defendant is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

269. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

270. Defendant engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to secure and protect Plaintiff's and Washington Subclass Members' Private Information in a confidential manner;

b. Failing to inform Plaintiff and Washington Subclass Members of Defendant's use of the Facebook Pixel and Conversions API tools;

c. Failing to inform Plaintiff and Washington Subclass Members of the extent of Defendant's data harvesting, tracking, and disclosure practices;

d. Failing to comply with common law and statutory duties pertaining to the security

and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Washington Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

g. Misrepresenting that certain sensitive Private Information would not be disclosed to third parties;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington Subclass Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

271. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's ability and intentions to

protect the confidential and sensitive Private Information of Plaintiff and Washington Subclass Members communicated for the purpose of medical treatment.

272. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Washington Subclass Members, that their Private Information would be held in a secure and confidential manner, rather than deliberately disclosed to third parties.

273. Defendant acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights.

274. Defendant's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010, *et seq.*. Alternatively, Defendant's conduct is injurious to the public interest because it has injured Plaintiff and Washington Subclass Members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons. Further, its conduct affected the public interest, including the thousands of Washington Residents impacted by Defendant's use of the Pixel and Conversions API tools.

275. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including the damage to their privacy and property interests in their Private Information.

276. Plaintiff and Washington Subclass members seek all monetary and non-monetary

relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

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

D. For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

DATE: August 3, 2023 Respectfully Submitted,

/s/ Andrew A. Lemmon
Andrew A. Lemmon (#53034)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
16212 Reitan Road NE
Bainbridge Island, WA 98110
T: (985) 783-6789
alemmon@milberg.com

Gary M. Klinger*
Alexandra M. Honeycutt*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Terence R. Coates*
Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Bryan L. Bleichner
Philip J. Krzeski
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Joseph M. Lyon*
The Lyon Law Firm
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiff and the Putative Class

* *pro hac vice* forthcoming

ClassAction.org