UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

J.C., *on behalf of herself and all others similarly situated,* Plaintiff, v. Catholic Health System, Inc. Defendant.	Civil Index No. 1:23-cv-00796-JLS **JURY TRIAL DEMANDED**

AMENDED CLASS ACTION COMPLAINT

1. Plaintiff J.C.,[1] at all times relevant herein, has been a patient of Catholic Health System, Inc. ("CHS" or "Defendant"), and brings this class action against Defendant in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, her counsels' investigation, and upon information and belief as to all other matters, as follows:

2. Plaintiff brings this case to address Defendant's unlawful 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") and Google, Inc. ("Google") without consent through the use of pixel tracking software that is embedded in Defendant's website.

1 Plaintiff brings this action anonymously out of a desire to protect her personal health information under the Health Insurance Portability and Accountability Act of 1996 and New York law.

3. Defendant owns and controls https://www.chsbuffalo.org/ ("Defendant's Website" or the "Website"), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more. Included within Defendant's Website is the MyChart Patient Portal, which Defendant encourages patients to sign up for and use so that they can more conveniently book appointments and schedule visits, review their health records and test results, pay bills, communicate with service providers, request prescription refills, and complete medical forms virtually and remotely.

4. Plaintiff and other Class Members who used Defendant's Website understandably thought they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiff and Class Members, however, Defendant had installed tracking technologies ("Tracking Tools" or "Tracking Technologies") onto its Website, including the login page for the MyChart Portal. These Tracking Tools, including Facebook's Tracking Pixel (the "Facebook Pixel" or "Pixel") and Google, Inc.'s Google Analytics tool or Google Tag Manager, track and collect communications with the Defendant via the Website and surreptitiously force the user's web browser to send those communications to undisclosed third parties, such as Facebook or Google.

Tracking Pixels

5. 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").[2]

[2] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites

6. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[3] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

7. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

8. When a website user visits a webpage containing Pixels, their device is commandeered, and their communications are surreptitiously duplicated and transmitted to third parties. Stated differently, Defendant's Website and Pixel purposely altered patients' web browsers, forcing them to duplicate and redirect communications to third-party web servers.

9. The information sent to third parties included the Private Information that Plaintiff and Class Members submitted to Defendant's Website related to their past, present, or future health conditions, including, for example, the type and date of a medical appointment and physician. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care and the type of medical care being sought. This disclosure would 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, or addiction.

---

about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited April 18, 2023).

[3] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited April 18, 2023).

Defendant's Website Employs the Facebook Pixel

10. Simply put, by installing the Facebook Pixel into its Website, Defendant effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled their browsers to disclose their communications with Defendant to Facebook.

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

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

13. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad

---

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

[5] https://revealbot.com/blog/facebook-conversions-api/ (last visited Jan. 24, 2023).

[6] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited Jan. 27, 2023).

[7] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 28, 2023).

blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

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

15. The information disclosed in this way by Defendant allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI.

16. Included within Defendant's Website is the MyChart Patient Portal, which Defendant encourages patients to sign up for and use so that they can more conveniently book appointments and schedule visits, review their health records and test results, pay bills, communicate with service providers, request prescription refills, and complete medical forms virtually and remotely.[8]

17. The MyChart Patient Portal is a software system designed and licensed to CHS by Epic Software Systems ("Epic"). Epic is a privately owned health care software company that provides services to 250 million patients, including two thirds of the U.S. population.

[8] https://www.chsbuffalo.org/mychart (last visited June 18, 2023).

18. Epic's MyChart software system was designed to permit licensees – such as CHS – to deploy "custom analytics scripts" within MyChart, including, for example, the Facebook Pixel or Google Analytics, all for the transmission of personally identifiable information, including medical and health-related information, and communications to third parties.[9]

19. As a result, hospitals that use analytics tools like the Facebook Pixel or Google Analytics on their websites may also have those tools embedded on the MyChart login page or even inside the MyChart patient portal.

20. Patients can log into MyChart through the Website or through a companion app ("MyChart App").

21. Through the Website, which includes the MyChart Patient Portal, and the MyChart App (collectively "Digital Platform"), CHS advertises to its prospective and current patients that its online functionality is a secure and private means of interacting with CHS and its health providers.

22. Plaintiff is unable to determine whether the Pixel was embedded on the MyChart login page or inside the MyChart portal. However, given Defendant's use of the Facebook Pixel on other pages of the Website (including that the Facebook Pixel operating on the Website shows is present on the MyChart login page, that the Pixel transmits the exact doctor that a patient is seeking, and that the Pixel transmits exact phrases a user types into free form text boxes on the Website), Plaintiff reasonably believes and therefore avers that Defendant used the Facebook Pixel to track information on its entire Website, including MyChart.

---

[9] *See* Feathers, T., *Pixel Hunt: Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022) (available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-isreceiving-sensitive-medical-information-from-hospital-websites).

The Department of Health and Human Services Has Warned About Use of the Pixel by Healthcare Providers

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

24. Healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, only in a limited way, to perform analysis on data key to operations:

> To be sure, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[10]

25. In addition, New York law provides patient rights, including that "[e]very patient shall have the right to have privacy in treatment and in caring for personal needs, confidentiality

[10] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited May 10, 2023) (emphasis added).

in the treatment of personal and medical records, and security in storing personal possessions. N.Y. Pub. Health Law § 2803(3)(f).

26. New York law also provides that "[u]nless the patient waives the privilege, a person authorized to practice medicine, registered professional nursing, licensed practical nursing, dentistry, podiatry or chiropractic shall not be allowed to disclose any information which he acquired in attending a patient in a professional capacity, and which was necessary to enable him to act in that capacity." N.Y. C.P.L.R. 4504.

27. The Office for Civil Rights (OCR) at 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 technologies").[11] 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." In other words, HHS has expressly stated that entities like Defendant that implement the Facebook Pixel have violated HIPAA Rules.

28. The HHS Bulletin further warns that:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks

[11] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Feb. 20, 2023).

> medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [12]

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

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

31. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, inter alia,: (i) failing to adequately review its marketing programs and web-based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain

---

[12] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dep't of Health and Hum. Servs. (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited June 18, 2023).

the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

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

33. Plaintiff seeks to remedy these harms and brings causes of action for (1) breach of fiduciary duty/confidentiality; (2) violation of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (3) invasion of privacy; (4) breach of implied contract; (5) unjust enrichment; (6) negligence; and (7) violation of the New York Consumer Law for Deceptive Acts and Practices Gen. Bus. Law § 349.

PARTIES

34. Plaintiff J.C. is a natural person and citizen of New York where she intends to remain.

35. Defendant CHS is a health care provider incorporated as a nonprofit in the State of New York and headquartered at 144 Genesee Street, Buffalo, New York 14203.

36. CHS is a not-for-profit healthcare organization that provides comprehensive healthcare to "Western New Yorkers across a network of hospitals, primary care centers, and

several other community ministries."[13] CHS is a health network spanning five hospitals, Kenmore Mercy Hospital, Mercy Hospital of Buffalo, Mount St. Mary's Hospital, Sisters of Charity Hospital, St. Joseph Campus, and numerous primary care center, imaging centers and community ministries.[14] In addition, CHS has more than 1,500 physicians and treats over 100 thousand patients a year.[15]

37. 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

38. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of $5,000,000.00, 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.

39. 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.*).

40. 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.

---

[13] *About Us*, Catholic Health, https://www.chsbuffalo.org/about-us (last visited June 18, 2023).

[14] *https://www.chsbuffalo.org/* (last visited June 18, 2023).

[15] *Id.*

41. 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

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

42. Defendant purposely installed the Pixel and Conversions API tools on many of its webpages within its Website and programmed those webpages to surreptitiously share its patients' private and protected communications with Facebook, including communications that contain Plaintiff's and Class Members' PHI and PII.

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

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

1. Facebook's Business Tools and the Pixel

45. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[16]

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

[16] *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 June 23, 2023).

47. 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.

48. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[17] Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[18]

49. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[19] When a user accesses a webpage that is hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

50. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website.

---

[17] *Specifications for Facebook Pixel Standard Events*, META BUSINESS HELP CENTER, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited June 23, 2023); *see Facebook Pixel, Accurate Event Tracking, Advanced*, META FOR DEVELOPERS, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also Best Practices for Facebook Pixel Setup*, META BUSINESS HELP CENTER, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited June 23, 2023); *App Events API*, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited June 23, 2023).

[18] *About Standard and Custom Website Events*, META BUSINESS HELP CENTER, https://www.facebook.com/business/help/964258670337005?id=1205376682832142(last visited June 23, 2023); *see also App Events API*, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited June 23, 2023).

[19] *Retargeting*, FACEBOOK, https://www.facebook.com/business/goals/retargeting.

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

52. By installing and implementing both tools, Defendant caused Plaintiff's and Class Member's communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via Conversions API.

53. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

2. 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

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

55. 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.

56. 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 HTTP 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 when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[20]

57. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as "Find a Doctor" 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 Website.

58. 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.

59. 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. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to CHS'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. Thus, Defendant is in

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

essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

60. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Personal Information intercepted.

61. 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 savvy users cannot evade. Facebook's workaround, for example, 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]." Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

62. 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."[21] 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.

63. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (*i.e.*, to bolster profits).

64. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

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

66. For example, when a patient visits chsbuffalo.org and selects the "Providers" 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.

[21] *See Best Practices for Conversions API*, META BUSINESS HELP CENTER https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited June 23, 2023).

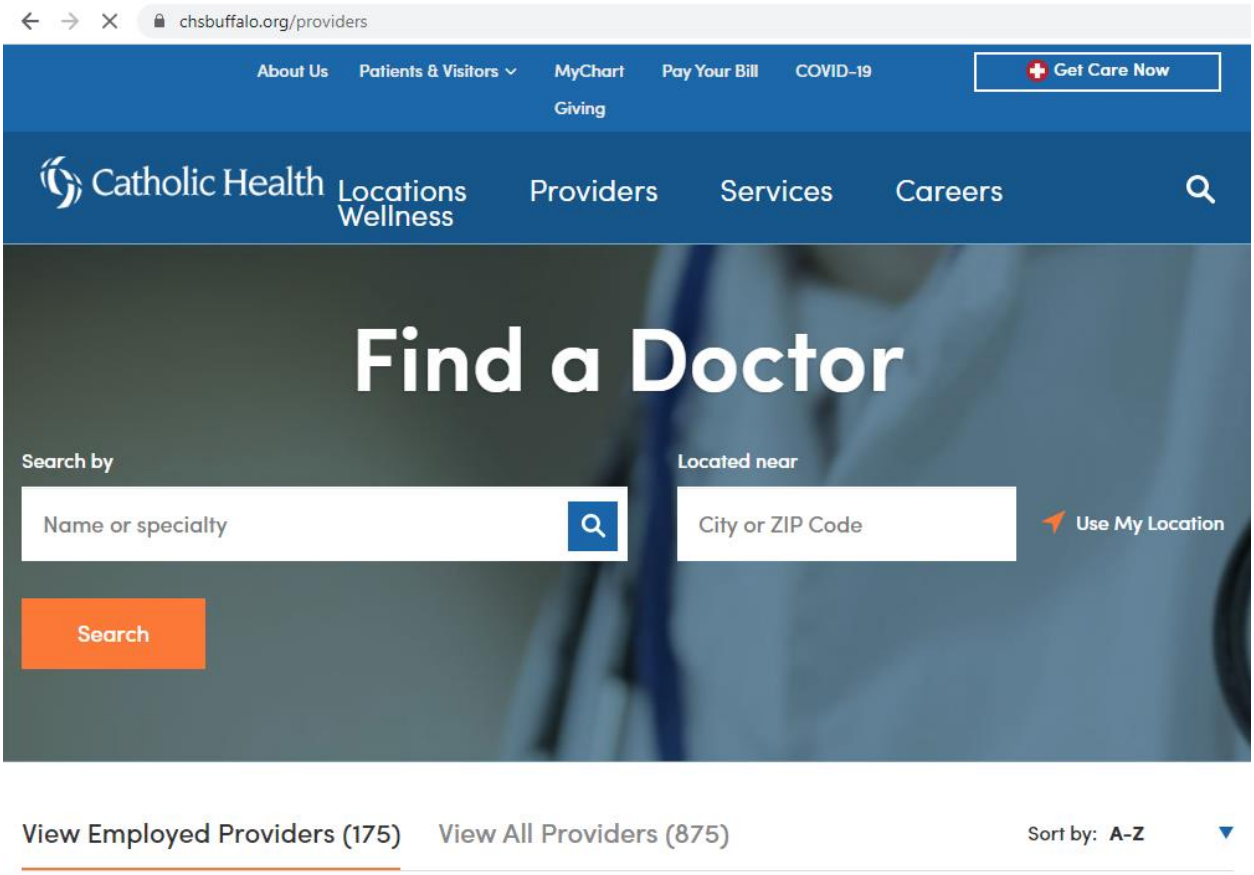


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting https://www.chsbuffalo.org/providers (last accessed June 22, 2023).

67. 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.[22]

[22] 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.

68. 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.

69. 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.

70. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, including, but not limited to, selected treatment locations, physicians, symptoms, medical conditions, zip codes typed into text boxes, text typed into general search boxes, and patient status, that information is transmitted to third parties, including but not limited to, Facebook.

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

71. 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 by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.[23]

72. Defendant's Pixel has its own unique identifier (represented as id= 280161489277215, id=2208812335999737, and id=360850294744926), which can be used to identify which of Defendant's webpages contain the Pixel.

[23] *Id.*

73. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.[24] However, Defendant's Website does not rely on the Pixel in order to function.

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

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

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

77. 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) status as medical patients and navigation to the patient portal; (2) health conditions; (3) desired medical treatment or therapies; (4) desired locations or facilities where treatment was sought; (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers); (6) symptoms connected to a particular health condition and (7) selected physicians.

78. 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

[24] *Id.*

contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.[25]

79. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

80. 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.

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

81. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"[26] and Facebook has built its more-than $300 billion market capitalization on mining and using that 'digital' oil. Thus, the large volumes of personal and sensitive health-related data Defendant provided to Facebook are actively viewed, examined, analyzed, curated, and put to use by the company. Facebook

[25] 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.

[26] https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited Apr. 5, 2023).

acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Facebook offers the Pixel free of charge[27] and the price that Defendant pays for the Pixel is the data that it allows Facebook to collect.

82. Facebook sells advertising space by emphasizing its ability to target users.[28] Facebook is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant).[29] This allows Facebook to make inferences about users beyond what they explicitly disclose, including their "interests," "behavior," and "connections."[30] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[31]

83. Advertisers can also build "Custom Audiences,"[32] which helps them reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[33] With Custom Audiences, advertisers can

---

[27] https://seodigitalgroup.com/facebook-pixel/ (last visited Apr. 18, 2023).

[28] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Apr. 18, 2023).

[29] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Apr. 18, 2023).

[30] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Apr. 18, 2023).

[31] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited April 18, 2023).

[32] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited April 18, 2023).

[33] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited April 18, 2023).

target existing customers directly. They can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[34] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Facebook. This data can be supplied to Facebook by manually uploading contact information for customers or by utilizing Facebook's "Business Tools" like the Pixel and Conversions API.[35]

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

85. Facebook receives over 4 petabytes[36] of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data to augment human effort.[37]

---

[34] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited April 18, 2023).

[35] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited April 18, 2023); Facebook, Create a Website Custom Audience, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited April 18, 2023).

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

[37] https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4 (last visited April 18, 2023). Facebook employees would not be able to view each piece of data individually – millions of them per second – without the aid of technology. Just as a microscope or telescope allows the user to see very small or very distant objects by zooming in, however, Facebook's big data management software allows the company to see all of this data at once by zooming out.

This process is known as "data ingestion" and allows "businesses to manage and make sense of large amounts of data."[38]

86. By using data ingestion tools, Facebook is able to rapidly translate the information it receives from the Pixel in order to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper's Facebook page.[39] This evidences that Facebook views and categorizes data as they are received from the Pixel.

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

> It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place and requires that there is an applicable Privacy Rule permission for disclosure.[40]

2. Defendant's Pixel Disseminates Patient Information Via Its Website

88. An example illustrates the point. If a patient uses the Website to find a Doctor, Defendant's Website directs them to communicate Private Information, including the particular

---

[38] https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/ (last visited April 18, 2023). Facebook uses ODS, Scuba, and Hive to manage its massive data stores. These technologies are not traditional databases; they are specialized databases for big data designed to process data specifically for analysis—"such as [viewing] hidden patterns, correlations, market trends and customer preferences."

[39] https://www.oberlo.com/blog/facebook-pixel (last visited April 18, 2023).

[40] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis in original) (last visited April 18, 2023).

specialty the patient is seeking and the patient's zip code. Unbeknownst to the patient, each and every communication is sent to Facebook via Defendant's Pixel, including the physician the patient selects, the location of that physician, the patient's attempt to call that physician for an appointment, and any text or phrases the patient types into the search bar.

89. In the example below, the user navigated to the "Find a Doctor" page in Defendant's Website:

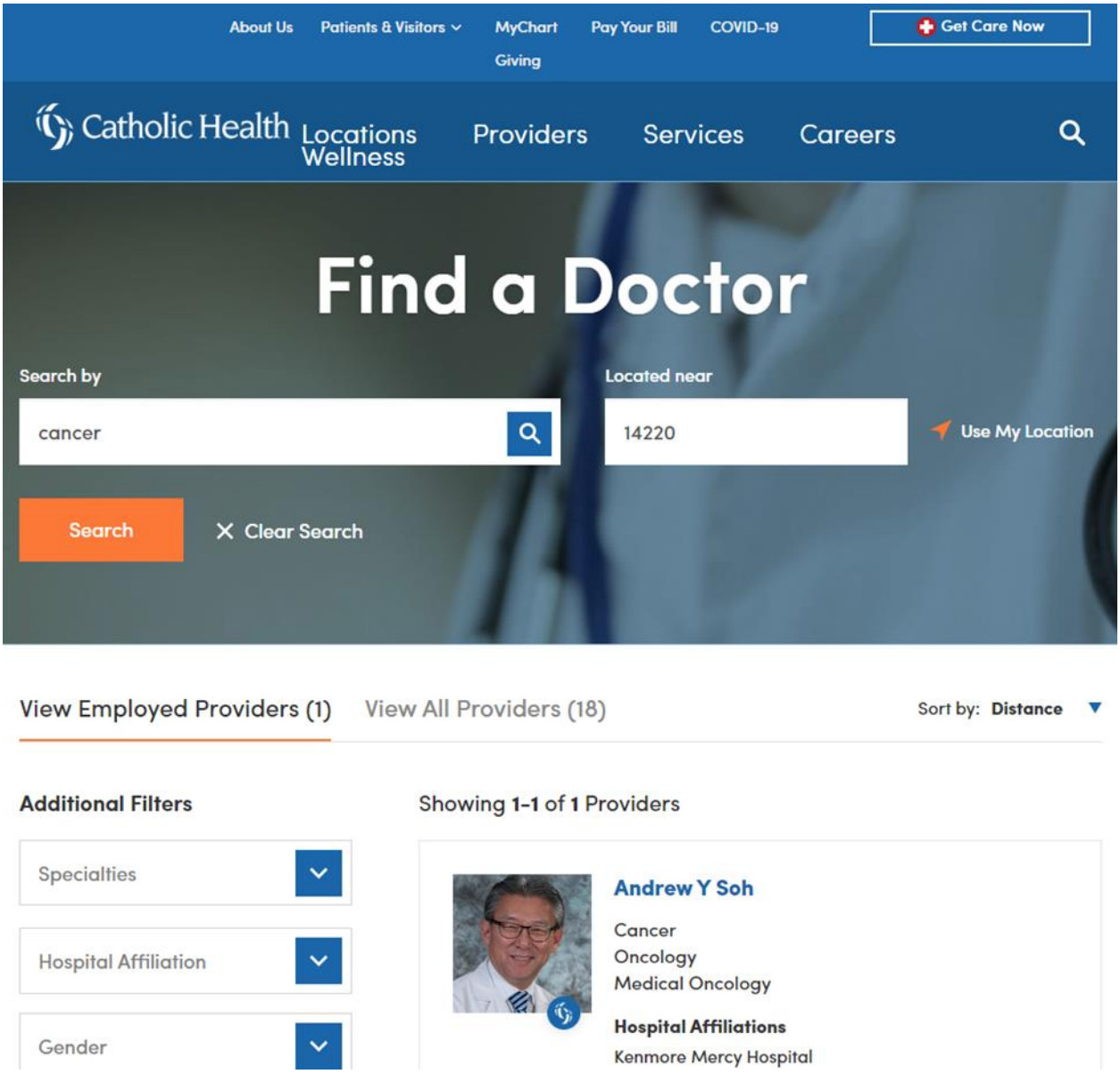


Figure 2. Screenshot taken from chsbuffalo.org as the user searches for a specialist in cancer and communicates information via the search bar and filtering tools.

90. Next, the user was prompted to input the specialty and location, and the user typed the desired specialty and zip code into the respective search boxes.

91. 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. The image below shows the "behind the scenes" portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Pixel sent this particular user's information to Facebook:

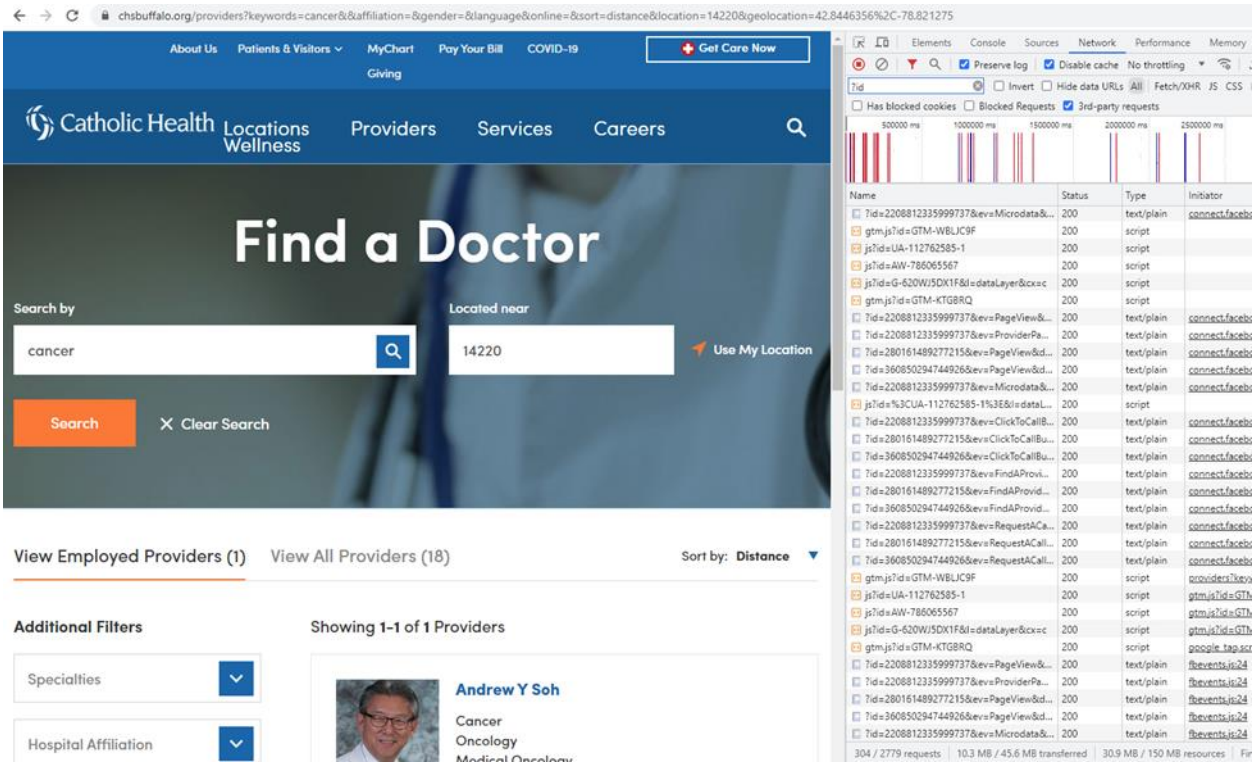


Figure 3. Screenshot taken from chsbuffalo.org which shows the mark-up (user-facing portion of the website) alongside the network traffic. Each entry in the column to the right represents just one instance in which the user's information was transmitted to Facebook via Defendant's pixel.

92. Thus, without alerting the user, Defendant's Pixel sends each and every

communication 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.

93. The following image reveals what information is sent to Facebook when the user takes the next action and selects the physician that fits the searched parameters.

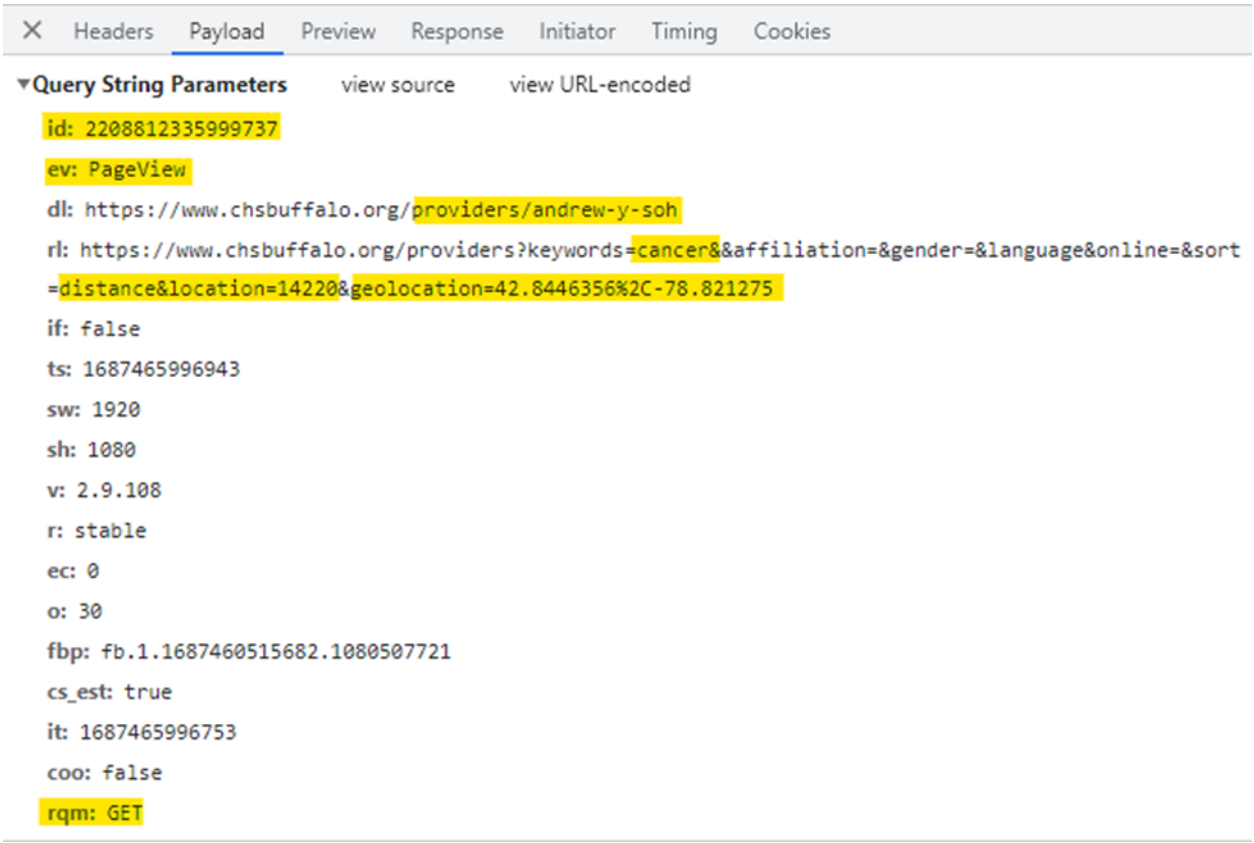


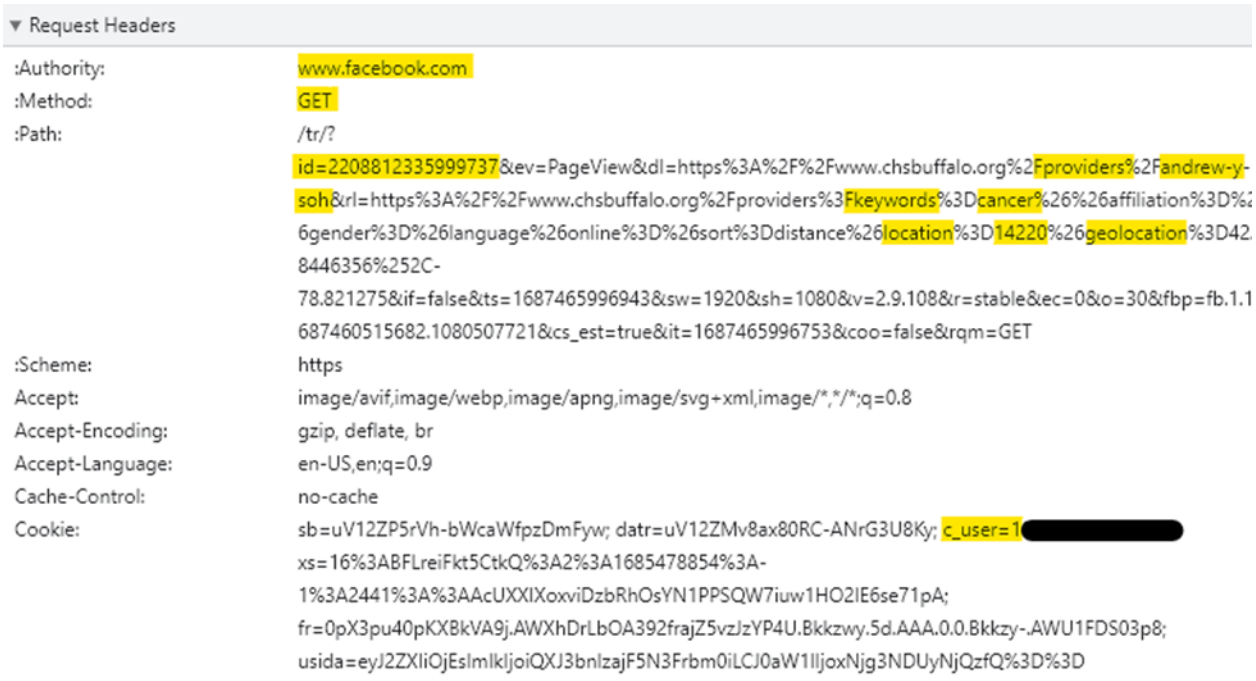
Figure 4. Screenshot taken from user's network traffic report during their physician search.

94. The first line of highlighted text, "id:2208812335999737" refers to Defendant's Pixel ID and confirms that Defendant has downloaded the Pixel into its Source Code for this particular webpage.

95. 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 viewing the particular physician's page.

96. The additional lines of highlighted text show Defendant has disclosed to Facebook that the user: (1) is a patient seeking medical care from Defendant via https://www.chsbuffalo.org/; (2) is seeking treatment for cancer; (3) is seeking treatment from this physician; and (4) is seeking treatment in the particular location, and is even geotagged for the user's specific location.

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.



▼ Request Headers

:Authority:	www.facebook.com
:Method:	GET
:Path:	/tr/? id=2208812335999737&ev=PageView&dl=https%3A%2F%2Fwww.chsbuffalo.org%2Fproviders%2Fandrew-y-soh&rl=https%3A%2F%2Fwww.chsbuffalo.org%2Fproviders%3Fkeywords%3Dcancer%26%26affiliation%3D%26gender%3D%26language%26online%3D%26sort%3Ddistance%26location%3D14220%26geolocation%3D42.8446356%252C-78.821275&if=false&ts=1687465996943&sw=1920&sh=1080&v=2.9.108&r=stable&ec=0&o=30&fbp=fb.1.1687460515682.1080507721&cs_est=true&it=1687465996753&coo=false&rqm=GET
:Scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9
Cache-Control:	no-cache

Cookie:	sb=uV12ZP5rVh-bWcaWfpzDmFyw; datr=uV12ZMv8ax80RC-ANrG3U8Ky; c_user=1[redacted]
	xs=16%3ABFLreiFkt5CtkQ%3A2%3A1685478854%3A-1%3A2441%3A%3AAcUXXIXoxviDzbRhOsYN1PPSQW7iuw1HO2IE6se71pA;
	fr=0pX3pu40pKXBkVA9j.AWXhDrLbOA392frajZ5vzJzYP4U.Bkkzwy.5d.AAA.0.0.Bkkzy-.AWU1FDS03p8;
	usida=eyJ2ZXIiOjEsImlkIjoiQXJ3bnlzajF5N3Frbm0iLCJ0aW1lIjoxNjg3NDUyNjQzfQ%3D%3D

Figure 5. Screenshot of the user's network traffic depicting the user's URL Request headers associated with Defendant's Pixel ID 2208812335999737.

98. The image demonstrates that the user's Facebook ID (highlighted as "c_user=" in the image above) was sent alongside the other data.[41]

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

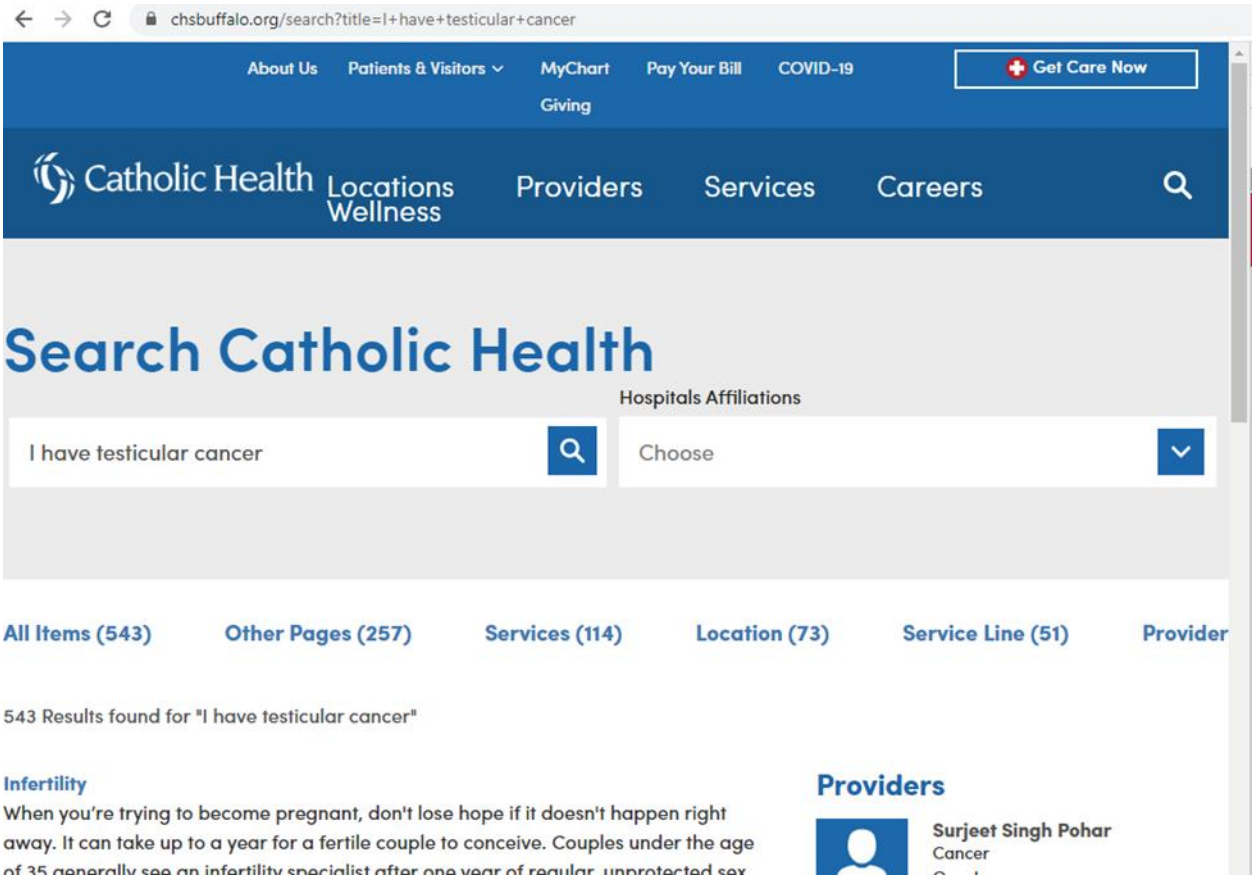


Figure 6. Screenshot taken when the user types "I have testicular cancer" into the general search bar on Defendant's homepage.

100. Resultantly, that exact phrase is sent to Facebook, thereby allowing the user's medical condition to be linked to their individual Facebook account for future retargeting and

[41] 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.

exploitation. This is simply unacceptable, and there is no legitimate reason for sending this information to Facebook.

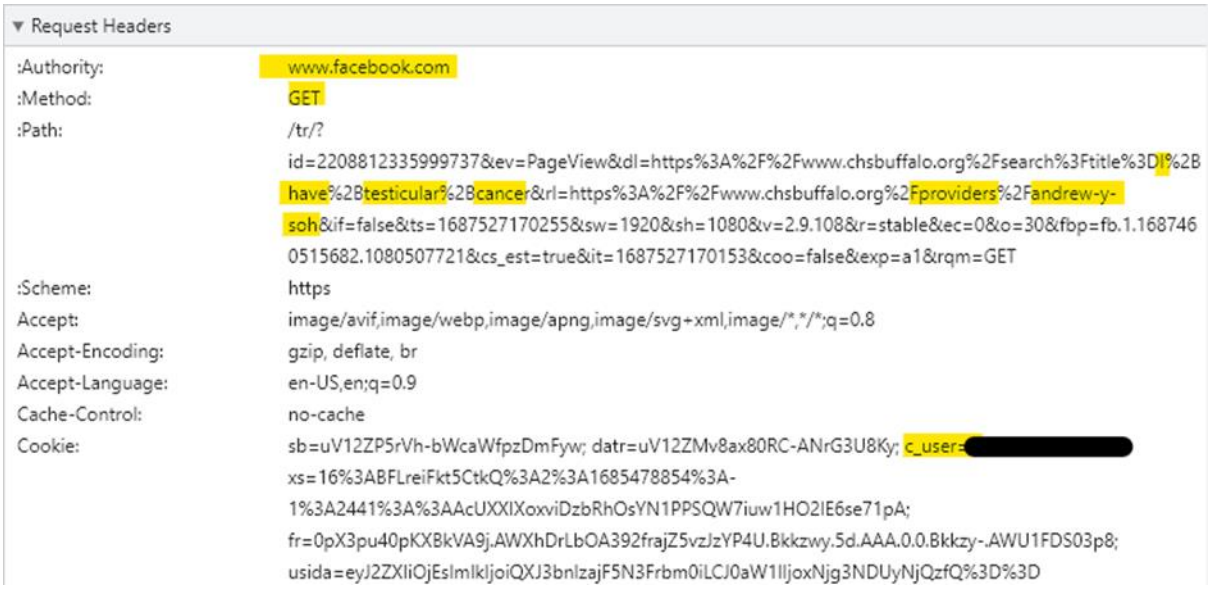


Figure 7. Screenshot take from the user's traffic report depicting the "Payload" and corresponding "Headers" associated with the user's online activity and communications to Defendant.

101. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook 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.

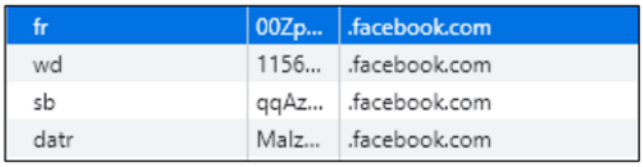
102. Facebook receives at least six cookies when Defendant's website transmits information via the Pixel**:**

Request Cookies ☐ show filtered ou

Name	Value	Domain
sb	uV1...	.facebook.com
datr	uV1...	.facebook.com
c_user	100...	.facebook.com
xs	16%...	.facebook.com
fr	0pX...	.facebook.com
usida	eyJ2...	.facebook.com

Figure 8.

103. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies:[42]



fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 9.

104. The fr cookie contains an encrypted Facebook ID and browser identifier.[43] Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[44]

105. The cookies listed in the two images above are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is

---

[42] The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

[43] Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May 11, 2023).

[44] *Cookies & other storage technologies*, FACEBOOK, https://www.facebook.com/policy/cookies/ (last visited June 23, 2023).

ultimately responsible for the manner in which individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout its website.

106. Defendant also revealed its website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user:[45]

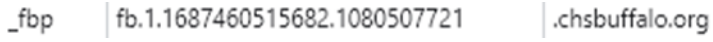


Figure 10.

107. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookies and c_user cookie, the _fbp cookie functions as a first-party cookie—i.e. a cookie that was created and placed on the website by Defendant.[46]

108. The Facebook Tracking Pixel uses both first- and third-party cookies.

109. Moreover, as seen in the image below, when patients visit https://mychart.chsbuffalo.org/MyChart/Authentication/Login to login into their MyChart account on Defendant's Website, the Pixel is running on the login page and transmitting that the patient is

[45] *Id.*

[46] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

logging into MyChart as represented by the _fbp cookie that is highlighted:

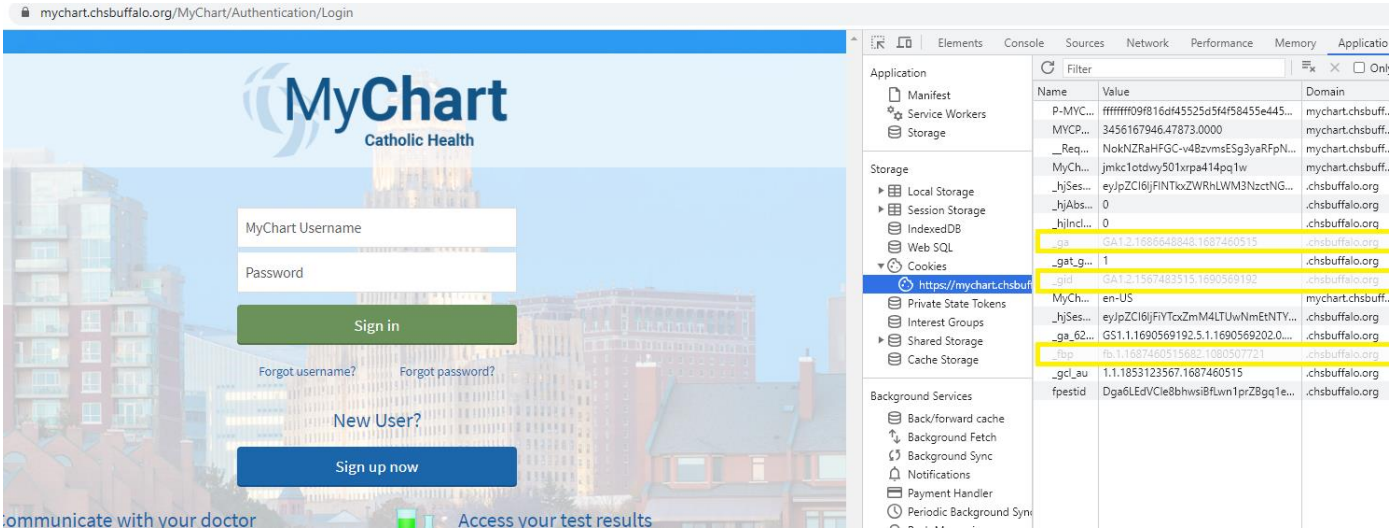


Figure 11: Screenshot showing the cookies that are running on the MyChart login page from Defendant's Website.

110. A closer image of the "Applications" tab from the image directly above shows that the Facebook Pixel, as well as Google ad cookies, are running on the MyChart login page:

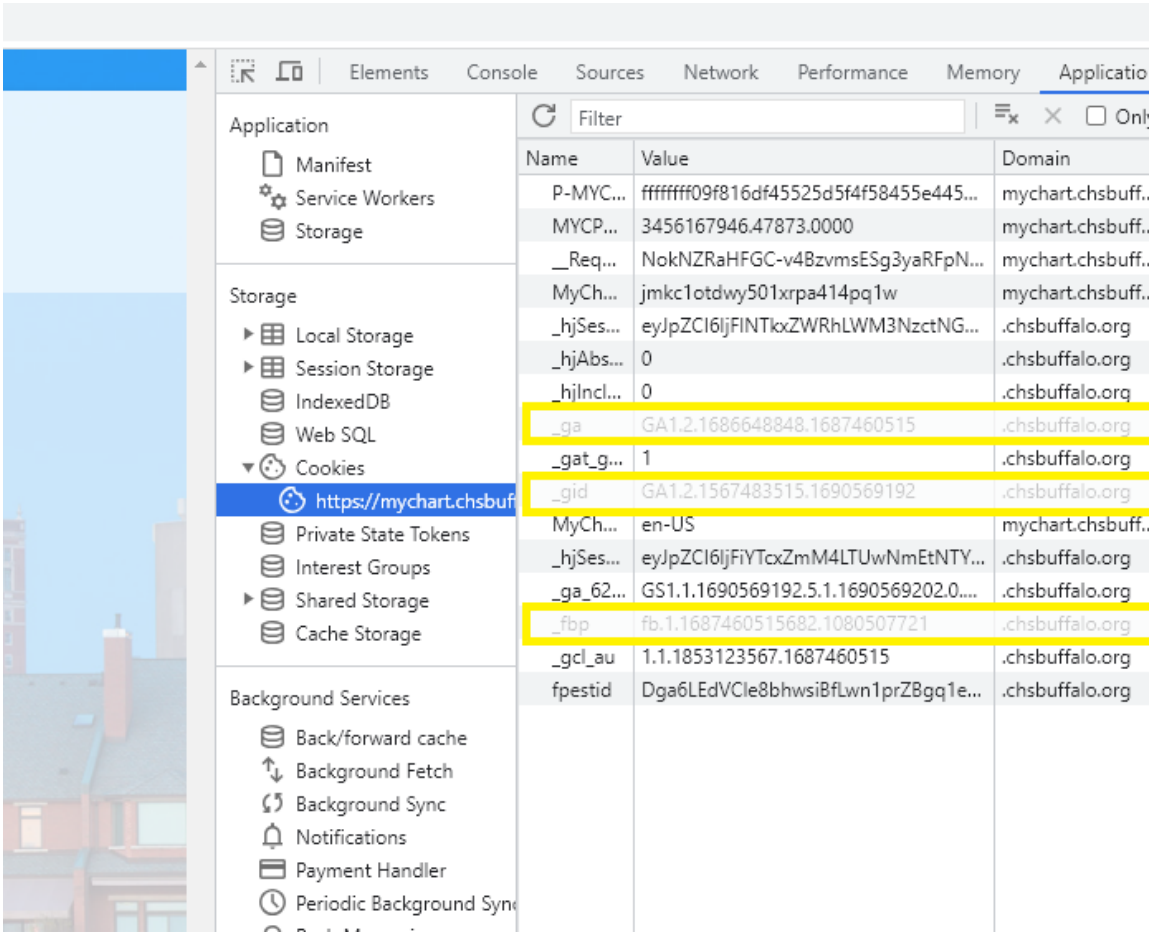


Figure 12. The screenshot above is a cropped portion of Figure 11.

111. In summation, Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, patients' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

112. 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.

113. The image below contains the content of the user's communication typed into the search bar, "I have testicular cancer", and Defendant does not appear to have enabled the anonymize feature provided by Google Analytics because the text "aip:" does not appear in the image.

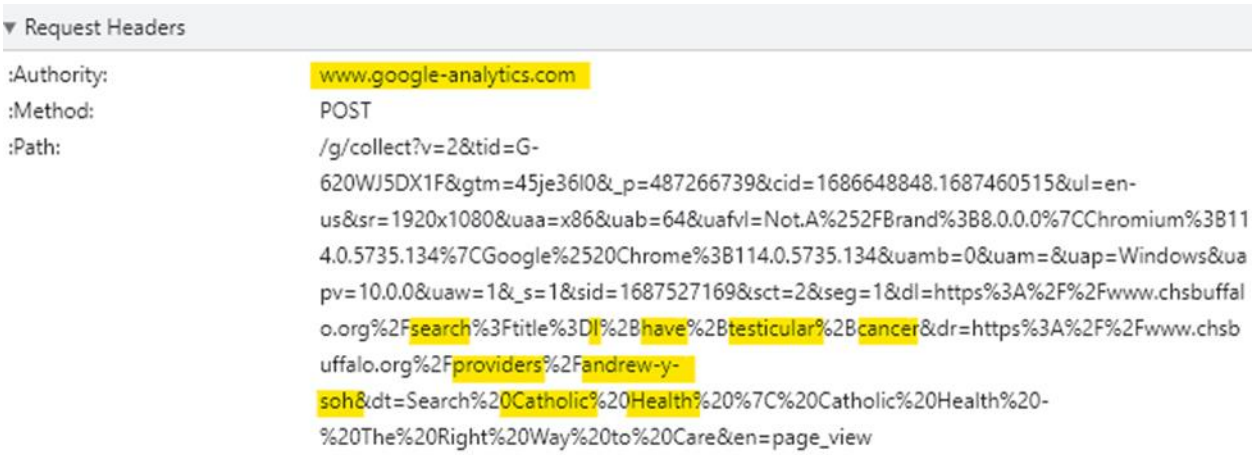


Figure 13. The screenshot above was captured from the user's network report and depict what types of information Google received. Notably, the user was executing their search through the Microsoft Edge web browser, not the Google Chrome browser. Stated differently, Google would not have received this information but for Defendant's use of Google's analytics tools.

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

115. 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 and Class Members' private communications to Facebook or Google.

116. In fact, Defendant's use of tracking technology was not reasonably knowable until at least June 16, 2022, when The Markup published an article entitled, "Facebook Is Receiving Sensitive Medical Information from Hospital Websites."[47] The Markup article was the result of an investigation called the Pixel Hunt project, which involved a crowd-sourced research initiative to learn where the Facebook pixel was collecting information on healthcare providers' websites.[48]

117. Another article from academics at the University of Illinois, which also addressed the topic, was published on November 17, 2022, entitled, "All Eyes On Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems."[49]

118. In the Fall of 2022, several members of Congress began asking questions about hospitals' disclosure of patient information to Facebook and others via tracking technology.

119. Senator Jon Ossoff questioned a Meta official on September 14, 2022 about Meta's collection of patient data to which the Meta official responded by saying he did not have an answer but would investigate and provide more information.[50]

120. On October 20, 2022, Senator Mark Warner issued a letter to Mark Zuckerberg, CEO of Meta, citing the Markup article and requesting information from Meta as to Meta's collection of patient health information via tracking technology on healthcare provider websites.[51] Senator Warner's letter stated, "I am troubled by the recent revelation that the Meta Pixel was

[47] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[48] *Id.*
[49] Mingjia Huo, Maxwell Bland, and Kirill Levchenko. 2022. *All Eyes On Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems.* In Proceedings of the 21st Workshop on Privacy in the Electronic Society (WPES '22), November 7, 2022, Los Angeles, CA, USA. ACM, New York, NY, USA, 15 pages. Available at https://doi.org/10.1145/3559613.3563190
[50] https://www.c-span.org/clip/senate-committee/user-clip-meta-response-to-sen-ossoff-question/5031355
[51] https://www.warner.senate.gov/public/index.cfm/2022/10/warner-expresses-concern-over-meta-s-collection-of-sensitive-health-information

installed on a number of hospital websites – including password-protected patient portals – and sending sensitive health information to Meta when a patient scheduled an appointment online. This data included highly personal health data, including patients' medical conditions, appointment topics, physician names, email addresses, phone numbers, IP addresses, and other details about patients' medical appointments."[52]

121. With journalists, researchers, academics, and Senators all first providing information in Summer through Fall 2022 about the dangers for patient health information presented by tracking technology, it is not reasonable to expect ordinary members of the public to have knowledge that their PHI and other sensitive information was being disclosed by their health care providers before that time.

C. Plaintiff J.C.'s Experience

122. Plaintiff, as Defendant's patient, has received healthcare services from 2015 through present day at hospitals and clinics in Defendant's network and has used Defendant's Website to communicate Private Information to Defendant on numerous occasions.

123. Plaintiff has been a Facebook user since at least 2010 and uses Facebook multiple times per day.

124. Plaintiff has used her desktop computer, cell phone, and tablet to access Facebook over the years.

125. On numerous occasions, Plaintiff accessed Defendant's Website on her desktop computer, cell phone, and tablet for the purpose of finding and obtaining medical treatment for her specific conditions. Plaintiff accessed Defendant's Website to receive healthcare services from

[52] *Id.*

Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

126. Plaintiff used Defendant's Website frequently and regularly from 2016 through the present to research medical symptoms, search for specific doctors and specialists who could help with specific conditions, make appointments, complete patient web forms, and check her medical records and test results.

127. Specifically, Plaintiff has used the public facing portions of Defendant's Website to search for orthopedic specialists and treatment options related to a degenerative disk disease, broken bones in her legs and ankles, and a variety of neck and back related conditions. She used Defendant's Website to search for this information for the first time in roughly 2016. She used Defendant's Website to search for this information as recently as this year, 2025.

128. Also using the public facing portions of Defendant's Website, Plaintiff booked a variety of appointments with her medical care providers. In the course of booking these appointments, Plaintiff shared her patient status, the date, time, and location of her appointments, the names and specialties of the healthcare providers she was seeing, and the purpose of her appointment. Specific appointments she has made since 2015 include consultations for neck and spinal surgeries, ongoing MRIs approximately every six months, and consultations for her ankle surgeries.

129. Plaintiff has used the public facing portion of Defendant's Website to find doctors and request appointments at Kenmore Mercy Hospital for her orthopedic care over the last five years. She has also used the public facing portion of Defendant's Website to schedule MRI appointments at Defendant's Rosewell facility.

130. Just since 2022, Plaintiff specifically recalls using Defendant's Website to research and book appointments with more than 10 specialists for orthopedic and oncological care, including an orthopedic surgery in 2023 at Kenmore Mercy for a broken ankle. Plaintiff previously had neck surgery and multiple spine surgeries at Defendant's facilities due in part to her degenerative disk disease and once following a car accident.

131. Following her visits to Defendant's Website, Plaintiff observed advertisements on her Facebook account related to the treatments she sought and received through medical providers she viewed on Defendant's Website. These advertisements included specific locations, providers, and treatments she had researched on Defendant's Website in connection with booking appointments for her healthcare.

132. For example, one day Plaintiff accessed Defendant's Website to research one of her orthopedic conditions and some corresponding treatments that may be available. Imminently thereafter, Plaintiff received targeted advertisements on Facebook relating to the very same orthopedic condition and the very same kind of treatments she had just researched on Defendant's Website.

133. In a separate example, in 2020, Plaintiff was using Defendant's Website (specifically the MyChart portal) to communicate with her healthcare providers regarding her orthopedic surgeries, and to complete forms and review records related to the same. Imminently after accessing her MyChart profile through Defendant's Website for these purposes, Plaintiff received targeted advertisements on Facebook for the exact specialists she had researched and communicated with and related to the exact surgical procedures she was communicating about.

134. Plaintiff has noticed similar instances in the past five years where she has seen Facebook advertisements related to local orthopedic care providers and pain management options

specifically for her degenerative disk disease shortly after using Defendant's Website to research, book appointments, or communicate with healthcare providers about those very issues.

135. Plaintiff also used Defendant's Website to access the portal to her MyChart records. Doing so required her to sign-in to her MyChart profile through the access portal on Defendant's Website.

136. Plaintiff has regularly used her MyChart profile, through Defendant's Website, for myriad purposes from 2015 through the present.

137. Specifically, Plaintiff used MyChart extensively in 2020 to review medical records including pre-surgery records and MRI/medical imaging results, fill out various forms related to surgeries, privacy disclosures, and general consent waivers, and communicate directly with healthcare providers about her orthopedic conditions. Plaintiff has signed into her MyChart profile through Defendant's Website at least every six months for the past five years and used it extensively even prior to that.

138. Plaintiff submitted medical information to Defendant via its Website. Because Defendant utilizes the Facebook Pixel, the Website's Source Code sends a secret set of instructions back to the individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and both the webpage's and, upon information and belief, MyChart portal's URLs to Facebook.

139. Pursuant to the systematic process described in this Complaint, 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.

140. As Defendant's patient, Plaintiff reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted to or disclosed to a third party. But for her status as Defendant's patient, Plaintiff would not have disclosed her Private Information to Defendant.

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

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

143. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' FIDs, IP addresses, and/or device IDs or other information they input into Defendant's Website, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients. Plaintiff's and Class Members identities could be easily determined based on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

144. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile

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

145. Based on the presence of the Pixel and Conversions API, Defendant unlawfully disclosed Plaintiff's Private Information to Facebook. The presence of Facebook advertisements confirms Defendant's unlawful transmission of Plaintiff's Private Information to Facebook. Said differently, Plaintiff did not disclose this Private Information to any other source—only Defendant's Website.

146. In sum, Defendant's Pixel transmitted Plaintiff's highly sensitive communications and Private Information to Facebook, including communications that contained private and confidential information, without Plaintiff's knowledge, consent, or express written authorization

147. Defendant breached Plaintiff's right to privacy and unlawfully disclosed her Private Information to Facebook. Specifically, Plaintiff had a reasonable expectation of privacy, based on her status as Defendant's patient, that Defendant would not disclose her Private Information to third parties.

148. Defendant did not inform Plaintiff that it shared her Private Information with Facebook.

149. By doing so without Plaintiff's consent, Defendant breached Plaintiff's and Class Members' right to privacy and unlawfully disclosed Plaintiff's Private Information.

150. Upon information and belief, as a "redundant" measure to ensure Plaintiff's Class Members' Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's and

Class Members' Private Information from electronic storage on Defendant's server directly to Facebook.

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

152. Plaintiff's emotional damages and the damage to her privacy are also concrete and significant. When Plaintiff agreed to pay the already high cost of her medical bills in exchange for her treatment from Defendant, she reasonably believed she was also paying for privacy and security related to that treatment. To discover that Defendant violated that trust to profit from her Private Information has caused Plaintiff serious emotional distress and undermined her faith in the healthcare system.

153. Plaintiff has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

D. Defendant's Conduct Is Unlawful and Violated Industry Norms

1. Defendant Violated HIPAA Standards

154. 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 patient for marketing purposes without the patients' express written authorization.[53]

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

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

156. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[54]

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

158. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

159. Under the HIPPA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated

[54] HHS.gov, HIPAA For Professionals (last visited April 12, 2023), https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

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

45 C.F.R. § 160.514.

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

161. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained

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

162. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

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

164. 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.[55]

165. 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

[55]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022).

> 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).[56]

166. As alleged above, there is an HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[57]

167. 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."

168. Defendant's actions violated HIPAA Rules per this Bulletin.

2. Defendant Violated New York Law

169. New York law has established policies and procedures for the maintenance, preservation, and storage of patient medical records.

170. New York law provides that all patients are entitled to privacy and confidentiality with respect to their treatment and medical records: "[e]very patient shall have the right to have privacy in treatment and in caring for personal needs, confidentiality in the treatment of personal and medical records, and security in storing personal possessions." N.Y. Pub. Health Law § 2803(3)(f).

171. New York law also provides that medical professionals are not allowed to disclose information obtained from a patient: "[u]nless the patient waives the privilege, a person authorized

---

[56]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)

[57] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

to practice medicine, registered professional nursing, licensed practical nursing, dentistry, podiatry or chiropractic shall not be allowed to disclose any information which he acquired in attending a patient in a professional capacity, and which was necessary to enable him to act in that capacity." N.Y. C.P.L.R. 4504.

172. Defendant's actions described herein violated New York law.

3. Defendant Violated Industry Standards

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

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

175. 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)

176. 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.

177. 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.

E. Plaintiff's and Class Members' Expectation of Privacy

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

179. 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.

180. Plaintiff and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

F. IP Addresses Are Personally Identifiable Information

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

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

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

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

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

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

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

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

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

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

189. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiff's and class members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. 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 its platform.

190. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

191. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so

through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

192. By utilizing the Pixel, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiff and Class Members and violating their rights under federal and New York law.

H. Plaintiff's and Class Members' Private Information Had Financial Value

193. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

194. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202.00 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434.00 per user, for a total of more than $200 billion industry wide.

195. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[58]

[58] *See* https://time.com/4588104/medical-data-industry/ (last visited February 16, 2023).

196. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[59]

TOLLING

197. 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 PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

198. 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.

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

> All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website and had their Private Information disclosed to a third party without authorization.

In the alternative, Plaintiff seeks to represent a "New York Class" defined as:

> All individuals residing in New York who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website, and had their Private Information disclosed to a third party without authorization or consent.

The Nationwide Class and New York Class are collectively referred to as the "Class."

200. 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

[59] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited March 1, 2023).

successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

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

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

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

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

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

g. whether Defendant's conduct violated the New York Deceptive Trade Practices Act, Gen. Bus. Law § 349;

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

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

204. **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.

205. **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.

206. **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 a large corporation 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.

207. **Policies Generally Applicable to the Class**, Fed. R. Civ. P. 23(b)(2). 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.

208. 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.

209. The litigation of the claims 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.

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

211. 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.

212. 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.

213. **Issue Certification**, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the following:

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

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

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

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

e. 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; and

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

COUNT I
BREACH OF FIDUCIARY DUTY/CONFIDENTIALITY
(On Behalf of Plaintiff and the Class)

214. Plaintiff incorporates all prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

215. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

216. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

217. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

218. Contrary to its duties as a medical provider and its express and implied 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.

219. These disclosures were made for commercial purposes without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

220. The unauthorized disclosures of Plaintiff's and Class Members' Private Information were intentionally caused by Defendant's employees acting within the scope of their employment. Alternatively, the disclosures of Plaintiff's and Class Members' Private Information occurred because of Defendant's negligent hiring or supervision of its employees, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees to properly discharge their duties under those policies and procedures.

221. Defendant's conduct went beyond mere marketing purposes – its primary motivation and determinative factors for intercepting and disclosing patient communications included:

a. deliberate circumvention of HIPAA's privacy protections by knowingly transmitting unencrypted PHI without required safeguards or business associate agreements;

b. intentional violation of N.Y. Public Health Law § 2803's patient privacy requirements by disclosing confidential treatment information without authorization;

c. purposeful evasion of patient consent requirements to monetize private health data; and

d. calculated deployment of redundant tracking mechanisms (Pixel and CAPI) specifically designed to defeat patients' privacy controls and technical protections.

222. The third-party recipients included, but may not be limited to, Facebook. Such information was received by these third parties in a manner that allowed them to identify the Plaintiff and the individual Class Members.

223. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel embedded in its Website, contemporaneously intercepted and disclosed the contents of Plaintiff's and Class Members' electronic communications to Facebook in three distinct ways:

a. first, the Pixel intercepted real-time communications about medical conditions and appointments, as evidenced by Plaintiff's searches for orthopedic specialists and scheduling of surgical consultations between 2020-2025;

b. second, the Pixel captured and transmitted patient portal login credentials and session data when Plaintiff accessed her MyChart account to view medical records and test results approximately every six weeks; and

c. third, Defendant's CAPI implementation provided a redundant server-side mechanism to ensure interception and transmission even when patients attempted to block the Pixel.

224. Defendant’s breach of the common law implied covenant of trust and confidence is evidenced by its failure to comply with federal and state privacy regulations, including:

a. by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

b. by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

c. by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

d. by failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiff’s and Class Members PHI;

e. by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. by failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);

g. by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

h. by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);

i. by failing to keep Private Information confidential as required by N.Y. C.P.L.R. 4504;

j. by failing to keep Private Information confidential as required by N.Y. Pub. Health Law § 2803(3)(f); and

k. by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

225. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

226. 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;

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

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

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

e. nominal damages for each independent violation;

f. 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;

g. 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;

h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and

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

COUNT II
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 Class)

227. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

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

229. 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.

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

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

232. Defendant's intentional interception and disclosure served criminal purposes beyond marketing, including:

a. violation of 42 U.S.C. § 1320d-6's criminal provisions by knowingly disclosing individually identifiable health information without authorization;

b. violation of N.Y. Penal Law § 156.05 by knowingly causing unauthorized access to patient computing devices;

c. violation of N.Y. Penal Law § 156.29 by unlawfully duplicating medical records and treatment information; and

d. violation of N.Y. Penal Law § 156.10 by knowingly gaining unauthorized access to computer systems with intent to commit further crimes.

233. This criminal intent is evidenced by Defendant's implementation of redundant tracking mechanisms specifically designed to circumvent patient privacy controls and technical protections, demonstrating its purpose went beyond mere marketing to intentionally violate state and federal privacy laws.

234. **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).

235. **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).

236. **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).

237. **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 deployed by Defendant to effectuate the sending and acquisition of patient communications.

238. Under the ECPA, CHS cannot escape liability merely because it was a party to the communications. The party exemption does not apply because CHS's participation in these communications was expressly for the purpose of committing criminal acts and torts, as evidenced by:

a. its knowing violation of HIPAA's criminal provisions;

b. its deliberate circumvention of New York's statutory privacy protections;

c. its intentional deployment of redundant tracking mechanisms specifically designed to defeat privacy controls; and

d. its purposeful structuring of the tracking mechanisms to capture and transmit protected health information in violation of state and federal law.

239. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel imbedded and ran on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff's and Class Members'

electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

240. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel imbedded and ran on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class Members' electronic communications, for purposes other than providing health care services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

241. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally redirected the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

242. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

243. By intentionally disclosing or endeavoring to disclose the electronic communications of 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).

244. 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).

245. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

246. Defendant accessed, obtained, and disclosed Plaintiff's and Class Members' Private Information with the specific intent of committing criminal and tortious acts, as evidenced by:

a. the timing of Defendant's actions - continuing to deploy and expand tracking mechanisms after the December 2022 HHS Bulletin explicitly warned that such disclosures violated HIPAA;

b. the scope of information captured - deliberately programming the Pixel to capture not just general browsing data but specific medical conditions, appointment details, and patient portal login attempts;

c. the methods employed - implementing both client-side (Pixel) and server-side (CAPI) tracking to ensure capture of Protected Information even when patients attempted to block such tracking; and

d. the commercial exploitation - using the intercepted Protected Information to create targeted advertising campaigns based on patients' specific medical conditions and treatments, demonstrating the interception was not incidental but rather central to Defendant's business strategy.

247. Defendant's criminal and tortious purpose is further demonstrated by the specific types of Protected Information it programmed its tracking mechanisms to intercept and disclose, including:

a. patient portal login credentials and session data;

b. search queries for specific medical conditions and treatments;

c. appointment scheduling details including dates, times, and provider specialties;

d. form submissions containing medical history and symptoms; and

e. website navigation patterns revealing treatment paths and medical interests.

248. This granular level of tracking goes far beyond what would be necessary for general marketing or website analytics, evidencing Defendant's specific intent to capture and monetize Protected Information in violation of state and federal law.

249. Defendant's criminal intent is also demonstrated by its efforts to conceal these tracking mechanisms from patients by:

a. failing to disclose the presence of tracking mechanisms in its privacy policies;

b. obtaining required authorizations for disclosure of Protected Information;

c. implementing tracking in a manner designed to be invisible to users; and

d. continuing these practices even after regulatory guidance explicitly deemed them unlawful.

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

251. 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.

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

253. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State

– namely, violations of the New York Patient's Bill of Rights, New York Public Health laws, and invasion of privacy, among others.

254. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

255. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

256. Defendant's acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and New York, including.

a. criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. criminal violation of New York Computer Crime statutes, including: Unauthorized use of computer (N.Y. Penal § 156.05); Unlawful duplication (N.Y. Penal § 156.29); and Computer trespass (N.Y. Penal § 156.10);

c. violation of the New York Patient's Bill of Rights, N.Y. Pub. Health § 2803-c;

d. violation of law regarding New York Civil Practice Law and Rules § 4504;

e. violation of the New York Deceptive Trade Practices Act, Gen. Bus. Law § 349; and

f. invasion of Privacy.

257. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

258. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

259. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. disclosed individually identifiable health information to Facebook and Google without patient authorization.

260. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook and Google source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

261. Under N.Y. Penal § 156.05, a person commits the offense of unauthorized use of a computer if he "knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization."

262. Defendant violated the N.Y. Penal § 156.05 in that Defendant knowingly used and accessed Plaintiff's and Class Members' computing devices and data as part of a deception and without their authorization, including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to send identifiers and the content of communications with Defendant simultaneously to Defendant and Facebook, Google, and others.

263. Under N.Y. Penal § 156.29, a person commits the offense of unlawful duplication of computer related materials if he copies, reproduces or duplicates in any manner computer material that contains records of the medical history or medical treatment of an identified or readily

identifiable individual or individuals with an intent to commit or further the commission of any crime under this chapter.

264. Defendant violated N.Y. Penal § 156.29 by exceeding its authorization to access Plaintiff's and Class Members' computers including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to make unauthorized copies of Plaintiff's and Class Members' electronic data and to send identifiers and the content of communications with Defendant simultaneously to Defendant and Facebook, Google, and others.

265. Under N.Y. Penal § 156.10, a person commits the offense of computer trespass if he knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization and:

a. he or she does so with an intent to commit or attempt to commit or further the commission of any felony; or

b. he or she thereby knowingly gains access to computer material.

266. Defendant violated N.Y. Penal § 156.10 when it knowingly and without Plaintiff or Class Members' authorization inserted the fbp, ga, and gid cookies on Plaintiffs' and Class Members' computing devices.

267. The fbp, ga, and gid cookies, which constitute programs, commanded Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

268. Defendant knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

269. Under New York's Rights of Patients in Certain Medical Facilities, N.Y. Pub. Health § 2803-c(3)(f), "[e]very patient shall have the right to have privacy in treatment and in caring for personal needs, confidentiality in the treatment of personal and medical records, and security in storing personal possessions."

270. Defendant violated the New York Rights of Patients by disclosing Plaintiff's and Class Members' Private Information to third parties without authorization or consent.

271. Under New York Civil Practice Law and Rules Section 4504, "[u]nless the patient waives the privilege" medical professionals are not "allowed to disclose any information which he acquired in attending a patient in a professional capacity, and which was necessary to enable him to act in that capacity."

272. Defendant violated N.Y. C.P.L.R. 4504 by disclosing Plaintiff's and Class Members' Private Information to third parties without authorization or consent.

273. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their individually-identifiable patient health information on its Website, because it used its participation in these communications to improperly share Plaintiff's and Class Members' individually-identifiable patient health information with Facebook and Google, third-parties that did not participate in these communications, that Plaintiff and Class Members did not know were receiving their individually-identifiable patient health information, and that Plaintiff and Class Members did not consent to receive this information.

274. Defendant accessed, obtained, and disclosed Plaintiff's and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it

would not have been able to obtain the information or the marketing services if it had complied with the law.

275. As such, Defendants cannot viably claim any exception to ECPA liability.

276. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable patient health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or the Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' individually-identifiable patient health information, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members;

d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

e. the diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

277. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100.00 a day for each day of violation or $10,000.00, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT III
INVASION OF PRIVACY
Violations of N.Y. Civ. Rights Laws §§ 50, 51
(On Behalf of Plaintiff and the Class)

278. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

279. Plaintiff and Class Members have a statutory privacy interest in their names, portraits, pictures, and voices under New York law.

280. Defendant knowingly used Plaintiff's and Class Members' names and other Private Information in the State of New York for advertising and trade purposes without first obtaining their written consent.

281. Specifically, Defendant transmitted Plaintiff's and Class Members' names and/or FID to third parties like Facebook for targeted advertising and other commercial purposes, as described herein.

282. Defendant's use of Plaintiff's and Class Members' names and Private Information did not serve any public interest.

283. The unlawful tracking of Plaintiff and Class Members' and disclosure of their names in connection with their Private Information has caused Plaintiff and Class Members to suffer damages. This includes damage to the value of their information, which Defendant appropriated for its own enrichment. Plaintiff and Class Members have also suffered nominal damages.

284. 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.

285. 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.

286. 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, plus prejudgment interest, and costs. Alternatively, Plaintiff and Class Members are entitled to nominal damages.

287. Plaintiff and Class Members are entitled to exemplary and/or punitive damages as a result of Defendant's knowing violations of their statutory rights to privacy.

288. 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 other third parties and the wrongful disclosure of the information cannot be undone.

289. 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.

290. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into Plaintiff's and Class Members' statutory privacy interests.

COUNT IV
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Class)

291. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

292. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care.

293. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

294. 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.

295. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

296. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties like Facebook.

297. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

298. 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 Class)

299. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

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

301. 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 to exceed the limited authorization and access to that information which was given to Defendant.

302. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

303. 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.

304. 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 against equity and good conscience 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.

305. 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
NEGLIGENCE
(On behalf of Plaintiff and the Class)

306. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

307. Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

308. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

309. 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.

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

311. The third-party recipients included, but may not be limited to, Facebook.

312. 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;

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

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

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

e. nominal damages for each independent violation;

f. 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;

g. 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;

h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

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 Class and appointing Plaintiff and Counsel to represent such Class;

b. for equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint 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;

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

b. for prejudgment interest on all amounts awarded; and

c. 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: February 14, 2025

Respectfully Submitted,

/s/ Philip J. Krzeski

Philip J. Krzeski
CHESTNUT CAMBRONNE PA
100 Washington Avenue S., Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
pkrzeski@chestnutcambronne.com

Randi A. Kassan
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Telephone: 516-741-5600
Fax: 516-741-0128
rkassan@milberg.com

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

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

Terence R. Coates
Dylan J. Gould
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Telephone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Counsel for Plaintiff and the Putative Class

ClassAction.org