E-FILED
Friday, 06 September, 2024 10:20:57 AM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
ROCK ISLAND DIVISION

ALANA HANNANT, individually, and on behalf of all others similarly situated, Plaintiff, v. CULBERTSON MEMORIAL HOSPITAL FOUNDATION d/b/a SARAH D. CULBERTSON MEMORIAL HOSPITAL, Defendant.	)	Case No.: JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, ALANA HANNANT, individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Class Action Complaint against Defendant, CULBERTSON MEMORIAL HOSPITAL FOUNDATION d/b/a SARAH D. CULBERTSON MEMORIAL HOSPITAL ("Culbertson" or "Defendant"), including by and through its agents, employees, and other representatives, and alleges, upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action to address Defendant's outrageous, illegal, and widespread practice of disclosing the confidential Personally Identifying Information[1] ("PII")

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

and/or Protected Health Information[2] ("PHI") (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google, LLC ("Google"), Microsoft, and potentially others ("the Disclosure").

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendant's, that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[3] OCR and FTC agree that such tracking technologies, like those present on Defendant's website, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[4] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Culbertson is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services (July 20, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last accessed April 9, 2024), attached as Exhibit A.

[4] *Id.*

including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information 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."[5]

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

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 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.

5. In December 2022, HHS released a bulletin on its website regarding the use of tracking technologies by entities covered by HIPAA—healthcare entities like Culbertson—and its

[5] *Id.*

business associates (the "December 2022 Bulletin").[6]

6. Therein, HHS defined tracking technologies, explaining:

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors.[7]

7. In the Bulletin, HHS was clear in unambiguous terms 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.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[8,9]

8. On March 18, 2024, HHS updated its December 2022 bulletin, "to increase clarity for regulated entities and the public" and reiterating the above basic privacy obligations.[10,11]

---

[6] *See* archived version of the December 2022 Bulletin at *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS.gov (Dec. 1, 2022), https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Mar. 30, 2024).

[7] *Id*.

[8] *Id*. (bold emphasis in original)

[9] Citing *to* 45 CFR 164.508(a)(3); s*ee also* 45 CFR 164.501 (definition of "Marketing").

[10] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022, updated Mar. 18, 2024), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last acc. June 20, 2024).

[11] On June 20, 2024, in *American Hospital Association, et al. v. Xavier Becerra, et al.,* Case No. 4:23-cv-01110-P (N.D. Tx., Jun. 20, 2024, Doc. 67), the U.S. District Court for the Northern District of Texas vacated HHS's March 14, 2024 Bulletin as to the "Proscribed Combination," *but* acknowledged that the Proscribed Combination could be PHI in certain circumstances.

9. Located in Rushville, Illinois, Defendant is a hospital system with more than 200 staff members. In addition to in-patient services, Culbertson maintains a 24-hour-a-day emergency department, multiple outpatient specialty clinics, and four family practice clinics."[12]

10. Despite its unique position as a trusted healthcare provider, Defendant knowingly configured and implemented into its website, https://cmhospital.com/ (the "Website") code-based tracking devices known as "trackers" or "tracking technologies," which collected and transmitted patients' Private Information to Facebook, Google, Microsoft, and possibly other third parties, without patients' knowledge or authorization.

11. Defendant encourages patients to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to learn about Culbertson on its website homepage[13], to find medical providers,[14] to find and research medical services,[15] to access a patient portal,[16] to pay bills,[17] to search the website, including for personal medical treatment information,[18] and more.

12. Plaintiff and the Class Members visited Culbertson's Online Platforms in relation to their past, present, and future healthcare needs and/or to transmit a payment for health care.

13. When Plaintiff and Class Members used Culbertson's Website and Online Platforms, they thought they were communicating exclusively with her trusted healthcare provider. Unbeknownst to them, Culbertson embedded pixels from Facebook, Google, Microsoft, and possibly others, into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class

[12] https://cmhospital.com/about-us (last visited Aug. 12, 2024).
[13] *Id*.
[14] https://cmhospital.com/providers (last visited Aug. 12, 2024).
[15] https://cmhospital.com/services (last visited Aug. 12, 2024).
[16] https://cmhospital.com/patients-and-visitors/patient-portal (last visited Aug. 12, 2024).
[17] https://culbertson.paymyhealthbill.com/quickpay (last visited Aug. 12, 2024).
[18] *E.g.*, search for "cancer," https://cmhospital.com/search?q=cancer (last visited Aug. 12, 2024).

Members to transmit intimate details about their medical treatment to third parties without their consent.

14. A tracker (also referred to as "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and her website interactions.[19] When a person visits a website with an tracker, it tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[20] Then, the tracker transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[21]

15. Among the trackers Culbertson embedded into its Website is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a website user's device and the URLs and domains they visit.[22] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[23] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with her Facebook profile.[24]

---

[19] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[20] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[21] *Id.*
[22] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[23] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[24] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses her Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." *What are Cookies?*, COULDFARE, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

16. Operating as designed and as implemented by Culbertson, the Meta Pixel allowed Defendant to unlawfully disclose Plaintiff's and Class Members' private health information, alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook, without their authorization or knowledge.

17. Facebook encourages and recommends use of its Conversions Application Programming Interface ("CAPI") alongside use of the Meta Pixel.[25]

18. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interactions from the website owner's private servers, which transmits the data directly to Facebook, without involvement from the website user's browser.[26, 27]

19. 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 Culbertson to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly. For this reason, Facebook

[25] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, *How to Implement Facebook Conversions API (In Shopify)*, FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[26] *What is the Facebook Conversion API and How to Use It*, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[27] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *Conversions API*, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

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."[28]

20. Culbertson utilized data from these trackers to market its services and bolster its profits. Facebook utilizes data from the Meta Pixel and CAPI to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells for profit.

21. On information and belief, the information that Culbertson's Meta Pixel, and possibly CAPI, sent to Facebook included the Private Information that Plaintiff and the Class Members submitted to Culbertson's Website and Online Platforms, including, *inter alia*: their browsing activities, including the pages they viewed and the buttons they clicked; information concerning their statuses as patients such as patient portal activities; information concerning their medical concerns such as the providers they searched for and viewed and the medical services they viewed; as well as her identifying information, such as IP addresses and identifying cookies.

22. Such information allows third parties (e.g., Facebook) to learn of a particular individual's health conditions and seeking of medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then target Plaintiff and Class Members with online advertisements, based on the information they communicated to Culbertson via the Website. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

[28] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

23. In addition to the Facebook Pixel (and Facebook Events) and likely CAPI, on information and belief, Culbertson installed other tracking technologies, DoubleClick Ads,[29] Google Analytics,[30] Microsoft Clarity,[31] which operate similarly to the Meta Pixel and transmitted Plaintiff's and Class Members' Private Information to unauthorized third parties.

24. Healthcare patients simply do not anticipate that her trusted healthcare provider will send her private health information to a hidden third party—let alone Facebook, a company with a sordid history of violating consumer privacy in pursuit of ever-increasing advertising revenue.

25. Neither Plaintiff nor any Class Member signed a written authorization permitting Culbertson to send their Private Information to Facebook or other third parties uninvolved in her treatment.

26. Despite willfully and intentionally incorporating the Meta Pixel, potentially CAPI, and other third-party trackers into its Website and servers, Culbertson has never disclosed to Plaintiff or Class Members that it shared her Information with Facebook, Google, Microsoft, and possibly others.

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

28. Culbertson owed common law, statutory, regulatory, and contractual duties to keep Plaintiff's and Class Members' communications and Private Information safe, secure, and confidential.

29. Upon information and belief, Culbertson utilized the Meta Pixel and other tracker

[29] https://marketingplatform.google.com/about/enterprise/ (last visited Aug. 12, 2024)
[30] https://marketingplatform.google.com/about/analytics/ (last visited Aug. 12, 2024)
[31] https://clarity.microsoft.com/ (last visited Aug. 12, 2024)

data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

30. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard her information from unauthorized disclosure.

31. Culbertson breached its common law, statutory, and contractual 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) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiff's and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

32. Plaintiff seeks to remedy these harms and bring causes of action for (I) Negligence; (II) Negligence *Per Se*; (III) Invasion of Privacy—Intrusion Upon Seclusion; (IV) Breach of Implied Contract; (V) Unjust Enrichment; (VI) Breach of Implied Duty of Confidentiality; (VII) Violation of Illinois Consumer Fraud and Deceptive Business Practices Act, ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq.*; (VIII) Violation of the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq.*; (IX) Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.;* (X) Violation of the Electronic Communications Privacy Act,

18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service"); (XI) Violation of Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq.*; and (XII) Violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*

PARTIES

33. Plaintiff, ALANA HANNANT, is a natural person and a resident and citizen of the State of Illinois, where she intends to remain, with a principal residence in Rushville, Illinois in Schuyler County. She is a patient of Defendant and a victim of its unauthorized Disclosure of Private Information.

34. Defendant, CULBERTSON MEMORIAL HOSPITAL FOUNDATION d/b/a SARAH D. CULBERTSON MEMORIAL HOSPITAL ("Culbertson" or "Defendant"), is a non-profit corporation with a principal place of business at 238 South Congress St., Rushville, Illinois 62681 in Schuyler County.

JURISDICTION & VENUE

35. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because it arises under the laws of the United States and under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one member of the class is a citizen of a state different from Defendant.

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

37. Venue is proper in this judicial district under 28 U.S.C. § 1391 (a) through (d) because: (i) a substantial part of the events giving rise to this action occurred in this judicial district

including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the Disclosure of Plaintiff's and Class members' Private Information; (ii) Defendant's principal place of business is located in this judicial district; (iii) Defendant collects and redistributes Class members' Private Information in this judicial district and (iv) Defendant caused harm to Class members residing in this judicial district.

COMMON FACTUAL ALLEGATIONS

A. Background

38. Founded in 1921[32], Defendant is a hospital system in Rushville, Schuyler County, Illinois, which made a "…commit[ment] to improve local healthcare services so our area residents can receive quality care close to home."[33]

39. Culbertson further states that in "the last few years, the hospital has invested in state-of-the-art services such as 3D Mammography and a patient-friendly MRI service. The hospital also added a Hospitalist program, in-house Sleep Lab, a Geriatric Behavioral Health program, privatized the surgical suite patient rooms, as well as poured more resources into speech, occupational and physical therapy services."[34]

40. Moreover, Defendant extolls its values of "collaborative communication," "ethical behaviors," and "community," stating, "[w]e're your local hospital. We live and breath this community, just like you.[35]"

41. According to Culbertson, it "…maintains an expert medical staff consisting of a physician, physician assistant, four nurse practitioners and a pediatric nurse practitioner. Additionally, a growing number of regional specialty physicians commute to our facilities in

[32] https://cmhospital.com/about-us/history (last visited Aug. 12, 2024).
[33] https://cmhospital.com/about-us (last visited Aug. 12, 2024).
[34] *Id.*
[35] *Id.*

Rushville and Beardstown each week to offer her expertise in the fields of Cardiology, Gastroenterology, Oncology, Pulmonology, Urology and more."[36]

42. Culbertson provides myriad medical services, including: cardiopulmonary rehabilitation; counseling services; diagnostic cardiovascular screening; Department of Transportation (DOT) Exams; echocardiograms; emergency services; food and nutrition services; imaging; infusion center; lab services; surgical services; nuclear medicine; oncology; cardiology; kidney, hypertension and diabetes care; colorectal care; endocrinology; gastroenterology; gynecology; neurology; otolaryngology; orthopedics; podiatry; pulmonology; urology; vascular surgery; therapy services, the Swing Bed program[37] that "allows the patient to 'swing' or transition from the acute care setting to a transitional care bed where they receive skilled nursing care transition from acute medical care to home…"; support groups, and therapy services.[38]

43. As of February 2023, Defendant had total revenue approximating $57 million.[39]

44. Culbertson promotes the comprehensive functionality of these tools and promotes their use, in service of its own goal of increasing profitability. In furtherance of that goal, Defendant purposely installed the Meta Pixel and other trackers onto its Website, for the purpose of gathering information about Plaintiff and Class Members to further its marketing efforts. But Culbertson did not only generate information for its own use: it also shared patient information, including Private Information belonging to Plaintiff and Class Members, with Facebook, and other unauthorized third parties.

i. Facebook's Business Tools and the Meta Pixel

[36] *Id.*
[37] https://cmhospital.com/services/swing-bed-program (last visited Aug. 12, 2024).
[38] https://cmhospital.com/services (last visited Aug. 12, 2024).
[39] *Sarah D. Culbertson Memorial Hospital*, AMERICAN HOSPITAL DIRECTORY, https://www.ahd.com/free_profile.php?hcfa_id=3e4dff698aa001b9d1bbc8d5c5ee79ac&ek=8da66ddc31b33de51122aaceeeeb9303 (last visited Aug. 12, 2024).

45. Facebook operates the world's largest social media company and generated nearly $134 billion in revenue in 2023, roughly 99% of which was derived from selling advertising.[40]

46. In conjunction with its advertising business, Facebook encourages and promotes its "Business Tools" to be used to gather customer data, identify customers and potential customers, target advertisements to those individuals, and market products and services.

47. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into her 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, clicks a button, fills out a form, and more.[41] Businesses that want to target customers and advertise her services can also create her own tracking parameters by building a "custom event."[42]

49. The Meta Pixel is a Business Tool used to "track[] the people and type of actions they take" on a website.[43] When an individual accesses a webpage containing the Meta Pixel, the communications with that webpage are instantaneously and surreptitiously duplicated and sent to

---

[40] *Meta Reports Fourth Quarter and Full Year 2023 Results*, META (Feb. 1, 2024), https://investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx.

[41] *Specifications for Facebook Pixel Standard Events*, META, https://www.facebook.com/business/help/402791146561655 (last visited June, 21, 2024); *see also 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 https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited June 21, 2024).

[42] *About Standard and Custom Website Events*, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

[43] *Retargeting*, META, https://www.facebook.com/business/goals/retargeting (last visited June 21, 2024).

Facebook, traveling directly from the user's browser to Facebook's server, based off instructions from the Meta Pixel.

50. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy, such as a homepage, and disable it on pages that do implicate patient privacy, such as Defendant's "Services" pages.

51. The Meta Pixel's primary purpose is to enhance online marketing, improve online ad targeting, and generate sales.[44]

52. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[45]

53. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything that is generally present in HTTP headers, a standard web protocol sent between any browser request and any server on the internet. This information may include data like IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** [Emphasis added.]
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values

[44] *See Meta Pixel*, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed June 21, 2024).
[45] *About Meta Pixel*, META, https://www.facebook.com/business/help/742478679120153 (last visited June 21, 2024).

unless you include them as part of Advanced Matching or optional values.[46]

54. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[47]

55. Facebook likewise benefits from Meta Pixel data and uses it to enhance its own ad targeting abilities.

ii. Defendant's method of transmitting Plaintiff's and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

56. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. 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).

57. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

58. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP

[46] *Meta Pixel*, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last visited June 21, 2024).
[47] *About Meta Pixel*, META, https://www.facebook.com/business/help/742478679120153 (last visited June 21, 2024).

Responses, along with corresponding cookies.[48]

59. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

60. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information. The entity's servers send the HTTP Response, which contains 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 a website.

61. 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.

62. 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.

63. In this way, the Meta Pixel acts much like a traditional wiretap: intercepting and transmitting communications intended only for the website host and diverting them to Facebook.

64. Separate from the Meta Pixel, third parties place cookies in the browsers of web users. These cookies can uniquely identify the user, allowing the third party to track the user as they browse the internet—on the third-party site and beyond. Facebook uses its own cookie to

[48] "Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." *What are cookies?*, CLOUDFLARE, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Aug. 12, 2024).

identify users of a Meta-Pixel-enabled website and connect her activities on that site to her individual identity. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the user associated with the information it has intercepted.

65. With substantial work and technical know-how, internet users can sometimes circumvent these browser-based wiretap technologies. To counteract this, third parties bent on gathering data implement workarounds that are difficult for web users to detect or evade. Facebook's workaround is Conversions API, which "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[49] This makes Conversions API a particularly effective tool because it allows sends Facebook data directly from the website server to Facebook, without relying on the user's web browser. Notably, client devices do not have access to host servers containing Conversions API, and thus, they cannot prevent (or even detect) this transmission of information to Facebook.

66. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the website server, Facebook instructs entities like Culbertson to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[50] Consequently, if a website owner utilizes the Meta Pixel on its website, it is also reasonable to infer that it implemented the Conversions API on its website

[49] *About Conversions API,* META, https://www.facebook.com/business/help/2041148702652965 (last visited June 21, 2024).
[50] *See Best Practices for Conversions API,* META, https://www.facebook.com/business/help/308855623839366 (last visited June 21, 2024).

server(s), in accordance with Facebook's documentation.

67. The Meta Pixel, Conversions API, and other third-party trackers do not provide any substantive content on the host website. Rather, their only purpose is to collect information to be used for marketing and sales purposes.

68. Accordingly, without any knowledge, authorization, or action by a user, a website owner can use its website source code to commandeer its users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Facebook, and others.

69. In this case, Culbertson employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

70. Consequently, when Plaintiff and Class Members visited Defendant's Website and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

iii. Defendant's Other Trackers: Google Analytics, DoubleClick Ads, and Microsoft Clarity.

74. Defendant also employed other trackers, including Google Analytics, DoubleClick Ads, and Microsoft Clarity, which, on information and belief likewise transmitted Plaintiff's and the Class Members' Private Information to third parties without Plaintiff's and Class Members' knowledge or authorization.

75. Most basically, "Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business."[51] Once a business implants the Google Analytics tracking measurement code on a its website, every time a user visits

[51] *Analytics Help, Introduction to Analytics How Google Analytics works*, GOOGLE https://support.google.com/analytics/answer/12159447?hl=en&ref_topic=14089939&sjid=3016588406699844463-NC (last visited Aug. 12, 2024).

a webpage, the tracking code will collect information about how that user interacted with the page.[52]

76. Google Analytics allows Defendant to track and share with Google (1) who uses its website; (2) what is performed on its website; (3) when users visit its website; (4) where on the website users perform these actions; and (5) how users navigate through the website to perform these actions. Google gathers this information using trackers embedded on Culbertson's Website and generates corresponding reports.[53]

77. To help Google generate reports (usually in realtime), trackers embedded in a website send Google (1) information about the user's device; (2) client- and user-specific identifiers; and (3) information about what event the user performed.

78. According to Google, "Google Tag Manager is a tag management system (TMS) that allows you to quickly and easily update measurement codes and related code fragments collectively known as ***tags*** on your website or mobile app. Once the small segment of Tag Manager code has been added to your project, you can safely and easily deploy analytics and measurement tag configurations from a web-based user interface."[54]

79. As Google goes onto describe:

> When Tag Manager is installed, your website or app will be able to communicate with the Tag Manager servers. You can then use Tag Manager's web-based user interface to set up tags, establish ***triggers*** that cause your tag to fire when certain events occur, and create ***variables*** that can be used to simplify and automate your tag configurations.
>
> A collection of tags, triggers, variables, and related configurations installed on a

[52] *Id*.
[53] *See generally A big list of what Google Analytics can & cannot do*, MARKETLYRICS, https://marketlytics.com/blog/list-of-things-google-analytics-can-and-cannot-do/ (last visited Aug. 12, 2024).
[54] *See Introduction to Tag Manager*, GOOGLE, https://support.google.com/tagmanager/answer/6102821?hl=EN#:~:text=Google%20Tag%20Manager%20is%20a,your%20website%20or%20mobile%20app (last visited Aug. 12, 2024).

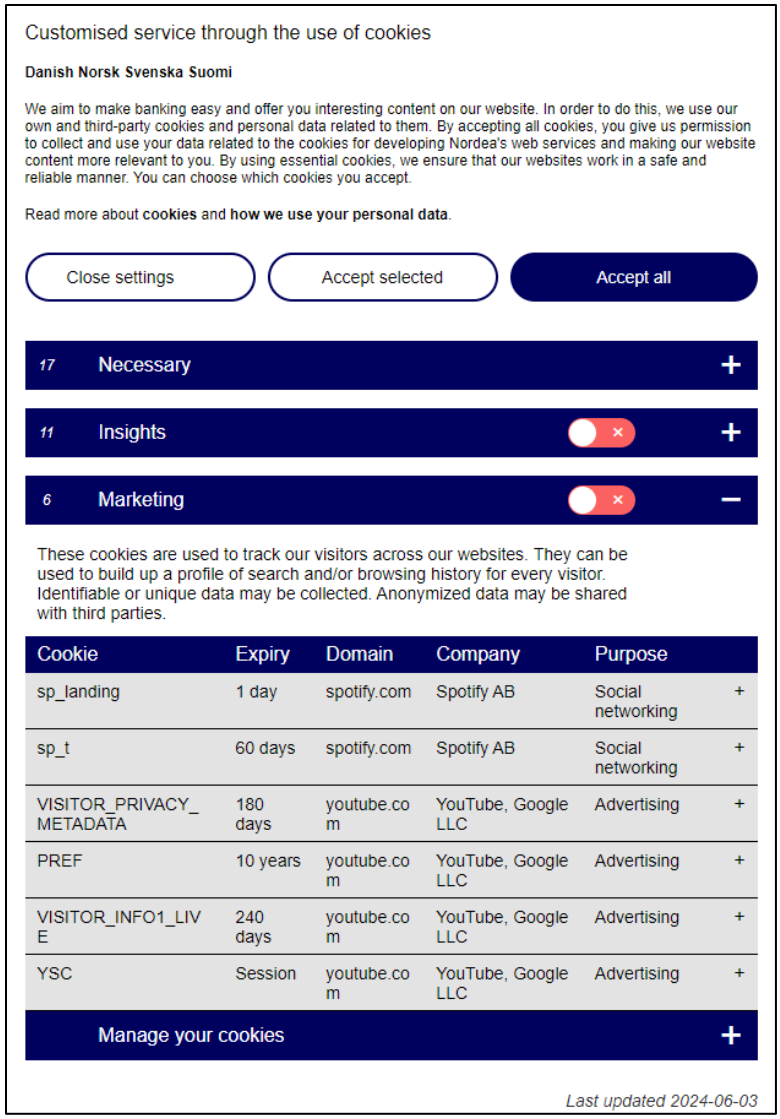
> given website or mobile app is called a ***container***. A Tag Manager container can replace all other manually-coded tags on a site or app, including tags from Google Ads, Google Analytics, Floodlight, and 3rd party tags.[55]

80. Defendant also utilizes Double Click Ads. Google's DoubleClick is "an integrated ad technology platform that enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns."[56]

81. DoubleClick includes DoubleClick Digital Marketing Manager ("Ad serving and management solutions for your digital advertising campaigns, including trafficking and reporting"), Google Analytics, and more.[57]

82. Information gathered through DoubleClick can be used by Google to personalize the advertisements users are targeted with across the web. *See*, e.g., https://www.nordea.com/en/doubleclick-cookies:

[55] *Id.*
[56] *DoubleClick Digital Marketing*, GOOGLE, https://support.google.com/faqs/answer/2727482?hl=en (last visited Aug. 12, 2024).
[57] *Id.*



Customised service through the use of cookies

Danish Norsk Svenska Suomi

We aim to make banking easy and offer you interesting content on our website. In order to do this, we use our own and third-party cookies and personal data related to them. By accepting all cookies, you give us permission to collect and use your data related to the cookies for developing Nordea's web services and making our website content more relevant to you. By using essential cookies, we ensure that our websites work in a safe and reliable manner. You can choose which cookies you accept.

Read more about **cookies** and **how we use your personal data**.

Close settings | Accept selected | Accept all

17 Necessary +

11 Insights +

6 Marketing −

These cookies are used to track our visitors across our websites. They can be used to build up a profile of search and/or browsing history for every visitor. Identifiable or unique data may be collected. Anonymized data may be shared with third parties.

Cookie	Expiry	Domain	Company	Purpose	
sp_landing	1 day	spotify.com	Spotify AB	Social networking	+
sp_t	60 days	spotify.com	Spotify AB	Social networking	+
VISITOR_PRIVACY_METADATA	180 days	youtube.com	YouTube, Google LLC	Advertising	+
PREF	10 years	youtube.com	YouTube, Google LLC	Advertising	+
VISITOR_INFO1_LIVE	240 days	youtube.com	YouTube, Google LLC	Advertising	+
YSC	Session	youtube.com	YouTube, Google LLC	Advertising	+

Manage your cookies +

Last updated 2024-06-03

83. Lastly, Culbertson utilized Microsoft Clarity. Microsoft Clarity captures anonymous user data and converts it into visual insights that reveals what users are doing, where they are clicking, and how they interacting with content on a web page.[58]

84. On information and belief, through these other trackers, Google Analytics DoubleClick Ads, and Microsoft Clarity, Culbertson transmitted Plaintiff's and the Class Members' Private Information to Facebook and those other third parties without Plaintiff's and

[58] Tara Porter, *What Is Microsoft Clarity: A Comprehensive Guide*, VISUALSP (July 6, 2024), https://www.visualsp.com/blog/what-is-microsoft-clarity/.

Class Members' knowledge or authorization.

iv. Culbertson Violated Its Own Privacy Policy

85. Defendant maintains and is covered by a Notice of Privacy Practices[59] (the "Privacy Policy") which is posted on Culbertson's Website.

86. On information and belief, Culbertson does not have a separate privacy policy applicable to its Website.

87. Defendant's Privacy Policy states, "[t]his notice describes how medical information about you may be used and disclosed and how you can get access to this information. **Please review it carefully**."[60]

88. Therein, Culbertson goes onto acknowledge, represent, and promise that, "[i]n these cases we never share your information unless you give us written permission: • Marketing purposes • Sale of your information…"[61]

89. Moreover, in its Privacy Policy, Culbertson provides enumerated purposes for which it may disclose patients' health information/PHI, *inter alia*: to treat you ("We can use your health information and share it with other professionals who are treating you."); to run its organization ("We can use and share your health information to run our practice, improve your care, and contact you when necessary."); to bill for services; to "[h]elp with public health and safety issues" (including "• Preventing disease • Helping with product recalls • Reporting adverse reactions to medications • Reporting suspected abuse, neglect, or domestic violence • Preventing or reducing a serious threat to anyone's health or safety"); to do research; to comply with the law ("• We will share information about you if state or federal laws require it, including with the

[59] *Privacy Policy*, Sarah D. Culbertson Memorial Hospital (Aug. 1 2019), https://cmhospital.com/about-us/privacy-policy, **attached as Exhibit B.**
[60] *Id.*
[61] *Id.*

Department of Health and Human Services if it wants to see that we're complying with federal privacy law."); to respond to organ and tissue donation requests; to work with a medical examiner or funeral director; to "[a]ddress workers' compensation, law enforcement, and other government requests[;]" and to "[r]espond to lawsuits and legal actions" ("We can share health information about you in response to a court or administrative order, or in response to a subpoena.").[62]

90. None of the foregoing purposes include the disclosure of patients' PHI/Private Information without authorization to third parties uninvolved in her treatment, for marketing purposes.

91. Despite its representations in Privacy Policy, Defendant does indeed transfer Private Information including PHI to third parties for marketing purposes, without written authorization, and without patients' knowledge. Using the Meta Pixel and other tracking technologies, such as Google Analytics, DoubleClick Ads, and Microsoft Clarity, Culbertson used and disclosed Plaintiff's and Class Member's Private Information and confidential communications to Facebook, and other unauthorized third parties, without written authorization, in violation of its Privacy Policy.

v. Defendant Unauthorizedly Disclosed Plaintiff's and the Class's Private Information via the Meta Pixel and Related Tracking Technologies

92. Culbertson disclosed Plaintiff's and Class Members' Private Information and confidential communications to Facebook and other third parties including Google, and Mircosoft, via the Meta Pixel and other tracking technologies, without Plaintiff's and Class Members' authorization, for marketing purposes.

93. On information and belief, the information that Defendant sent to Facebook

[62] *Id.*

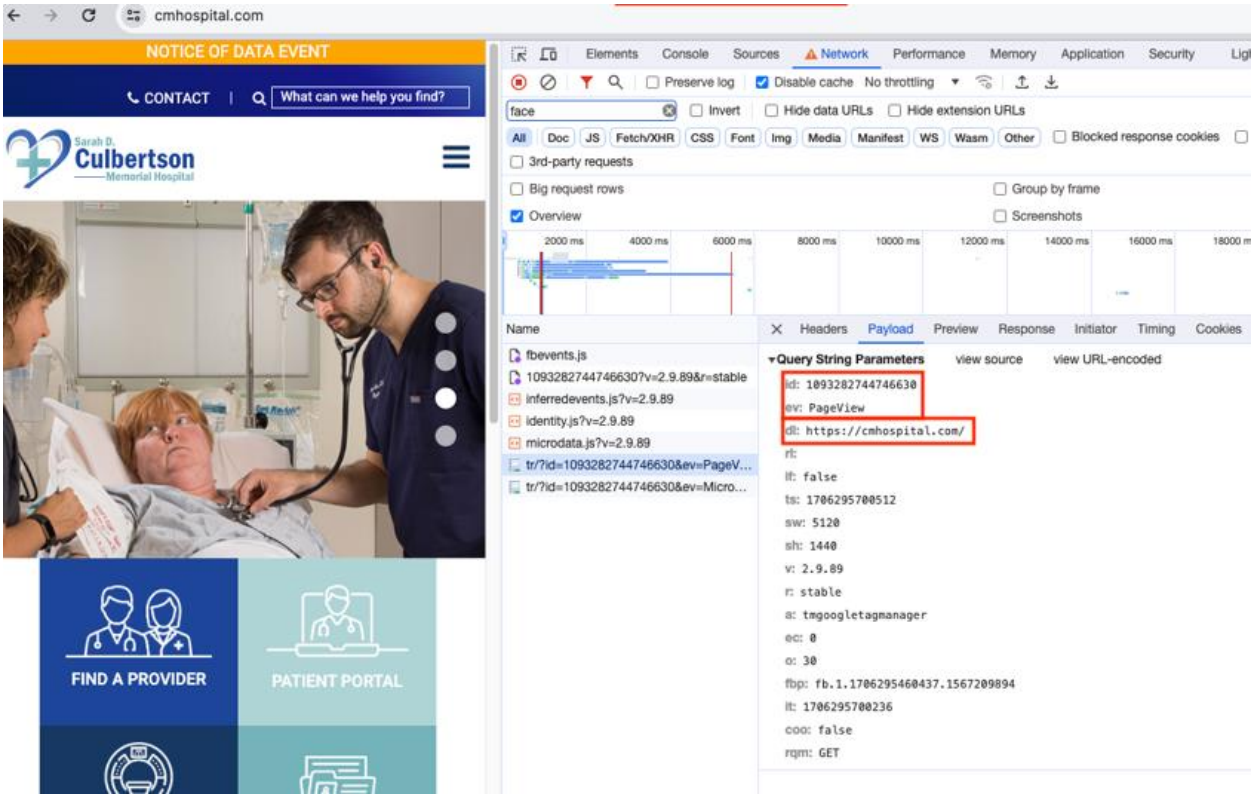
included the Private Information that Plaintiff and the Class Members submitted to Defendant's Website and Online Platforms, including, *inter alia*: her browsing activities; the pages they viewed and the buttons they clicked; information concerning their statuses as patients such as patient portal activities; information concerning their medical concerns such as the providers they searched for and viewed, and the medical services they viewed; as well as their identifying information, such as IP addresses and identifying cookies.

94. On information and belief, Culbertson has disclosed patients' data to Facebook via Meta Pixel with ID 1093282744746630 ("Pixel 1") from at least June 23, 2021 through as recently as October 31, 2023.

95. On information and belief, Culbertson has disclosed patients' data to Google via a Google Tag Manager ("GTM") with account with ID GTM-P99ZF6J from at least October 19, 2013 through as recently as October 31, 2023.

96. On information and belief, Culbertson first installed a Google Analytics tracker with ID UA-33430411 ("UA1") no later than October 19, 2013. Culbertson continued to install UA1 directly via HTML until at least October 31, 2023.

97. Culbertson used Pixel 1 to track patients' activities and disclosed information about patients to Facebook. Culbertson transmitted PageView and Microdata events to Facebook about patients' activities on the Website as soon as they arrived on Culbertson's homepage.



98. The PageView and Microdata events inform Facebook that the patients were viewing the page on "https://cmhospital.com/" with the Microdata event further disclosing that the patients were learning about Culbertson, which is a "full-service critical access hospital," offering "inpatient, outpatient, and emergency services, obstetric care, surgical care, extensive rehabilitation programs," and more.[63]

99. As patients continued to browse Culbertson's website beyond the homepage, Culbertson continued to disclose information about the patients through PageView, Microdata, and SubscribedButtonClick events. Through these Meta Pixel events, Culbertson disclosed information about patients':

(i) keyword search activities;

(ii) (ii) physician search activities;

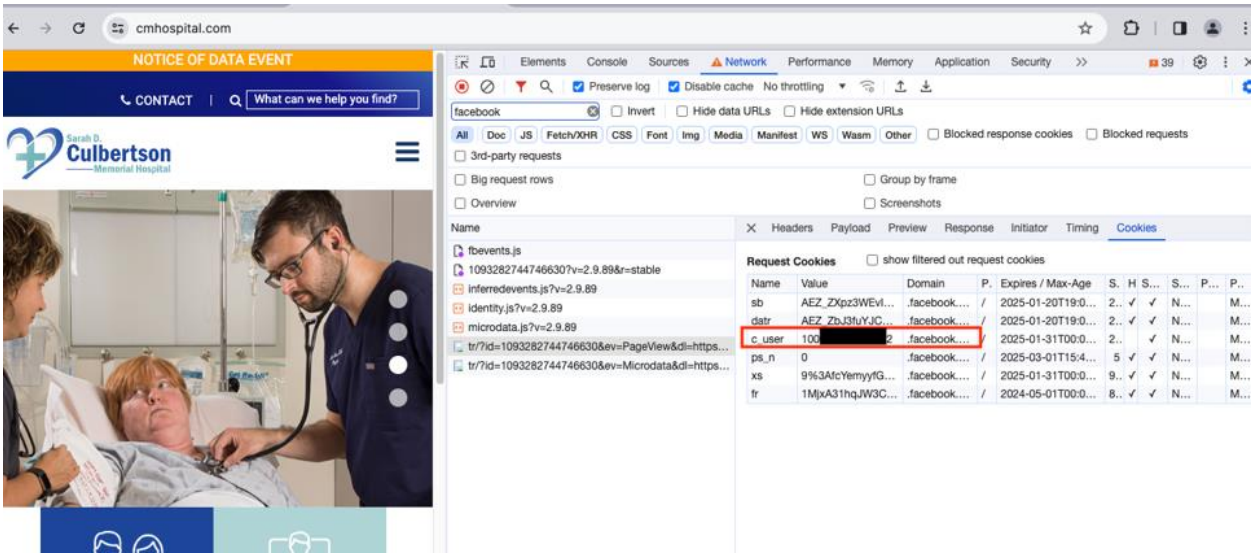
[63] *See* https://cmhospital.com/ (last visited Aug. 12, 2024).

(iii) (iii) services browsing activities;

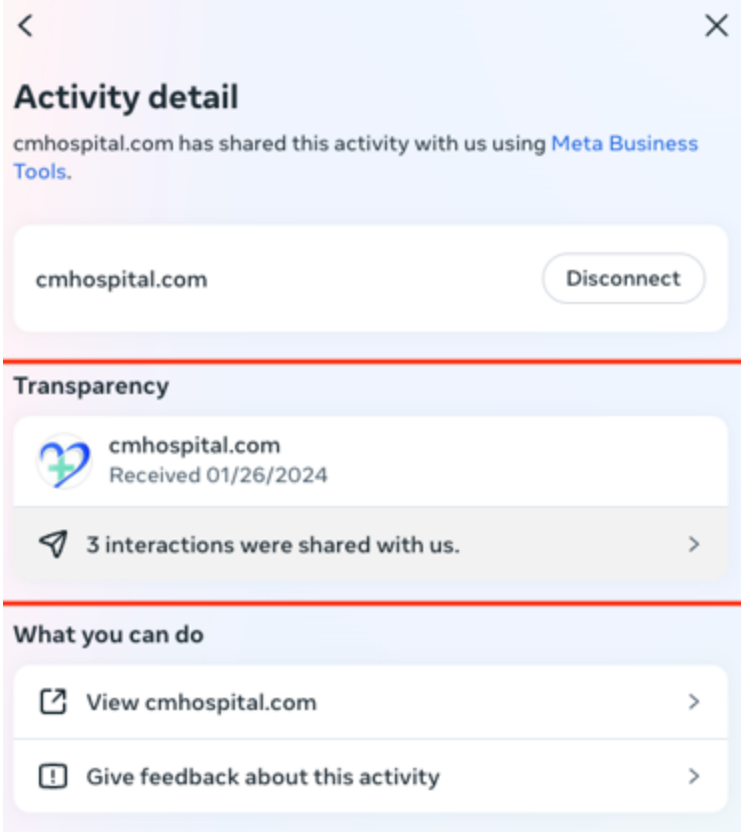
(iv) (iv) bill pay activities; and,

(v) (v) patient portal activities.

100. In each of the Meta Pixel events that Culbertson sent to Facebook, Culbertson included the "c_user" cookie, which Facebook uses to identify users. Facebook could therefore connect cookie data that Culbertson transmitted with specific patients.



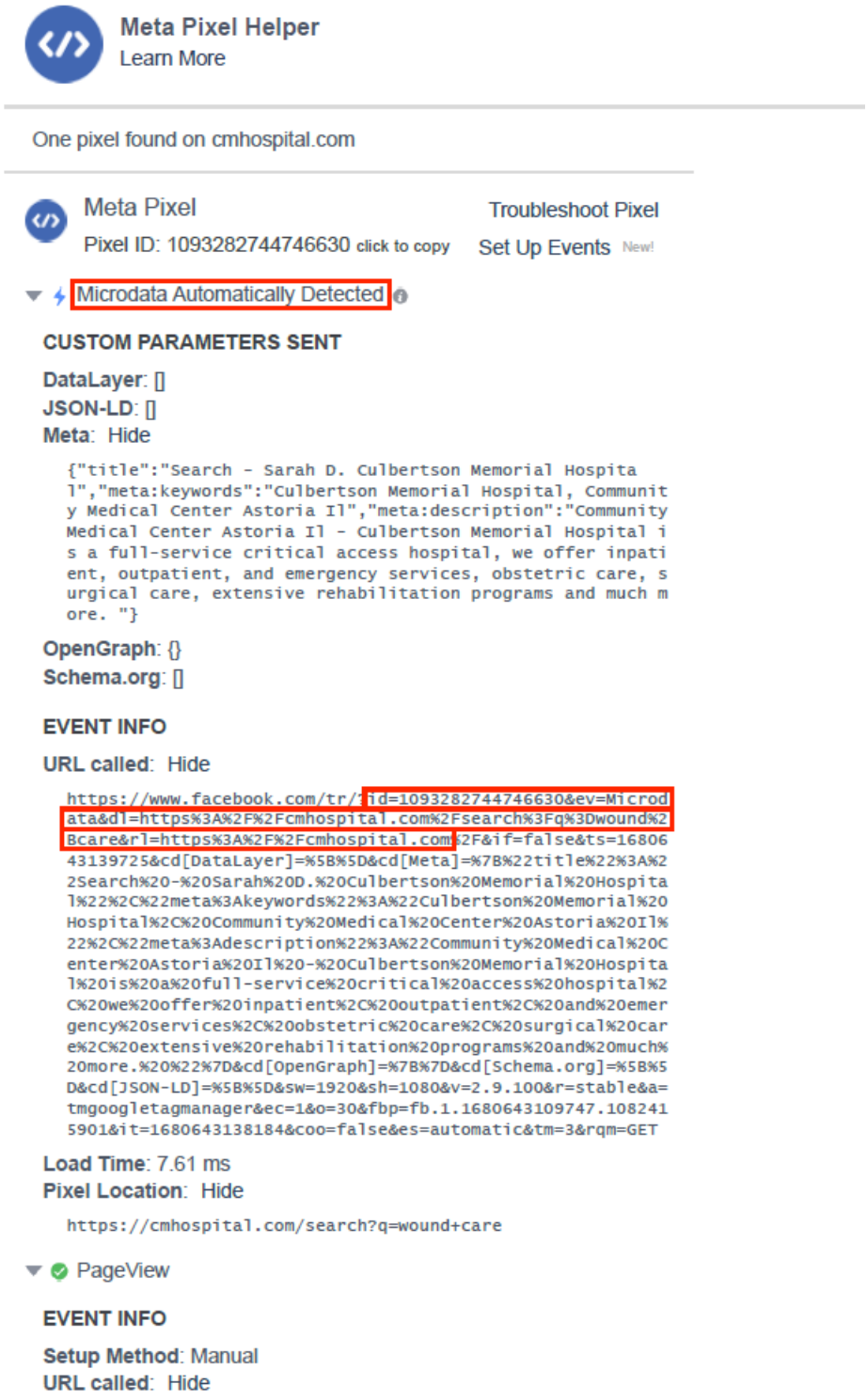
101. Furthermore, Facebook's "Your activity off Meta technologies" report confirms that Facebook received the data Culbertson shared with Facebook.



Culbertson Disclosed Patients' Keyword Search Activities

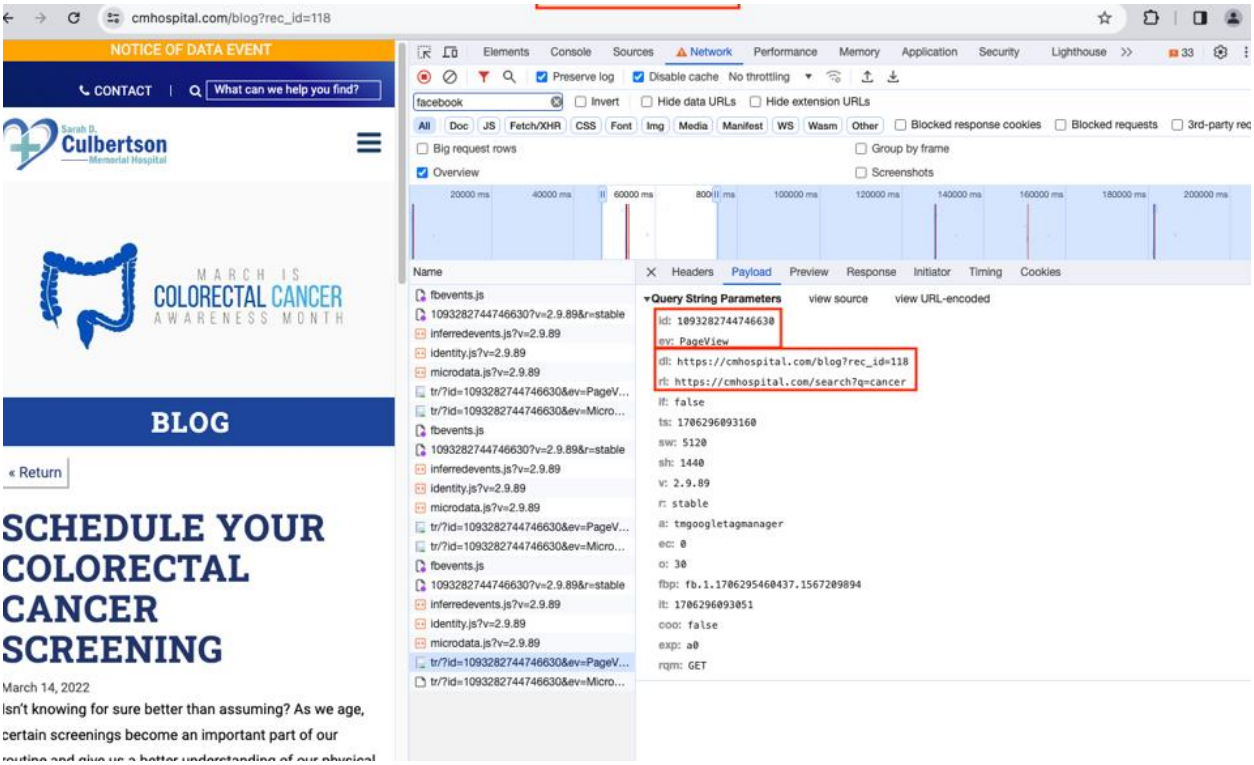
102. When patients conducted keyword searches and physician searches on Culbertson's website, Culbertson disclosed information about those searches to Facebook.

103. From the homepage, patients could conduct keyword searches. For example, a patient could search for the keywords such as "wound care," or "cancer." Upon the patient's search, Culbertson sent PageView and Microdata events informing that the patient conducted a keyword search.



104. Culbertson also tracked patients' activities as they interacted with their keyword search results, disclosing which pages they viewed and her contacts with Culbertson.

105. For example, if a patient searched for the keyword, "cancer," when the patient clicked to view a blog about scheduling a colorectal cancer screening from her search result page, Culbertson transmitted a pair of Pageview and Microdata events, which informed Facebook that the patient navigated to a blog post after conducting a search for cancer, and the Microdata event disclosed that the patient was learning about the importance of scheduling "Your Colorectal Cancer Screening."



106. As the patient clicked to call Culbertson from the blog page, Culbertson then transmitted a SubscribedButtonClick event, which, together with the Microdata event described in paragraph 105 *supra*, revealed that:

(i) the patient clicked to call CMH on the colorectal cancer screening blog page;

(ii) the phone number that the patient dialed; and,

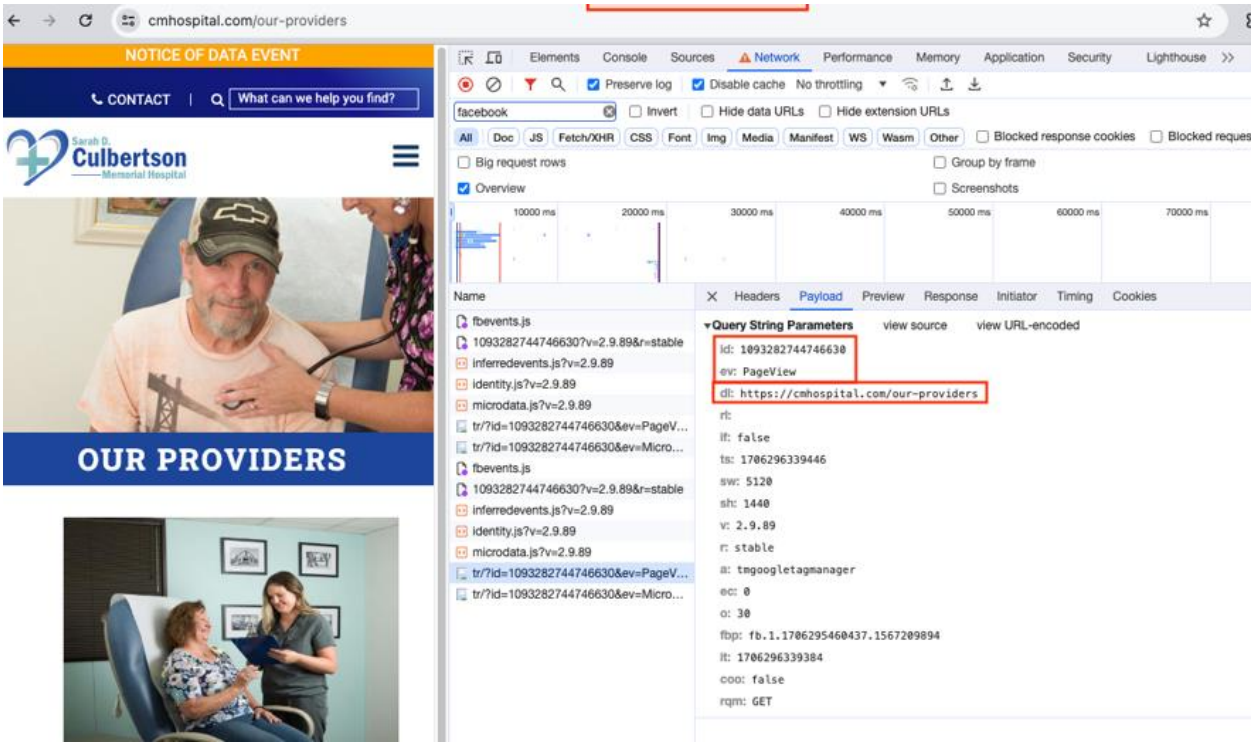
(iii) that the patient clicked to call Culbertson after conducting a search for

cancer.

Culbertson Disclosed Patients' Physician Searches

107. Not only did Culbertson disclose data about patients' keyword searches, but it also shared information with Facebook when patients conducted searches for physicians.

108. As patients landed on the pages to search for physicians, Culbertson transmitted PageView and Microdata events disclosing the patients' activities.



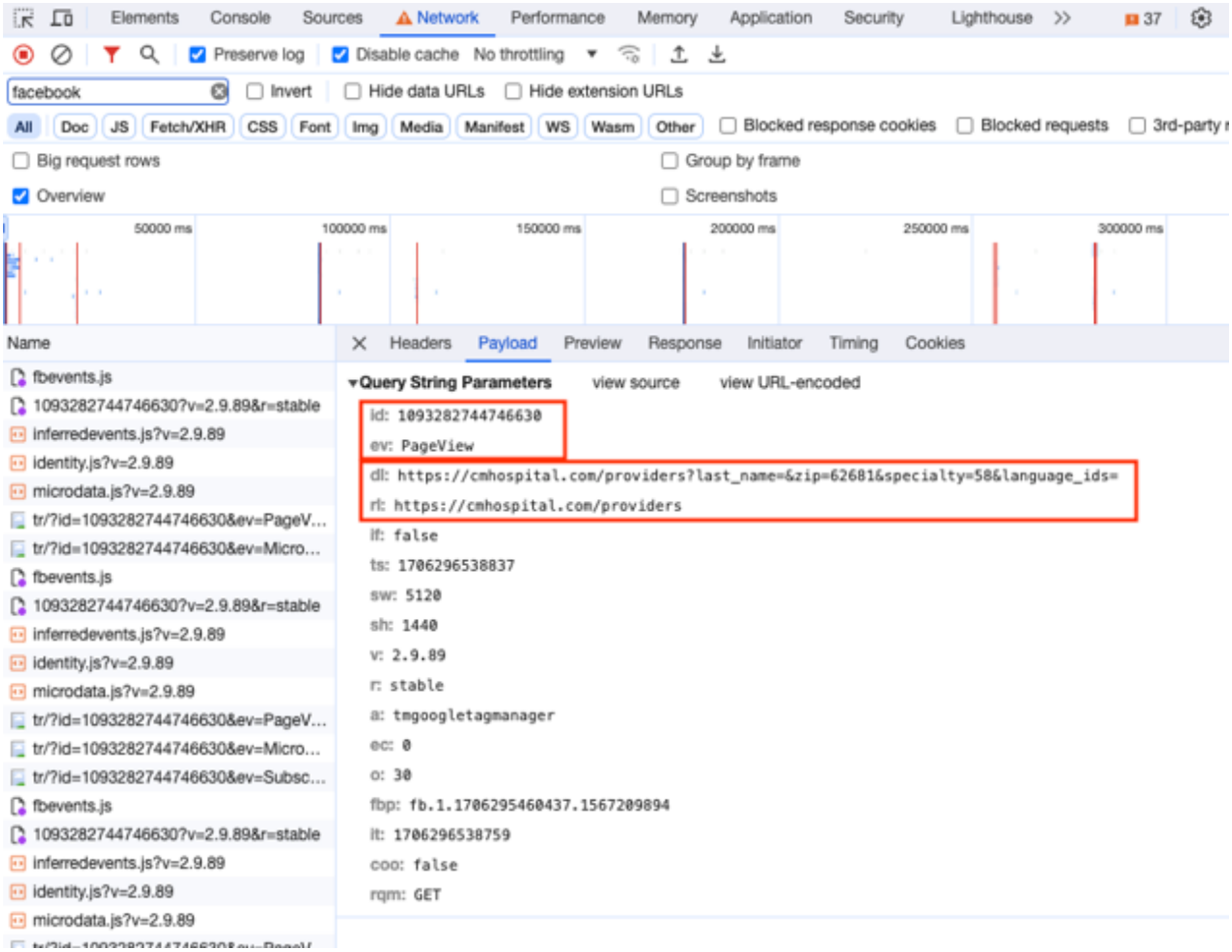
109. Culbertson also disclosed when a patient clicked to access the provider search function via a SubscribedButtonClick event.

110. As a patient clicked the button to search for physicians based on her parameters, Culbertson transmitted a SubscribedButtonClick event which informed Facebook the patient clicked "SEARCH" to "Find a Provider."

111. The SubscribedButtonClick event also informed Facebook of the parameters by which the patient searched for a physician: physician last name, zip code, medical specialty, and

language.

112. For instance, the patient could search for physicians near zip code, 62681 with a specialty in cancer care, upon which CMH transmitted PageView and Microdata events.



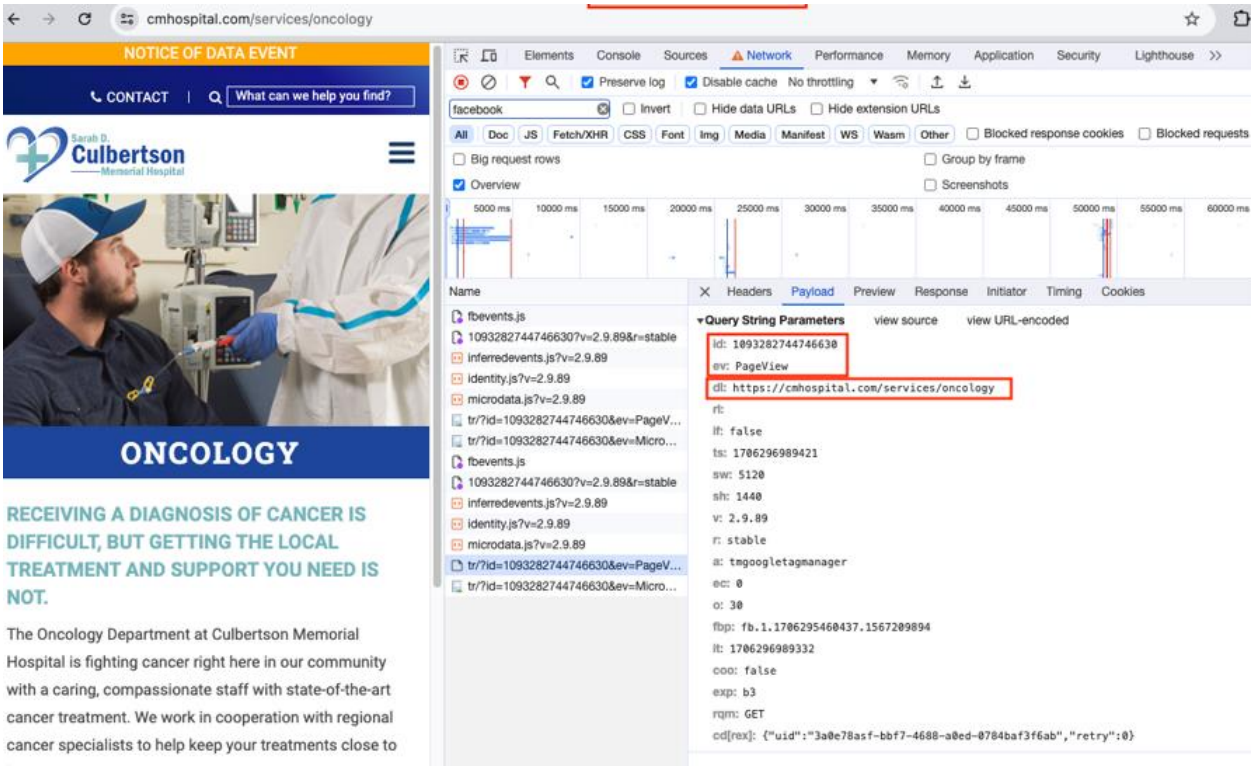
Defendant Disclosed Patients' Browsing Activities

80. Culbertson shared patients' browsing activities as they explored medical services offered.

81. When a patient loaded the page for Culbertson's services, Culbertson sent PageView and Microdata events, both of which inform Facebook that the patient was on the page, "https://cmhospital.com/services/."

82. As the patient continued to explore more detailed pages about specific medical services offered by Culbertson, Culbertson continued to transmit Pixel events with details about the patient's activities.

83. For example, when a patient navigated to the Oncology page, CMH transmitted a pair of PageView and Microdata events informing Facebook the patient was on the page for "services/oncology," where they can "Learn about the Oncology department at Culbertson Memorial Hospital and the quality cancer care that is offered by our caring, compassionate staff."



84. When the patient clicked to call Culbertson from the Oncology page, Culbertson sent a SubscribedButtonClick event which revealed that the patient clicked to call "tel:(217) 322-4321" while they were on the page, "Oncology – Sarah D. Culbertson Memorial Hospital."

Culbertson Disclosed Patients' Bill Pay Activities

85. Culbertson also shared patients' bill pay activities with Facebook.

86. Upon a patient's navigation to the Online Bill Pay page, Culbertson sent PageView

and Microdata events. Both events revealed that the patient was on the page for "patients-and-visitors/online-billpay," and the Microdata event informed Facebook that the patient was on a page where they could "Pay your bill for Culbertson Memorial Hospital online."

87. As the patient clicked a button to pay her medical bills, Culbertson then sent a SubscribedButtonClick event, which reveals the patient clicked to "Submit Payment," to pay her medical bill.

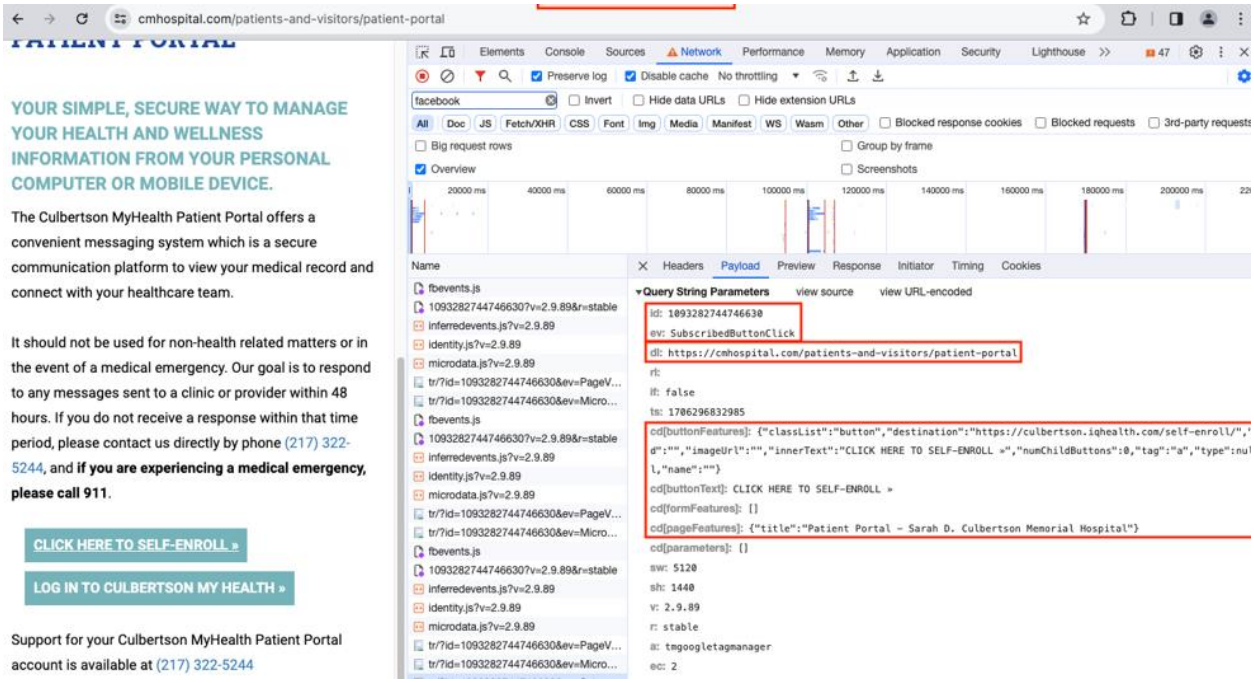
Culbertson Disclosed Patients' Patient Portal Activities

88. Culbertson shared information with Facebook about patients' patient portal activities.

89. As a patient opened Culbertson's page about its patient portal ("Patient Portal Landing Page"), Culbertson transmitted PageView and Microdata events informing Facebook that the patient was on the page, "https://cmhospital.com/patients-and-visitors/patient-portal."

90. The Microdata event provides Facebook with more details about the page, including that the patient could "Log in to the Culbertson Memorial Hospital patient portal using your username and password in order to get access to your personal health record."

91. Once the Patient Portal Landing Page loaded, the patient could click on various buttons to access either the patient portal or to enroll for the patient portal. Each of these events triggered a SubscribedButtonClick event, disclosing that the patient "CLICK[ED] HERE TO SELF ENROLL" or clicked to "LOG IN TO CULBERTSON MY HEALTH," respectively.



92. The Patient Portal Landing Page has changed over time. For instance, as of April 4, 2023, the page presented various patient portals onto which patients could log in.

93. As of April 4, 2023, Culbertson still disclosed when a patient clicked to access the various patient portals presented. For example, when a patient clicked to access Culbertson's hospital patient portal, Culbertson sent a SubscribedButtonClick event informing the patient clicked to access the "HOSPITAL PATIENT PORTAL."

94. Similarly, when the patient clicked to load Culbertson's clinic patient portal, Culbertson transmitted a SubscribedButtonClick event informing Facebook that the patient clicked to access the "CLINIC PATIENT PORTAL."

95. Culbertson could have chosen not to use the Meta Pixel and other tracking technology such as Google Analytics, DoubleClick Ads, and Microsoft Clarity, or it could have configured its trackers to limit the information that it communicated to third parties, but it did not. Instead, it intentionally took advantage of these trackers' features and functions, resulting in the Disclosure of Plaintiff' and Class Members' Private Information.

96. Defendant used and disclosed Plaintiff's and Class Members' Private Information to Facebook, Google, Microsoft, and potentially others, for the purpose of marketing its services and increasing its profits and reducing its marketing costs.

97. On information and belief, Culbertson shared, traded, or sold Plaintiff's and Class Members' Private Information with Facebook in exchange for improved targeting and marketing services and reduced marketing costs.

98. Plaintiff and the proposed Class Members never consented, agreed, authorized, or otherwise permitted Culbertson to intercept her communications or to use or disclose her Private Information for marketing purposes. Plaintiff and the proposed Class Members, patients of Culbertson, were never provided with any written notice that Defendant disclosed its patients' Protected Health Information to Facebook, Google, Microsoft, and others, nor were they provided any means of opting out of such disclosures. Culbertson nonetheless knowingly disclosed Plaintiff's and Class Members' Private Information including Protected Health Information to unauthorized entities.

99. Plaintiff and Class Members relied on Culbertson to keep her Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

100. Furthermore, Culbertson actively misrepresented it would preserve the security and privacy of Plaintiff's and Class Members' Private Information. In actuality, Culbertson shared data about Plaintiff's and Class Members' activities on the Online Platforms alongside identifying details about the Plaintiff and Class Members, such as her IP addresses.

101. By law, Plaintiff and the Class Members are entitled to privacy in their Private Information, including Protected Health Information, and confidential communications.

Culbertson deprived Plaintiff and Class Members of their privacy rights when it; (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information, (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook and others, and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining her express written consent.

B. Plaintiff Hannant's Experience

102. Plaintiff Alana Hannant has been a patient of Defendant for approximately two years. She received healthcare services from Culbertson and physicians in Culbertson's network, including imaging and a biopsy.

103. Plaintiff Hannant used Culbertson's Website and Online Platforms beginning on or around November 2021 and last in September 2023.

104. Plaintiff Hannant used the Website and Online Platforms to: find a specific physician, to research treatments, including information related to an MRI test, to search for treatment information; to find out how to obtain medical records; to use the patient portal, and more.

105. After Plaintiff Hannant used the Online Platforms, advertisements for MRI tests and advertisements for doctors treating back problems began appearing in her Facebook feed.

106. Plaintiff Hannant relied on Defendant's Website and Online Platforms to communicate confidential patient information. She discovered that Defendant was unauthorizedly disclosing her Private Information to Facebook via the Meta Pixel and other trackers in November 2023.

107. Plaintiff accessed Defendant's Online Platforms at Culbertson's direction and

encouragement in relation to her past, present, and future health and healthcare needs.

108. Plaintiff reasonably expected that her online communications with Culbertson were confidential, solely between herself and Culbertson, and that, as such, those communications would not be transmitted to or intercepted by a third party.

109. Plaintiff provided her Private Information to Defendant and trusted that the information would be safeguarded according to Culbertson's Privacy Policy and the law.

110. On information and belief, through its use of the Meta Pixel and other tracking technologies, Culbertson disclosed to Facebook:

a. the pages and content Plaintiff viewed;

b. plaintiff' seeking of medical treatment;

c. plaintiff' status as a patient;

d. information regarding Plaintiff' patient portal activity;

e. the specialties of the medical providers Plaintiff searched for and viewed;

f. the names of the medical providers Plaintiff searched for and viewed;

g. the search results that Plaintiff clicked on;

h. the medical services Plaintiff viewed; and,

i. Plaintiff' identity via her IP addresses and/or "c_user" cookie and/or Facebook ID.

111. By failing to receive the requisite consent, Culbertson breached confidentiality and unlawfully disclosed Plaintiff' Private Information.

112. As a result of Culbertson's Disclosure of Plaintiff's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff have suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of her Private Information; unauthorized access of her Private Information by third parties;

b. Plaintiff now receive targeted health-related advertisements on Facebook, reflecting her private medical treatment information;

c. Plaintiff paid Culbertson for medical services and the services she paid for included reasonable privacy and data security protections for her Private Information, but Plaintiff did not receive the privacy and security protections for which she paid, due to Defendant's Disclosures;

d. The portion of Culbertson's revenues and profits attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

e. The portion of Culbertson's savings in marketing costs attributable to collecting Plaintiff' Private Information without authorization and sharing it with third parties;

f. The portion of Culbertson's revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff as a result of collecting Plaintiff' Private Information without authorization and sharing it with third parties;

g. Value to Plaintiff of surrendering her choice to keep her Private Information private and allowing Culbertson to track her data. The amount of these damages can be based on a baseline monthly compensation provided to participants in a Google consumer research study, the Ipsos Screenwise Panel where the baseline compensation to participants was $3 per device

per month;

h. Embarrassment, humiliation, frustration, and emotional distress;

i. Decreased value of Plaintiff's Private Information;

j. Lost benefit of the bargain;

k. Increased risk of future harm resulting from future use and disclosure of her Private Information; and

l. Statutory damages.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

113. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[64] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

114. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[65]

[64] Kurt Wagner & Bloomberg, *Facebook Admits Another Blunder with User Data*, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.
[65] *Report on Investigation of Facebook Inc. Data Privacy Concerns*, NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.

115. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that matter, more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing her data with Facebook.[66] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing her data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[67]

116. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[68]

117. In June 2022, an investigation by The Markup[69] revealed that the Meta Pixel was

[66] Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.
[67] *Id.*
[68] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does with Your Data*, or Where It Goes: Leaked Document, VICE (June 21, 2024) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[69] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed June 21, 2024).

embedded on the websites of 33 of the top 100 hospitals in the nation.[70] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[71] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[72]

118. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of her allergic reactions, details about her upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[73]

119. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on her websites, The Markup identified seven health systems that had installed the Meta Pixel inside her password-protected patient portals.[74]

120. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[75]

---

[70] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*

D. Defendant Violated HIPAA Standards

121. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[76]

122. If a HIPAA covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate agreement ("BAA") or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information.[77]

123. Facebook will not sign a BAA and is therefore is not HIPAA complaint.[78]

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

125. 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.[79]

---

[76] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[77] *Covered Entities and Business Associates,* U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Aug. 12, 2024).
[78] Liyanda Tembani, *Is Facebook HIPAA compliant? (Update 2024)*, PAUBOX, https://www.paubox.com/blog/facebook-hipaa-compliant (last visited Aug. 12, 2024).
[79] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*,

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

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[80]

127. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology (the "December 2022 Bulletin").[81]

128. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[82]

129. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with

---

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[80] *Marketing*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[81] *See* archived version of the December 2022 Bulletin at *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Dec. 1, 2022), https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited June 21, 2024).

[82] *Id.*

> such vendors. **Regulated 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**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.[83]

130. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel is a violation of HIPAA Rules.

E. Defendant Violated FTC Standards, and the FTC and HHS Take Action

131. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[84]

132. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online

[83] *Id.* (emphasis in original) (internal citations omitted).
[84] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), attached as Exhibit A.

activities."[85]

133. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules"[86] and that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes."[87]

134. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[88]

135. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health]

[85] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.
[86] *Id.*
[87] *Id.*
[88] *Statement of the Commission: On Breaches by Health Apps and Other Connected Devices*, U.S. FED. TRADE COMMISSION, (Sept. 15, 2021) https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf) (emphasis added).

information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[89]

136. As such, the FTC and HHS have expressly stated that conduct like Defendant's runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

137. On March 18, 2024, HHS updated its December 2022 bulletin in the "March 2024 Bulletin," expanding the circumstances in which HHS would consider information from any unauthenticated website visitor to be considered PHI, and its disclosure to be a violation of HIPAA.[90,91]

138. The March 2024 Bulletin added guidance on when the disclosure of individually identifiable health information ("IIHI") is impermissible under HIPAA, explaining that: "the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI ***if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care***."[92]

139. However, in contrast, when a user visits a website related to his or her past, present,

---

[89] *See, e.g., U.S. v. Easy Healthcare Corp*., Case No. 1:23-cv-3107 (N.D. Ill. 2023); *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023),; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023); *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021).

[90] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH AND HUMAN SVCS. OFFICE FOR CIVIL RIGHTS (Dec. 1, 2022, updated Mar. 18, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[91] On June 20, 2024, in *American Hospital Association, et al. v. Xavier Becerra, et al.*, Case No. 4:23-cv-01110-P (N.D. Tx., Jun. 20, 2024, Doc. 67), the U.S. District Court for the Northern District of Texas vacated HHS's March 14, 2024 Bulletin as to the "Proscribed Combination," *but* acknowledged that the Proscribed Combination could be PHI in certain circumstances.

[92] *Supra*, n.92 (bold, italicized emphasis added).

or future health, health care, or payment for health care, such as "…looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care[,]" such that the disclosure of her information would be PHI, HIPAA rules apply, and that disclosure would be a violation of HIPAA.[93]

F. Defendant Violated Industry Standards

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

141. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Culbertson and its physicians.

142. 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).

143. 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

[93] *Id.*

for which access would be granted.

144. 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 . . . release patient information only in keeping ethics guidelines for confidentiality.

G. Defendant Violated Standards Set Forth in Illinois Law.

171. Under the Illinois Medical Patient Rights Act ("MPRA"), 410 Ill. Comp. Stat. 50/3(d), Plaintiff and Class Members have rights to privacy and confidentiality in her health care.

172. The MPRA provides:

> Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients, except that such information may be disclosed: (1) to the patient, (2) to the party making treatment decisions if the patient is incapable of making decisions regarding the health services provided, (3) for treatment in accordance with 45 CFR 164.501 and 164.506, (4) for payment in accordance with 45 CFR 164.501 and 164.506, (5) to those parties responsible for peer review, utilization review, and quality assurance, (6) for health care operations in accordance with 45 CFR 164.501 and 164.506, (7) to those parties required to be notified under the Abused and Neglected Child Reporting Act or the Illinois Sexually Transmissible Disease Control Act, or (8) as otherwise permitted, authorized, or required by State or federal law. This right may be waived in writing by the patient or the patient's guardian or legal representative, but a physician or other health care provider may not condition the provision of services on the patient's, guardian's, or legal representative's agreement to sign such a waiver.

410 Ill. Comp. Stat. 50/3(d).

173. Furthermore, the Illinois Personal Information Protection Act ("IPIPA") protects Plaintiff's and Class Members' Medical Information and Personal Information from unauthorized disclosure. 815 Ill. Comp. Stat. 530/5, /45.

174. Defendant is a "Data Collector" and subject to the provisions of the IPIPA. *See* 815 Ill. Comp. Stat. 530/5.

175. The IPIPA provides that:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 Ill. Comp. Stat. 530/459(a).

176. Defendant's Disclosure of Plaintiff's and Class Members' Private Information to third parties, including Facebook, Google, and Microsoft, and possibly others, through the operation of the Pixel on its Website and Online Platforms violated Plaintiff's and Class Members' rights to privacy and confidentiality in their receipt of healthcare services and fell below the applicable standard for safeguarding the confidential Private Information of Plaintiff and the Class Members.

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

177. 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 marketing and sales purposes, unrelated to patient care.

I. IP Addresses are Personally Identifiable Information

178. Defendant also disclosed and otherwise assisted Facebook and possibly others with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel Google Analytics DoubleClick Ads, and Microsoft Clarity and other tracking technologies.

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

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

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

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

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

184. Under HIPAA, an IP address is 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).

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

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

186. Defendant's use of the Meta Pixel and other tracking technology was for the tortious purpose of invading Plaintiff and Class Members' privacy, breaching its fiduciary duty, and violating HIPAA, all for marketing and profits.

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

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

189. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

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

190. The data concerning Plaintiff and Class Members, collected and shared by Defendant, has tremendous economic value. Data collected via the Meta Pixel, Google Analytics DoubleClick Ads, and Microsoft Clarity and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct her ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[94] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[95] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[96]

191. Plaintiffs had a recognizable property interest in their browsing history. That browsing history has economic value, and by sharing, or facilitating the sharing of, such information with third parties such as Google and Facebook without prior approval, KSB took something of value from Plaintiffs and provided it to third parties without compensating Plaintiffs for the use of their Private Information and data, thus, causing the Plaintiffs economic injury.

192. Plaintiffs' Private Information, which was taken by Defendant without permission, had value even though it was not "for sale." The browsing history and data mined from individuals

[94] *Audience Ad Targeting*, META, https://www.facebook.com/business/ads/ad-targeting (last visited June 21, 2024).
[95] *Id.*
[96] *See How to Create a Lookalike Audience on Meta Ads Manager*, META BUSINESS CENTER, https://www.facebook.com/business/help/465262276878947 (last visited June 21, 2024).

using the internet has significant economic value. If it did not have value, then entire industries that sell and trade this data would not exist. There is an entire data industry and estimates suggests that that industry generates billions of dollars.

193. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[97]

194. This business model is not limited to Facebook. Data harvesting 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 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

195. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[98]

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."[99]

---

[97] *See* Rishi Iyengar, *Here's How Big Facebook's Ad Business Really Is*, CNN (Updated 9:19 AM July 1, 2020), https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html.

[98] *See* Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME, (Jan. 9, 2017 at 9:00 a.m.), https://time.com/4588104/medical-data-industry/.

[99] *See* Christina Farr, *Hospital Execs Say They are Getting Flooded with Requests for Your Health Data*, CNBC, (Dec. 18, 2019 at 8:27 a.m.), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

TOLLING, CONCEALMENT, AND ESTOPPEL

197. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

198. Defendant seamlessly incorporated Meta Pixel and other trackers such as Google Analytics DoubleClick Ads, and Microsoft Clarity into its Website and Online Platforms while providing users with no indication that their Website usage was being tracked and transmitted to third parties. Defendant knew that its Website incorporated Meta Pixel, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, Google, Microsoft, and other third parties.

199. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendant's conduct, because there were no disclosures or other indication that they were interacting with websites employing the Meta Pixel or any other tracking technology.

200. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of Plaintiff's and the Class's Private Information continued unabated up. What is more, Culbertson was under a duty to disclose the nature and significance of its data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

201. Plaintiff brings this nationwide class action on behalf of herself, and on behalf of all other similarly situated persons.

202. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All patients of Defendant residing in the United States whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

203. Further, Plaintiff seeks to represent an Illinois Subclass, defined as:

All patients of Defendant who are Illinois Citizens and whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.

204. The Nationwide Class and Illinois Subclass are collectively referred to as "the Class."

205. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as her immediate family members.

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

207. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23(a)(1)-(4).

208. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendant, and the Class is identifiable within Defendant's records.

209. Ascertainability. Class Members are readily identifiable from information in Defendant's possession, custody, and control.

210. Commonality and Predominance: 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 Plaintiff's and

Class Members' Private Information;

b. whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

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

h. whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendant's conduct breached its duties of care and amounts to negligence;

j. whether Defendant was negligent *per se*;

k. whether Defendant committed invasion of privacy—intrusion upon seclusion;

l. whether Defendant breached its implied contract with Plaintiff and the Class Members; or in the alternate, whether Defendant was unjustly enriched;

m. whether Defendant breached its implied duty of confidentiality;

n. whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.;

o. whether Defendant's conduct violated the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.;

p. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.*;

q. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service");

r. whether Defendant's conduct violated Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq*.;

s. whether Defendant's conduct violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*

t. whether Plaintiff and the Class Members are entitled to damages, including actual, compensatory, and nominal damages;

u. the measure of Plaintiff's and the Class Members' damages; and,

v. whether Plaintiff and the Class Members are entitled to punitive damages.

211. Defendant has engaged in a common course of conduct toward Plaintiff and the Class Members, in that the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully disclosed and accessed in the same way. As set forth above, the common issues arising from Defendant's conduct affecting Class Members predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

212. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use and incorporation of Meta Pixel and other tracking technology.

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

214. Adequacy: 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 Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff have suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

215. Superiority and Manageability: 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 her 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 larger organizations such as 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.

216. 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. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas 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. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

219. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful

use and disclosure and failure to properly secure the Private Information of Plaintiff and the Class Members, Defendant may continue to refuse to provide proper notification to and obtain proper consent from Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

220. Moreover, Defendant has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

221. 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 Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding her 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 the disclosure of patient information;

d. whether Defendant was negligent and/or negligent *per se*;

e. whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

f. whether Defendant breached the contract;

g. in the alternate, whether Defendant was unjustly enriched;

h. whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been used and disclosed to third parties;

i. whether Defendant failed to implement and maintain reasonable security procedures and practices;

j. whether Defendant invaded Plaintiff and the Class Members' privacy;

k. whether Defendant breached its implied duty of confidentiality;

l. whether Defendant violated the Illinois Consumer Fraud and Deceptive Business Practices Act, ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq.*;

m. whether Defendant violated the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq.*;

n. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.*;

o. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service");

p. whether Defendant's conduct violated Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq.*;

q. whether Defendant's conduct violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*; and,

r. whether Plaintiff and the 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
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

222. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

223. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

224. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

225. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiff's and Class Members' Private Information.

226. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way

of data harvesting, advertising, and increased sales.

227. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff' and Class Members' injuries.

228. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or imminently will suffer injury and damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

229. Defendant's breach of its common-law duties to exercise reasonable care and negligence, directly and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation: the unauthorized access of her Private Information by third parties; improper disclosure of her Private Information; receipt of targeted advertisements reflecting private medical information; lost benefit of her bargain; lost value of her Private Information and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost time and money incurred to mitigate and remediate the effects of use of her information, as to targeted advertisements that resulted from and were caused by Defendant's negligence; value to Plaintiff and the Class Members of surrendering her choices to keep their Private Information private and allowing Defendant to track their data; increased risk of future harm resulting from future use and disclosure of Plaintiff' and the Class Members' Private Information; and other injuries and damages as set forth herein. These injuries are ongoing, imminent, immediate, and continuing.

230. Defendant's negligence directly and proximately caused the unauthorized access and Disclosure of Plaintiff's and Class Members' Private Information, PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

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

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

171. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

172. Plaintiff bring this negligence *per se* count in the alternative to her common law negligence claim.

173. Pursuant to the laws set forth herein, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, and Illinois law, including the Illinois Medical Patient Rights Act ("MPRA"), 410 Ill. Comp. Stat. 50/3(d), and the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. 530/5, /45, *et seq*., Defendant was required by law and industry standards to maintain adequate and reasonable data and

cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information.

174. Plaintiff and Class Members are within the class of persons that these statutes and rules were designed to protect.

175. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

176. Defendant owed a duty to timely and adequately inform Plaintiff and Class Members, in the event of their PII and PHI being improperly disclosed to unauthorized third parties.

177. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-parties such as Facebook, and others gaining access to Plaintiff's and Class Members' PII and PHI, and resulting in Defendant's liability under principles of negligence *per se*.

178. Defendant violated its duty under Section 5 of the FTC Act and/or HIPAA by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

179. Plaintiff's and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

180. As a proximate result of Defendant's negligence *per se* and breach of duties as set forth above, Plaintiff and Class Members were caused to, *inter alia*, have her data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking

treatment for specific medical conditions, fear, anxiety and worry about the status of their PII and PHI, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over her PII and PHI, all of which can constitute actionable actual damages.

181. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual, and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence *per se*.

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

COUNT III
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

183. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

184. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and Online Platforms.

185. Plaintiff and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendant to receive and that they understood Defendant would keep private.

186. As set forth above, Defendant disclosed Plaintiff' and the Class Members' Private

Information and confidential communications to Facebook and other third parties, without their authorization or knowledge.

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

188. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations in its Notice of Privacy Practices and elsewhere. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

189. Defendant's Disclosure of PHI coupled with PII—Private Information—is highly offensive to the reasonable person.

190. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights, and other injuries and damages as set forth in the preceding paragraphs.

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

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

193. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff

and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

194. Plaintiff also seek such other relief as the Court may deem just and proper.

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

195. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

196. As a condition of receiving medical care from Defendant, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received.

197. In so doing, Plaintiff and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policy and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen. Implicit in the agreement between Defendant and its patients, Plaintiff and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

198. Culbertson had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Defendant.

199. Defendant had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

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

201. Plaintiff and Class Members fully performed their obligations under the implied

contract with Defendant. Culbertson did not. Plaintiff and Class Members would not have provided their confidential Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control her Private Information for uses other than receiving medical treatment from Defendant.

202. Defendant breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to unauthorized third parties, including Facebook, Google, and Microsoft.

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

204. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) injury-in-fact and damages, including monetary damages; loss of privacy; unauthorized disclosure of Private Information; unauthorized access to Private Information by third parties; use of the Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of Private Information; lost benefit of the bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of their information.

205. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

206. Plaintiff re-allegex and incorporatex the above allegations as if fully set forth herein.

207. This claim is pleaded in the alternative to Plaintiff's breach of implied contract claim.

208. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information—Private Information—that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, for marketing purposes, and for sale or trade with third parties.

209. Plaintiff and Class Members would not have used Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Private Information to third parties.

210. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

211. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy practices and procedures that Plaintiff and Class Members paid for, and those purchases with unreasonable data privacy practices and procedures that they received.

212. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members themselves. Under unjust enrichment principles, it would be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Petition.

213. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of the conduct and the unauthorized Disclosure alleged herein.

COUNT VI
BREACH OF IMPLIED DUTY OF CONFIDENTIALITY
(On Behalf of Plaintiff and the Class)

214. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

215. Plaintiff and Class Members were patients of Defendant and received healthcare services from Defendant.

216. Defendant agreed to keep Plaintiff's and Class Members' Private Information and communications confidential as part of establishing and maintaining the healthcare services in the provider/patient relationship between Defendant and Plaintiff and Class Members.

217. There is a duty of confidentiality implied in every healthcare provider and patient relationship, akin to an implied contract, such that healthcare services providers may not disclose confidential information acquired through the healthcare provider-patient relationship.

218. The implied duty of confidentiality is at least as extensive as Defendant's statutory obligations as a healthcare services provider to maintain patient confidentiality.

219. Under the Illinois Medical Patient Rights Act, "health care provider[s]" must "refrain from disclosing the nature or details of services provided to patients." 410 Ill. Comp. Stat. 50/3.

220. Under 735 ILCS 5/8-802, "[n]o physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character."

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

222. Plaintiff and Class Members performed all required conditions of their implied contracts with Defendant.

223. Defendant breached the implied duty of confidentiality to Plaintiff and Class Members by intentionally deploying Pixels on its Website and Online Platforms that caused the transmission of Private Information including PII, PHI, and confidential communications to third parties, including Facebook.

224. Plaintiff seekx all monetary and non-monetary relief allowed by law.

COUNT VII
VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.
(On Behalf of Plaintiff and the Class, and the Illinois Subclass)

225. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

226. The Illinois Consumer Fraud and Deceptive Practices Act ("CFDPA") makes it unlawful to employ "[u]nfair methods of competitions and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in [this section] . . . in the conduct of any trade or commerce." 815 Ill. Comp. Stat. § 505/2.

227. Defendant is a "person" as defined by 815 Ill. Comp. Stat. § 505/1.

228. Plaintiff and the Class Members are "consumers" as defined by 815 Ill. Comp. Stat. § 505/1.

229. Defendant was engaged "in the conduct of trade or commerce" by hosting and publishing its Website that it encouraged its patients to use and where it advertised her healthcare

services to the public.

230. Plaintiff's and the Class Members' payments to Defendant for health care services were for household and personal purposes.

231. Defendant used unfair and deceptive acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. § 505/2, including but not limited to the following.

a. Defendant encouraged its patients to use its Website and Online Platforms while representing its commitment to protecting the privacy of her Personal Information. Meanwhile, Defendant shared Plaintiff's and Class Members' Private Information with Facebook, Google, and Microsoft, and possibly others, without Plaintiff's and Class Members' knowledge or consent.

b. Defendant promised that it would not use Plaintiff's and Class Members' PHI for undisclosed purposes without Plaintiff's and Class Members' permission. At the same time, Defendant knowingly collected Plaintiff's and Class Members' Private Information and transmitted to third parties like Facebook, exclusively for the purpose of marketing and profits. On information and belief, Defendant then used this information to market its services to Plaintiff and Class Members.

c. Plaintiff and Class Members relied on Defendant's representations in using Defendant's Online Platform and thought they were communicating only with her trusted healthcare provider. In actuality, Defendant was surreptitiously intercepting and transmitting Plaintiff's and Class Member's communications from Plaintiff's and Illinois Subclass Members' browsers directly to Facebook.

232. Defendant's Disclosure of Plaintiff and Class Members' Private Information was willful, knowing, and done with intent that Plaintiff and Class Members rely upon the concealment, suppression or omission of a material fact: that Defendant was tracking Plaintiff's and Class Members' Private Information, using it for advertising purposes without her permission, and disclosing that information to unauthorized third parties.

233. Had Plaintiff and Class Members been aware that her Private Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential medical information to Defendant.

234. Furthermore, the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. § 530/20, provides that a violation of that statute constitutes an unlawful practice under the CFDPA.

235. Defendant is a "data collector" under IPIPA. 815 Ill. Comp. Stat. § 530/5.

236. As a data collector, Defendant owns or licenses information concerning Illinois residents—Plaintiff and the Illinois Subclass.

237. The IPIPA protects Medical Information and Personal Information.

238. The IPIPA requires a data collector that "maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 Ill. Comp. Stat. § 530/45(a).

239. IPIPA's rights are not subject to waiver. 815 Ill. Comp. Stat. § 530/15.

240. The IPIPA further requires that data collectors "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most *expedient* time possible and

without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." 815 Ill. Comp. Stat. § 530/10 (emphasis added).

241. As alleged above, Defendant violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiff' and Illinois Subclass Members' PHI and PII. Defendant further violated the IPIPA by failing to give Plaintiff and Illinois Subclass Members expedient notice without unreasonable delay.

242. The CFDPA provides that "[a]ny person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person. The court, in its discretion may award actual economic damages or any other relief which the court deems proper." 815 Ill. Comp. Stat. Ann. 505/10a(a). Further, "the Court may grant injunctive relief where appropriate and may award, in addition to the relief provided in this Section, reasonable attorney's fees and costs to the prevailing party." *Id*. at 505/10a(b).

243. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the CFDPA, Plaintiff and Class Members have suffered damages for which Defendant is liable, including, but not limited to, the following.

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

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

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff' and Class Members' knowledge or informed consent and without sharing the benefit of such value.

d. 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.

e. Defendant's actions diminished the value of Plaintiff' and Class Members' personal information.

244. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the Court. Had Plaintiff and Class Members been aware that their Private Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential medical information to Defendant.

245. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, *inter alia*, actual damages, reasonable attorneys' fees and costs, and injunctive relief.

COUNT VIII
VIOLATION OF THE ILLINOIS EAVESDROPPING STATUTE, 720 Ill. Comp. Stat. 5/14, *et seq*.
(On Behalf of Plaintiff and the Class)

246. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

247. The Eavesdropping Article of the Illinois Criminal Code (the "Illinois Eavesdropping Statute" or "IES") states that it is a felony for any person to knowingly and intentionally "use[] an eavesdropping devise, in a surreptitious manner, for the purpose of transmitting or recording all or part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation." 720 Ill. Comp. Stat. 5/14-2(a), -4.

248. The IES also states that it is a felony for any person to knowingly and intentionally "use[] or disclose[] any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all of the parties." *Id*.

249. For purposes of the IES, "eavesdropping device" means "any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means." 720 Ill. Comp. Stat. 5/14-1(a).

250. For purposes of the IES, "surreptitious" means "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 Ill. Comp. Stat. 5/14-1(g).

251. For purposes of the IES, "private electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. . . . Electronic communication does include any communication from a tracking device." 720 Ill. Comp. Stat. 5/14-1(e).

252. "A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution." *Id*.

253. Defendant intentionally recorded and/or acquired Plaintiff's and Class Members' private electronic communications, without the consent of Plaintiff and Class Members, using the Pixel and similar tracking technologies on its Online Platforms.

254. Defendant intentionally recorded and/or acquired Plaintiff's and Class Members'

private electronic communications for the purpose of disclosing those communications to third parties, including Facebook and Google, without the knowledge, consent, or written authorization of Plaintiff or Class Members.

255. Plaintiff's and Class Members' communications with Defendant constitute private conversations, communications, and information.

256. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Online Platforms.

257. Plaintiff and Class Members communicated sensitive PHI and PII that they intended for only Defendant to receive and that they understood Defendant would keep private.

258. Plaintiff and Class Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiff's or Class Members' authorization, consent, or knowledge.

259. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations, Notice of Privacy Practices, and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that her communications regarding healthcare with their healthcare providers will be kept confidential.

260. Plaintiff and Class Members were unaware that her Private Information was being surreptitiously recorded and transmitted to third parties as they communicated with Defendant through its Online Platforms.

261. Without Plaintiff's or Class Members' knowledge, authorization, or consent, Defendant used the Pixel imbedded and concealed into the source code of its Online Platforms to secretly record and transmit Plaintiff's and Class Members' private communications to hidden third parties, such as Facebook and Google, as described in the preceding paragraphs.

262. Under the IES, "[a]ny or all parties to any conversation or electronic communication upon which eavesdropping is practices contrary to this Article shall be entitled to the following remedies: (a) [t]o an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either; (b) [t]o all actual damages against the eavesdropper or his principal or both; [t]o any punitive damages which may be awarded by the court or by a jury. . . ." 720 Ill. Comp. Stat. 5/14-6.

263. The eavesdropping devices used in this case include, but are not limited to:

a. Plaintiff's and Class Members' personal computing devices;

b. Plaintiff's and Class Members' web browsers;

c. Plaintiff's and Class Members' browser-managed files;

d. Facebook's Pixel;

e. Internet cookies;

f. Other tracking technology including Google Analytics with Google Tag Manager ("GTM"), DoubleClick Ads, and Microsoft Clarity;

g. Defendant's computing servers;

h. Third-party source code utilized by Defendant; and

i. Computer servers of third-parties (including Facebook) to which Plaintiff' and Class Members' communications were disclosed.

264. The eavesdropping devices outlined above are not excluded "tracking devices" as that term is used in the IES, 720 ILCS 5/14-1(e), to the extent that they perform functions other than collection of geo-locational data.

265. Defendant is a "person" under the IES. 720 Ill. Comp. Stat. 5/2-15.

266. Defendant aided in the interception of communications between Plaintiff and

Class Members and Defendant that were redirected to and recorded by third parties without Plaintiff' or Class Members' consent.

267. Under the IES, Plaintiff and the Class Members are entitled to injunctive relief prohibiting further eavesdropping by Defendant, actual damages, and punitive damages.

268. Defendant's violation of the IES caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members

b. intended to remain private is no longer private;

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

d. 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 sharing the benefit of such value;

e. 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; and

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

269. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT IX
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. §§ 2511(1), *et seq.*
(On Behalf of Plaintiff and the Class)

270. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

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

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

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

274. **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." *See* 18 U.S.C. § 2510(8).

275. **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." See 18 U.S.C. § 2510(4), (8).

276. **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. Defendant's Website.

277. The tracking technology deployed by Defendant effectuated the sending and acquisition of patient communications.

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

279. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the tracking technology including the Pixel, which tracked, stored ,and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook, Google, and Microsoft.

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

281. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to 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).

282. 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).

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

284. Defendant intentionally used the wire or electronic communications to increase its profit margins and save on marketing costs.

285. Defendant specifically used the Pixel to track and to utilize Plaintiff's and Class Members' Private Information for financial gain.

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

287. Plaintiff and Class Members did not authorize Defendant to acquire the content of her communications for purposes of invading Plaintiff' and Class Members' privacy via the tracking technology.

288. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of its Website, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation or matter that would be highly offensive to a reasonable person; and (ii) violation of HIPAA, the FTC Act, invading Plaintiff and Class Members' privacy, and in breach of its fiduciary duty of confidentiality.

COUNT X
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

18 U.S.C. § 2511(3)(a)
UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
(On Behalf of Plaintiff and the Class)

289. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

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

291. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant's Website is an electronic communication service which provides to users thereof the ability to send or receive electronic communications; in the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiff' and Class Members' Private Information.

292. **Intentional Divulgence**. Defendant intentionally designed the tracking technology and was or should have been aware that, if so configured, it could divulge Plaintiff' and Class Members' Private Information. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with her exchange with Defendant's Website, to which they directed her communications.

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

294. **Exceptions do not apply**. In addition to the exception for communications

directly to an electronic communications service ("ECS")[100] or an agent of an ECS, the ECPA states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication."

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

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;" c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." U.S.C. § 2511(3)(b).

295. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

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

[100] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

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

298. Defendant's divulgence of the contents of patient communications on its Website through the tracking technology was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiff and Class Members did not authorize Defendant to divulge the contents of her communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

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

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

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

COUNT XI
VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("STORED COMMUNICATIONS ACT")
18 U.S.C. § 2702, *et seq.*
(On Behalf of Plaintiff and the Class)

302. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

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

304. **Electronic Communication Service**. ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant intentionally procures and embeds various Plaintiff's Private Information through the tracking technology used on Defendant's Website, which qualifies as an Electronic Communication Service.

305. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

306. Defendant stores the content of Plaintiff's and Class Members' communications on Defendant's Website and files associated with it.

307. When Plaintiff or Class Members make a Website communication, the content of that communication is immediately placed into storage.

308. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through the tracking technology.

309. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—" a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;" c. "with the lawful consent of the originator or an addressee or intended recipient

of such communication, or the subscriber in the case of remote computing service;" d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;" e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;" f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A." g. "to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;" h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

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

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

312. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a

provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

313. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on its Website to Facebook or other third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of the Defendant's services nor (ii) necessary to the protection of the rights or property of Defendant.

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

315. Defendant's divulgence of the contents of user communications on its Website was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiff and Class Members did not authorize Defendant to divulge the contents of her communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

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

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

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

fee and other litigation costs reasonably incurred.

COUNT XII
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA")
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiff and the Class)

319. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

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

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

322. Defendant's conduct caused "loss to 1 or more persons during any 1-year period… aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class Members' Private Information as set forth in detail herein, which were never intended for public consumption.

71. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiff and the Class Members' Private Information and communication being made available to Defendant, Facebook, Google, Microsoft, and/or other third parties without adequate legal privacy protections.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, ALANA HANNANT, and on behalf of all others similarly situated, pray for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and Plaintiff's counsel as Class Counsel;

B. for an award of actual damages, compensatory damages, consequential damages, and punitive damages, in an amount to be determined, as allowable by law;

C. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff' and Class Members' Private Information and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

D. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

E. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. for an award of attorneys' fees under the common fund doctrine, and any other applicable law;

G. costs and any other expenses, including expert witness fees incurred by Plaintiff in connection with this action;

H. pre- and post-judgment interest on any amounts awarded; and

I. such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and all others similarly situated, hereby demands a trial by jury on all issues so triable.

Dated: September 6, 2024

Respectfully submitted,

/s/ Lynn A. Toops

Lynn A. Toops, (No. 63337-43)
Mallory K. Schiller (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
mschiller@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
Emily E. Schiller (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com
eschiller@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina C. Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS & BORELLI, PLLC
One Magnificent Mile
980 North Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

Counsel for Plaintiff and the Proposed Class