

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF IOWA**

Eileen Yeisley, on behalf of herself and all other similarly situated, Plaintiff, v. University of Iowa Hospitals & Clinics, Defendant.	Case No. JURY TRIAL DEMANDED
--	--

CLASS ACTION COMPLAINT

Plaintiff Eileen Yeisley is a current user of University of Iowa Hospitals & Clinics (“UIHC” or Defendant). She brings this class action against UIHC in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, her counsels’ investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this class action lawsuit to address Defendant’s unlawful and widespread unauthorized practice of disclosing Plaintiff’s and Class Members’ confidential personally identifiable information (PII) and protected health information (PHI) (collectively referred to as Private Information) to third parties, including Meta Platforms, Inc. d/b/a Meta (Facebook).

2. Defendant manages or controls the two websites www.uihealthcare.org and University of Iowa Hospitals & Clinics (“Defendant’s Website”), which it encourages individuals to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions

and treatment options, signing up for events and classes.

3. Defendant installed and implemented the Facebook Tracking Pixel (the Pixel or Facebook Pixel) on its Website, which secretly enables the unauthorized transmission and disclosure of Plaintiff and Class Members' PII and PHI as they are communicated to Defendant.

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

5. By implementing Conversions API, Defendant secretly enabled additional unauthorized transmissions and disclosures of Plaintiff and Class Members' PII and PHI.¹

6. More specifically, Defendant's Websites direct Plaintiff's and Class Members' communications to automatically and surreptitiously be sent to Facebook's servers, and this occurs on every webpage that Defendant has installed the Pixel and Conversions API.²

7. Thus, operating as designed and as implemented by Defendant, the Pixel

¹ "Conversions API works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited: Jan. 25, 2023).

² "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel . . . This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited: January 27, 2023)

allows the Private Information that Plaintiff and Class Members submit to Defendant to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID (FID).

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

Tracking Pixel

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

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

11. The Pixel can share the user's Facebook User ID⁴ for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the

³ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Jan. 31, 2023).

⁴ The Facebook "User ID is a string of numbers that doesn't personally identify you but does connect to your Facebook profile." A Facebook "User ID [is generated] automatically, whether or not you choose to create username." <https://www.facebook.com/help/211813265517027> (last visited: January 27, 2023).

same web browser.⁵ Cookies are only transmitted to the owner site from the user's web browser and cannot be accessed by any other site.

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

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

Conversions API

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

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

⁵ "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." <https://www.cloudflare.com/learning/privacy/what-are-cookies> (last visited: January 27, 2023).

⁶ <https://revealbot.com/blog/facebook-conversions-api/> (last visited: January 24, 2023).

⁷ <https://www.facebook.com/business/help/2041148702652965?id=818859032317965>

Information on its own server and then transmits it to Facebook from Defendant's server.

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

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

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

19. Conversions API tracks the user's website interaction, including Private Information, and then transmits this data to Facebook. Indeed, Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your

(last visited: January 25, 2023).

⁸ "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only." <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/> (last visited: January 27, 2023).

⁹ "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." <https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req-rec-params> (last visited: January 27, 2023).

¹⁰ <https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events> (last visited: January 27, 2023).

customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results.”

Purpose of this Lawsuit

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

21. The information that Defendant's Pixel and Conversions API sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including for example, the type of medical treatment sought, the particular health condition, and the fact that the individual attempted to or did book a medical appointment. Such Private Information would allow a third party (e.g., Facebook) to know that a specific individual was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific individual was being treated for a specific type of medical condition such as cancer, pregnancy, dementia, or HIV.

22. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and Conversions API.

23. For instance, Plaintiff submitted medical information to Defendant's Website and used the Website to search for a physician, communicate Private Information with her physician, complete patient web forms, and review medical healthcare records.

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

Website to Facebook.

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

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

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

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

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

those individuals to protect and safeguard that information from unauthorized disclosure.

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

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

32. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their PII and PHI to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' PII and PHI through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of individual's PII and PHI.

33. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost time and opportunity costs

associated with attempting to mitigate the actual consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (vi) the continued and ongoing risk to their Private Information.

34. Plaintiff seeks to remedy these harms and bring causes of action for (i) Invasion of Privacy, (ii) unjust enrichment; (iii) breach of implied contract; (iv) violations of the Electronics Communication Privacy Act (ECPA), 18 U.S.C. § 2511(1)—unauthorized interception, use, and disclosure; (v) violations of ECPA, 18 U.S.C. § 2511(3)(a)—unauthorized interception, use, and disclosure; (vi) violations of Title II of the ECPA, 18 U.S.C. § 2702, *et seq.*—Stored Communications Act; (vii) violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, *et seq.*; and (viii) breach of confidence.

PARTIES

Plaintiff Eileen Yeisley

35. Plaintiff is a natural person and citizen of Iowa where she intends to remain. On numerous occasions, Plaintiff accessed Defendant's Website on her mobile device and/or computer. Plaintiff used the Website to find and obtain medical treatment. Pursuant to the systematic process described in this Complaint, Plaintiff's Private Information was intentionally disclosed to Facebook, and this data included her PII, PHI, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's PII and PHI.

36. Plaintiff has received healthcare services at Defendant's healthcare facilities since the early 1980s and has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions over the last five years.

37. Plaintiff used Defendant's Website, including the UIHC Webpage, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

38. Plaintiff has been a Facebook user since 2009.

39. Plaintiff accessed Defendant's Website, including the UIHC Webpage, to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

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

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

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

Defendant University of Iowa Health Care

43. Defendant University of Iowa Hospitals & Clinics is headquartered at 200 Hawkins Drive, Iowa City, IA 52242. Defendant presents itself as providing “world class family-centered health care, extensive medical research, and comprehensive teaching programs for many health care professions.”¹¹ “With more than 250 specialty and subspecialty clinics, UI Hospitals & Clinics offers the most comprehensive health care in the state.” Defendant employs over 11,200 individuals, including over 1,100 staff physicians and dentists, nearly 800 resident and fellow physicians, and more than 5,000 nursing staff members.

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

JURISDICTION & VENUE

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

46. This Court has federal question jurisdiction under 29 U.S.C. § 1331

¹¹ <https://uihc.org/about-us>.

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

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

48. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

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

49. Defendant purposely and intentionally installed the Pixel and Conversions API tools on its webpages within its Website, and it programmed those webpages to surreptitiously share its potential and current users' private and protected communications with Facebook, including communications that contain Plaintiff's and Class Members' PHI and PII.

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

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

i. Facebook's Business Tools and the Pixel.

52. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling

advertising space.¹²

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

54. Facebook’s Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

55. The Business Tools are automatically configured to capture “Standard Events” such as when a user visits a particular webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, button clicks, etc.¹³ Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a “custom event.”¹⁴

56. One such Business Tool is the Pixel, which “tracks the people and type of

¹² Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results*, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Nov. 14, 2022).

¹³ Facebook, *Specifications for Facebook Pixel Standard Events*, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>. (last visited Jan. 31, 2023); *see* Facebook, *Facebook Pixel, Accurate Event Tracking, Advanced*, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; *see also* Facebook, *Best Practices for Facebook Pixel Setup*, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; Facebook, *App Events API*, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Jan. 31, 2023).

¹⁴ Facebook, *About Standard and Custom Website Events*, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; *see also* Facebook, *App Events API*, *supra*.

actions they take.”¹⁵ When a user accesses a webpage that is hosting the Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook’s servers—traveling from the user’s browser to Facebook’s server.

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

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

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

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

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

61. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each “client device” (such as computer, tablet, or smart phone) accessed web

¹⁵ Facebook, *Retargeting*, <https://www.facebook.com/business/goals/retargeting>.

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

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

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

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

codes, among other data.¹⁶

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

65. 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.

66. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When individuals visit Defendant's website via an HTTP Request to UIHC's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is, in essence, handing individuals a tapped phone, and once the Webpage is loaded into the individual's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook.

¹⁶ One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

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

68. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that savvy users cannot evade. Facebook's workaround, for example, is called Conversions API. Conversions API is an effective workaround because it does the transmission from their own servers and does not rely on the User's web browsers. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."¹⁷ Thus, the communications between individuals and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

69. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in

¹⁷ Facebook, *Prepare your Business to Use the Conversions API*, <https://www.facebook.com/business/help/1295064530841207?id=818859032317965> (last accessed Jan. 31, 2023).

addition to the [] Pixel, and share the same events using both tools,” because such a “redundant event setup” allows Defendant “to share website events [with Facebook] that the pixel may lose.”¹⁸ Thus, it is reasonable to infer that Facebook’s customers who implement the Facebook Pixel in accordance with Facebook’s documentation will also implement the Conversions API workaround.

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

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

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

73. For example, when an individual visits <https://uihc.org/services> and selects “Heart and Vascular Services,” the patient’s browser automatically sends an HTTP Request to Defendant’s web server. Defendant’s web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below.

¹⁸See <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited Jan. 23, 2023).

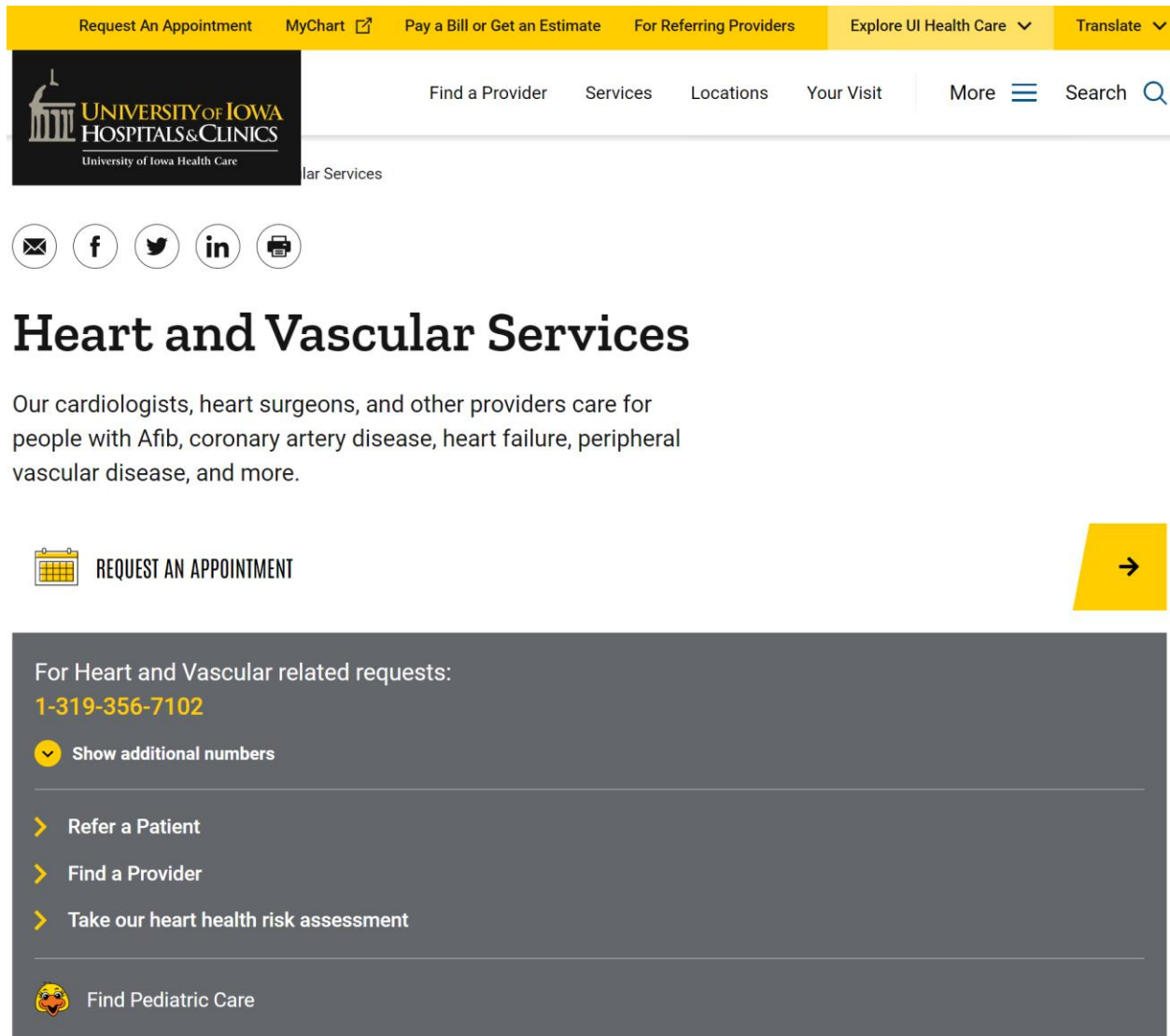


Figure 1 Image taken from <https://uihc.org/services/heart-and-vascular-services>.

74. The individual visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

75. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,¹⁹ effectively open a spying

¹⁹ These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware

window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

76. Looking to the previous example, Defendant's Source Code manipulates the individual's browser by secretly instructing it to duplicate the individual's communications (HTTP Requests) and send those communications to Facebook.

77. This occurs because the Pixel embedded in Defendant's Source Code is programmed to automatically track and transmit individuals' communications, and this occurs contemporaneously, invisibly, and without the individual's knowledge.

78. Thus, without each individuals' consent, Defendant has effectively used its Source Code to commandeer the individuals' computing devices, thereby re-directing their Private Information to third parties.

79. The information that Defendant's Pixel sends to Facebook may include, amongst other things, the individuals' Private Information, and other confidential information.

80. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, it is transmitted to Facebook, including, but not limited to, appointment type and date, physician selected, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information.

of them.

B. Defendant's Pixel and/or Conversions API Tracking Practices caused Plaintiff's and Class Members' Private Information to be sent to Facebook.

81. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API on its Website to secretly track individuals by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.²⁰

82. Defendant's Website contains a unique identifier that indicates that the Pixel is being used on a particular webpage, identified as 7366111505820508.

83. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.²¹ However, Defendant's Website does not rely on the Pixel in order to function.

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

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

86. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did

²⁰ *Id.*

²¹ *Id.*

they intend for Facebook to be a party to their communications with Defendant.

87. Defendant's Pixel and Conversions API sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) sought treatment or therapies; (4) appointment requests and appointment booking information; (5) registration or enrollment in medical classes (such as breastfeeding courses); (6) locations or facilities where treatment is sought; (7) which webpages were viewed; and (8) phrases and search queries conducted via the general search bar.

88. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individuals' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.²²

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

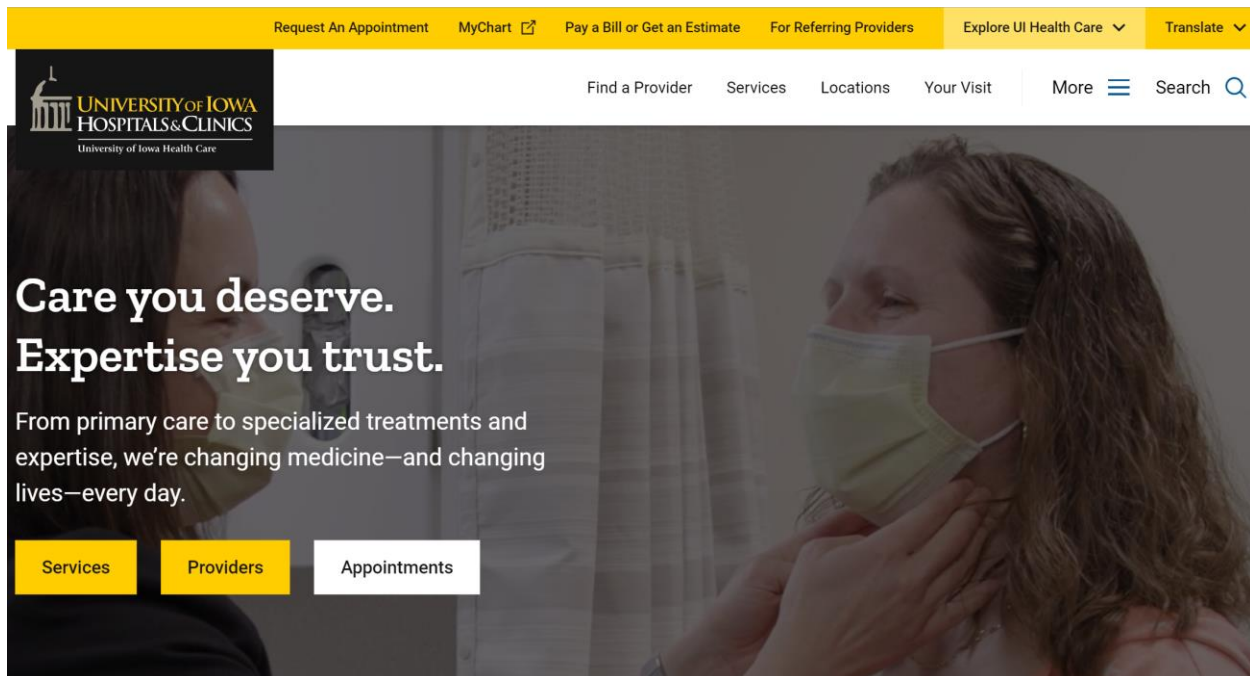
²² Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

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

i. Defendant's Pixel Disseminates Personal Information via www.uich.org.

91. An example illustrates the point. If an individual uses www.uich.org to book an appointment with a cardiologist, Defendant's Webpage directs them to a series of screens that ask the individual to communicate additional information. Unbeknownst to the individual, each and every communication is sent to Facebook via Defendant's Pixel, as evidenced by the images below.

92. In order to book an appointment, the user visits www.uich.org and clicks the "services" button.



93. Next, Defendant directs the user to select from a list of “featured services” or search for all services.

The screenshot displays the top navigation bar of the University of Iowa Hospitals & Clinics website. The bar is yellow and contains links for 'Request An Appointment', 'MyChart', 'Pay a Bill or Get an Estimate', 'For Referring Providers', 'Explore UI Health Care', and 'Translate'. Below this is a dark blue header with the university's logo and a search bar. The search bar contains the text 'Ex: cancer, heart, back pain' and a magnifying glass icon. To the right of the search bar is a button labeled 'VIEW ALL SERVICES' with a yellow background and a right arrow. Below the header is a section titled 'Services' with a large search bar and a button labeled 'OR' and 'VIEW ALL SERVICES' with a right arrow. Below this is a section titled 'Featured services' with six cards, each representing a different medical service: Family Medicine, Heart and Vascular Services, Holden Comprehensive Cancer Center, Obstetrics and Gynecology, Ophthalmology and Visual Sciences, and Orthopedics and Rehabilitation. Each card has a title, a right arrow, and a brief description of the service.

Request An Appointment **MyChart** **Pay a Bill or Get an Estimate** **For Referring Providers** **Explore UI Health Care** **Translate**

UNIVERSITY of IOWA HOSPITALS & CLINICS
University of Iowa Health Care

Find a Provider Services Locations Your Visit More Search

Home / Services

Services

Ex: cancer, heart, back pain

OR **VIEW ALL SERVICES**

Featured services

Family Medicine →

Your family medicine provider can see everyone in the family, in every generation, from birth, for life. And when anyone in the family needs specia...

Heart and Vascular Services →

Our cardiologists, heart surgeons, and other providers care for people with Afib, coronary artery disease, heart failure, peripheral vascular disea...

Holden Comprehensive Cancer Center →

Holden Comprehensive Cancer Center is Iowa's only NCI-designated comprehensive cancer center and has held that designation since 2000. The NCI desi...

Obstetrics and Gynecology →

Our world class OBGYN specialists provide care for you at every stage of life. We emphasize preventive care and offer

Ophthalmology and Visual Sciences →


Expert eye care for the entire family—vision screenings, treatments for

Orthopedics and Rehabilitation →

Injuries and diseases in the bones, joints, muscles, and connective tissues can be






94. The user then selects the “request an appointment” button, whereafter Defendant invites the user to schedule online and provide contact information, patient information, and insurance information.

[Request An Appointment](#)
[MyChart](#)
[Pay a Bill or Get an Estimate](#)
[For Referring Providers](#)
[Explore UI Health Care](#)
[Translate](#)




[Find a Provider](#)
[Services](#)
[Locations](#)
[Your Visit](#)
[More](#)
[Search](#)

[Home](#) / [Request an Appointment](#)


Request an Appointment



Schedule Online

Request an appointment through our webform or through MyChart.


> [Schedule through MyChart](#)



Call to Schedule

Speak with a scheduling assistant directly to discuss appointment options.

> [Call 800-777-8442 \(toll-free\)](#)



Same-Day Care

Same-day care is available at our UI QuickCare and UI Urgent Care locations. For medical emergencies call 911.

> [UI Urgent Care](#)

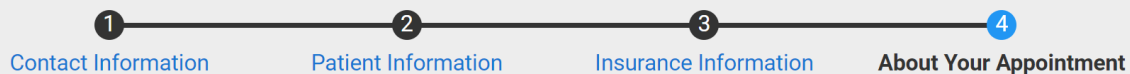
> [UI QuickCare](#)

> [Emergency Care](#)

Fill out an appointment request form

If you have a MyChart account, [log on to MyChart to schedule your appointment](#). If you do not have a MyChart account, fill out this appointment request form and a scheduling assistant will contact you shortly.

To expedite your appointment request, you will need information from your **health insurance card**.



Preferred Physician or Department Specialty *

Heart and Vascular Services

< Previous

Submit Appointment Request

95. Without alerting the user, Defendant's Pixel sends each and every

communication the user made to the Defendant via the Webpage to Facebook, and the image below confirms that the communications Defendant sends to Facebook contain the user's Private Information.

```

▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=736611150582050&ev=Microdata&dl=https%3A%2F%2Fuihc.org%2Fservices%2Fheart-and-vascular-services&rl=
https%3A%2F%2Fuihc.org%2Fservices&if=false&ts=167773867319&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22He
art%20and%20Vascular%20Services%20%7C%20University%20of%20Iowa%20Hospitals%20%26%20Clinics%22%2C%22meta%3Adescr
ption%22%3A%22Our%20cardiologists%2C%20heart%20surgeons%2C%20and%20other%20providers%20care%20for%20people%20wit
h%20Afib%2C%20coronary%20artery%20disease%2C%20heart%20failure%2C%20peripheral%20vascular%20disease%2C%20and%20m
ore.%22%7D&cd[OpenGraph]=%7B%22og%3Asite_name%22%3A%22University%20of%20Iowa%20Hospitals%20%26%20Clinics%22%2C%2
2og%3Atype%22%3A%22Umbrella%20Care%22%2C%22og%3Aurl%22%3A%22https%3A%2F%2Fuihc.org%2Fservices%2Fheart-and-vascul
ar-services%22%2C%22og%3Atitle%22%3A%22Heart%20and%20Vascular%20Services%22%2C%22og%3Adescription%22%3A%22Our%20
cardiologists%2C%20heart%20surgeons%2C%20and%20other%20providers%20care%20for%20people%20with%20Afib%2C%20corona
ry%20artery%20disease%2C%20heart%20failure%2C%20peripheral%20vascular%20disease%2C%20and%20more.%22%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1920&sh=1080&v=2.9.97&r=stable&a=tmgoogletagmanager&ec=1&o=30&fbp=fb.1.16777
69944440.1178272021&it=167773865818&coo=false&es=automatic&tm=3&rqm=GET
:scheme: https
:accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
:accept-encoding: gzip, deflate, br
:accept-language: en-US,en;q=0.9
:cache-control: no-cache
:cookie: datr=Faa8Y1K6mwXJGAT883Z3Zdp0; sb=Faa8Ypp_NV49mr2N6oZnTRGR; c_user=[REDACTED] xs=26%3A91RYN0C91iAOJQ%3A2%
3A1677098418%3A-1%3A2977%3A%3AAcUbhPOfRQeyQxeYeI5qktPagIc85WGoQrYEni7eSg; fr=09IC35uCXvT1fuOYv.AWUv1Oh_eiA5kQhe_
zcZLn1_gU.BkALzg.rw.AAA.0.0.BkAMd4.AWwVGOB-PVA
:pragma: no-cache
:referer: https://uihc.org/
:sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
:sec-ch-ua-mobile: ?0
:sec-ch-ua-platform: "Windows"
:sec-fetch-dest: image
:sec-fetch-mode: no-cors
:sec-fetch-site: cross-site
:user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safa
ri/537.36

```

96. The third line of highlighted text, “id=736611150582050,” refers to the Defendant’s Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

97. The remainder of that third line of text identifies and categorizes which

actions the user took on the Webpage (e.g., “heart-and-vascular-services,” “vascular%20disease”). Thus, this identifies the user as having viewed the particular Webpage.

98. The remaining lines of text identify: (1) the user as a patient seeking medical care from Defendant via www.uihc.org; (2) who is in the process of booking an appointment or searching for medical treatment; (3) whether appointment is for herself as opposed to someone else (appearing as “who=me” in the text above); and (4) the appointment is with an “heart%20and%20vascular%20services” (aka the “reason” for the appointment);

99. Finally, the second line of highlighted text (“GET”), demonstrates that Defendant’s Pixel sent the user’s communications, and the Private Information contained therein, alongside the user’s Facebook ID (c_user = ID).²³

²³ The user’s Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiff has redacted the corresponding string of numbers to preserve the user’s anonymity.

ii. Plaintiff has Specific Evidence of Defendant's Tracking Pixel Communicating with Facebook regarding her Private Information.

100. Plaintiff submitted PHI to Defendant via the Website. Because Defendant utilizes the Facebook Pixel, the Website's Source Code sends a secret set of instructions back to the individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and the webpage's URL to Facebook. For instance, when Plaintiff visited Defendant's webpage for a medical condition, the Facebook Pixel reports back the Plaintiff's FID as well as the web page and other data specified by Defendants secretly to Facebook.

101. Accordingly, during the same transmissions, the Website routinely provide Facebook with its users' FIDs, IP addresses, and/or device IDs or other the information they input into Defendant's Website, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.²⁴ Plaintiff's and Class Members identities could be easily determined based on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

102. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that

²⁴ <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Nov. 14, 2022)

it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

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

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

105. Defendant did not inform Plaintiff that it shared her Private Information with Facebook and other unauthorized third parties.²⁵ Moreover, Defendant's privacy

²⁵ Defendant also shares Plaintiff's and Class Members Private Information with Google Analytics (analytics.google.com) which allows Defendant to leverage its Website visitor's traffic to "[a]dvertise more effectively by linking your Ads account to Analytics." See https://analytics.withgoogle.com/?utm_source=google-

policy does not state that its patients' Private Information will be shared with Facebook or other unauthorized third parties without prior written consent.

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

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

108. Plaintiff suffered damages in the form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the invasion of privacy; (iii) diminution of value of the Private Information; (iv) statutory damages; (v) the continued and ongoing risk to her Private Information; and (vi) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff's medical conditions and other confidential information she communicated to Defendant via the Website.

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

C. Defendant's Conduct is Unlawful and Violates its Patients' Rights.

growth&utm_medium=cpc&utm_campaign=2019-q4-amer-all-gafree-analytics&utm_content=analytics&gclid=CjwKCAjwiOCgBhAgEiwAjb5whBGXXTuujOX3sdbwNHkoDKGwKp8MZSuno8yu8yQ3-Zor5EEDdct6sRoCuZoQAvD_BwE&gclsrc=aw.ds (last visited March 6, 2023).

i. Defendant's Conduct Violates its Own Privacy Policies and Promises.

110. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep Private Information private and confidential and they will only disclose Private Information under certain circumstances.²⁶

111. Defendant publishes several privacy policies that represent to patients and Website visitors that Defendant will keep sensitive information confidential and will only disclose PII and PHI under certain circumstances, none of which apply here.

112. Defendant's privacy policy explains Defendant's legal duties with respect to Private Information and the exceptions in which Defendant can lawfully use and disclose Plaintiff's and Class Members' Private Information, including:

- Follow the law;
- Help with public health and safety issues;
- Respond to organ and tissue donation requests;
- Work with a medical examiner or funeral director
- Handle workers' compensation;
- Respond to lawsuits and legal actions; and
- With your written permission

113. Defendant's HIPAA Notice of Privacy Practices does not permit Defendant to intercept, transmit, and/or disclose Plaintiff's and Class Members' Private Information to third parties, including Facebook, *for marketing purposes* and will only make these

²⁶ <https://uihealthcare.org/privacy-policy> (last visited: February 10, 2023).

disclosures with written authorization.²⁷

114. Defendant violated its own Privacy Policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties for marketing purposes without adequately disclosing that it shares Private Information with third parties for those purposes and without acquiring the specific patients' consent or authorization. Furthermore, as required by Defendant's own HIPAA Notice of Privacy Practices, it is "required by law [that UIHC] notify you of a breach of your unsecured medical information" without unreasonable delay but in no case later than 60 days after we discovery the breach."²⁸ Defendant has provided no such notice.

ii. Defendant Violated HIPAA Standards

115. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.²⁹

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

117. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act

²⁷ <https://uihc.org/hipaa-notice-privacy-practices-english> (last accessed March 7, 2023).

²⁸ *Id.*

²⁹ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

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.³⁰

118. 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).³¹

119. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").³²

³⁰ https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited March 10, 2023).

³¹ <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (last visited Nov. 3, 2022)

³² See <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

120. The Bulletin expressly provides:

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. **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 for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.

121. HHS Privacy Bulletin (internal citations omitted) (emphasis in original).³³

122. The HHS Privacy Bulletin also identifies several harms that may result from an impermissible disclosure of an individual's PHI, including:

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.

HHS Privacy Bulletin (internal citations omitted) (emphasis in original).³⁴

123. According to HHS, HIPAA "[r]egulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a

³³ *Id.*

³⁴ *Id.*

regulated entity's website, including individually identifiable health information that the individual provides when they use regulated entities' websites." The information an individual provides may include a medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code.³⁵

124. All of the above listed information that is collected on a regulated entity's website, like Defendant's websites, is PHI, "even if the individual does not have an existing relationship with the regulated entity and even if the [information], such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services." When a regulated entity, again like Defendant, collects the individual's information, that information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.³⁶

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

iii. Defendant Violated Iowa Public Policy.

126. Iowa has a strong and clearly defined public policy in favor of protecting the privacy of individuals' health information.

³⁵ *Id.*

³⁶ *Id.*

127. In its statute establishing a state health information network, the Iowa General Assembly declared that “[a]ll health information technology efforts shall endeavor to . . . protect the privacy of individuals and the confidentiality of individual’s [health] information.”³⁷

128. Likewise, Iowa courts have recognized the important public policy of protecting the privacy of individuals’ health information.³⁸

129. Defendant violated this public policy by implementing the Facebook Pixel.

iv. Defendant Violated Industry Standards.

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

131. The American Medical Association’s (“AMA”) Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

132. 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).”

133. 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

³⁷ Iowa Code § 135D.3(1)(d); *see also* Iowa Code § 228.2 (prohibiting disclosure of mental health information).

³⁸ *See, e.g., In the Interest of A.M.*, 856 N.W.2d 365, 377–78 (Iowa 2014) (discussing the public policy favoring mental health patients’ right to privacy).

effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

134. AMA Code of Medical Ethics Opinion 3.3.2 provides: "Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must: . . . (c) release patient information only in keeping ethics guidelines for confidentiality."

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

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

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

vi. IP Addresses are Personally Identifiable Information.

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

138. An IP address is a number that identifies the address of a device connected

to the Internet.

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

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

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

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

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

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

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

vii. Defendant was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures.

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

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

147. 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.

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

TOLLING

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

CLASS ACTION ALLEGATIONS

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

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

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

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

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

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

155. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiff and Class Members to Facebook and/or additional third parties.
- d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI would be disclosed to third parties;

- e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;
- f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PII and PHI;
- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- h. Whether Defendant violated the consumer protection statutes asserted as claims in this Complaint;
- i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;
- k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and
- l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their PII and PHI.

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

157. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling

conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

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

159. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's

challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

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

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

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

163. Unless a classwide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and

Defendant may continue to act unlawfully as set forth in this Complaint.

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

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

- a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;
- b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;
- c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the

information disclosed to third parties; and

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

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

COUNT I:
INVASION OF PRIVACY
(On Behalf of Plaintiff and the National Class)

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

168. The Private Information of Plaintiff and Class Members consist of private and confidential facts and information that were never intended to be shared beyond private communications.

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

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

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

172. Defendant's willful and intentional disclosure of Plaintiff's and Class

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

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

174. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed the Pixel onto its Website because the purpose of the Pixel is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

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

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

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

178. Defendant's wrongful conduct will continue to cause great and irreparable

injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

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

180. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII and PHI and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II:
UNJUST ENRICHMENT
(On behalf of Plaintiff and the National Class)

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

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

183. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible,

and other benefits, including substantial monetary compensation.

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

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

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

COUNT III:
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
("ECPA") 18 U.S.C. § 2511(1) *et seq.*
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the National Class)

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

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

189. 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.

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

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

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

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

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

- a. Plaintiff's and Class Members' browsers;
- b. Plaintiff's and Class Members' computing devices;

- c. Defendant's web-servers; and
- d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications.

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

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

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

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

199. 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).

200. **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, including invasion of privacy, among others.

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

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

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

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

205. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of Minn. Stat. § 325D.44, subd. 1.

COUNT IV:
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS
SERVICE

18 U.S.C. § 2511(3)(a)
(On Behalf of Plaintiff and the National Class)

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

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

208. **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).

209. Defendant’s Website is an electronic communication service that gives users the ability to send or receive electronic communications to Defendant and, upon information and belief, medical professionals who contract with, but are not employed by Defendant. In the absence of Defendant’s Website, internet users could not send or receive communications regarding Plaintiff’s and Class Members’ PII and PHI.

210. Defendant’s Website is a conduit of communication between Plaintiff and Class Members and their respective medical providers, including third parties who are not

employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

211. **Intentional Divulgence.** Defendant intentionally designed and/or implemented the Pixel and Conversions API tracking and was or should have been aware that it could divulge Plaintiff's and Class Members' PII and PHI.

212. **While in Transmission.** Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

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

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

- "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"
- "with the lawful consent of the originator or any addressee or intended recipient of such communication;"
- "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or

- “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).

215. 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.

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

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

218. Defendant’s divulgence of the contents of user communications on Defendant’s browser through the Pixel and Conversions API code was not done “with the lawful consent of the originator or any addresses or intended recipient of such communication[s].” As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not

procure the “lawful consent” from the Websites or apps with which Plaintiff and Class Members were exchanging information.

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

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

221. 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; and reasonable attorneys’ fees and other litigation costs reasonably incurred.

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

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

223. 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).

224. **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).

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

226. Defendant intentionally procures and embeds various Plaintiff’s PII and PHI through the Pixel and Conversions API used on Defendant’s Website, which qualifies as an Electronic Communication Service.

227. **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).

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

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

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

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

232. **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—

- (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
- (2) as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;
- (3) 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;
- (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
- (5) 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;
- (6) to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A;
- (7) to law enforcement agency—
 - (A) if the contents—
 - (i) were inadvertently obtained by the service provider; and
 - (ii) appear to pertain to the commission of a crime;

(8) 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

(9) 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.

233. 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.

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

235. 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.

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

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

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

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

240. 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 if applicable in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VI:
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA) 18 U.S.C.
§ 1030, ET SEQ.
(On Behalf of Plaintiff and the National Class)

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

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

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

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

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

246. 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 and personally identifiable data and content – including the Website visitor's electronic communications with the Website, URLs of web pages visited, and/or other electronic communications in real-time which were never intended for public consumption.

247. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiff and the Class being made available to Defendant, Facebook, and/or other third parties without

adequate legal privacy protections.

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

COUNT VII:
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the National Class)

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

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

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

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

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

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

255. The harm arising from a breach of provider-patient confidentiality includes

erosion of the essential confidential relationship between the healthcare provider and the patient.

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

- i.* Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- ii.* Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- iii.* Defendant eroded the essential confidential nature of the provider-patient relationship;
- iv.* General damages for invasion of their rights in an amount to be determined by a jury;
- v.* Nominal damages for each independent violation;
- vi.* Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- vii.* 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;
- viii.* Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and

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

PRAYER FOR RELIEF

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

- A. For an Order certifying the National Class and Iowa Subclass and appointing Plaintiff and Counsel to represent such a Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;
- D. For an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Date: April 21, 2023

Respectfully Submitted,

**SHINDLER, ANDERSON, GOPLERUD
& WEESE P.C.**

/s/ Brian O. Marty
Brian O. Marty
5015 Grand Ridge Drive, Suite 100
West Des Moines, IA 50265
Tel: (515) 223-4567
Fax: (515) 223-8887
marty@sagwlaw.com

/s/ J. Barton Goplerud
J. Barton Goplerud
5015 Grand Ridge Drive, Suite 100
West Des Moines, IA 50265
Tel: (515) 223-4567
Fax: (515) 223-8887
goplerud@sagwlaw.com

Daniel E. Gustafson*
David A. Goodwin*
Joseph E. Nelson*
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
jnelson@gustafsongluek.com

Brian C. Gudmundson*
Hart L. Robinovitch*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com

hart.robinovitch@zimmreed.com

Nathan D. Prosser*

HELLMUTH & JOHNSON PLLC

8050 West 78th Street

Edina, MN 55439

Phone: (952) 522-4291

nprosser@hjlawfirm.com

Aaron N. Halstead*

Aaron J. Bibb*

HAWKS QUINDEL S.C.

409 East Main Street

Madison, WI 53703

Phone: (608) 257-0040

ahalstead@hq-law.com

abibb@hq-law.com

Nicholas A. Migliaccio*

MIGLIACCIO & RATHOD LLP

412 H Street N.E., Suite 302

Washington, D.C. 20002

Phone: (202) 470-3520

nmigliaccio@classlawdc.com

Scott David Hirsch*

SCOTT HIRSCH LAW GROUP PLLC

6810 N. State Road 7

Coconut Creek, FL 33073

Tel: (561) 569-7062

scott@scotthirschlawgroup.com

*pro hac vice forthcoming

Attorneys for Plaintiff and Class Members

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Eileen Yeisley

(b) County of Residence of First Listed Plaintiff Linn
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Shindler Anderson Goplerud & Weese PC, 5015 Grand
Ridge Dr, West Des Moines, IA 50265, 515-223-4567

DEFENDANTS

University of Iowa Hospitals & Clinics

County of Residence of First Listed Defendant Johnson
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff ☒ 3 Federal Question
(U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant ☐ 4 Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State | <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 INTELLECTUAL PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
18 U.S.C. § 2511; 18 U.S.C. § 2702; 18 U.S.C. § 1030

Brief description of cause:

Disclosure of personally identifiable information as a result of tracking methods

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No**VIII. RELATED CASE(S) IF ANY**

(See instructions):

JUDGE

DOCKET NUMBER

DATE

April 21, 2023

SIGNATURE OF ATTORNEY OF RECORD

/s/ Brian O. Marty

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____