

Exhibit *A*

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

<i>L.C., individually and on behalf of all others similarly situated,</i> Plaintiff, v. FERTILITY CENTERS OF ILLINOIS, PLLC, Defendant.	Case No. JURY TRIAL DEMANDED
---	---

CLASS ACTION COMPLAINT

Plaintiff (“Plaintiff”) bring this class action lawsuit, individually and on behalf of all others similarly situated (the “Class Members”), against Fertility Centers of Illinois, PLLC (“Defendant”). The allegations set forth herein are based on Plaintiff’s personal knowledge and on information and good faith belief as to all other matters based upon investigation by counsel.

INTRODUCTION

1. Fertility treatment can be a difficult journey—both physically and emotionally. One in eight couples has trouble getting pregnant or carrying a pregnancy, and 7.4 million women have received infertility treatment.¹ Despite the prevalence of infertility, information concerning fertility and reproductive health is among the most confidential and sensitive information in our

¹See *How to Support Someone Experiencing Infertility*, <https://www.nm.org/healthbeat/healthy-tips/emotional-health/How-to-Support-Someone-Experiencing-Infertility> (last visited Feb. 28, 2024).

society. According to a recent study, most infertile women choose to keep their struggle private from family or friends.²

2. Regarding the need to keep information about reproductive health private, the Department of Health and Human Services (“HHS”) has noted:

A positive, trusting relationship between individuals and their health care providers is essential to an individual's health and well-being. The prospect of releasing highly sensitive PHI can result in medical mistrust and the deterioration of the confidential, safe environment that is necessary to quality health care, a functional health care system, and the public's health generally. That is even more true in the context of reproductive health care, given the potential for stigmatization and other adverse consequences to individuals resulting from disclosures they do not want or expect.³

3. The mishandling of such private and sensitive health information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.⁴ Simply put, if people do not trust that their sensitive private information will be kept private and secure, they may be less likely to seek medical and fertility treatment which can lead to much more serious health consequences down the road. In addition, protecting

²See *What to Say to Someone Struggling With Infertility*, <https://www.nytimes.com/2020/04/17/parenting/support-friend-infertility.html> (last visited Feb. 28, 2024).

³See *HIPAA Privacy Rule To Support Reproductive Health Care Privacy*, <https://www.federalregister.gov/documents/2023/04/17/2023-07517/hipaa-privacy-rule-to-support-reproductive-health-care-privacy> (last visited Feb. 28, 2024).

⁴See Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022) (“While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it’s even more verboten in addiction treatment, as patients’ medical history can be inherently criminal and stigmatized.”), <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited Feb. 28, 2024).

medical information and making sure it is kept confidential and not disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

4. Defendant Fertility Centers of Illinois, PLLC provides fertility treatment to couples seeking to start a family.⁵ Defendant has locations throughout Illinois and provides treatments such as artificial insemination, in vitro fertilization, and genetic testing.⁶

5. As part of the medical services it provides, Defendant owns, controls and maintains a website for its clinics, <https://www.fcionline.com> (the “Website”).

6. Defendant actively encourages patients and prospective patients to use the Website, to communicate with their healthcare providers, manage medical appointments for fertility services, and search medical conditions concerning fertility conditions and treatment options. The Website invites patients to share and search for personal medical information about their own reproductive health. And patients, trusting that this extremely private and sensitive information will be safeguarded, share intimate and personal medical information with Defendant through the Website.

7. Defendant knows that its patients expect the intimate details of their treatment to remain confidential. In an effort to reassure its patients that their information is protected, Defendant proclaims to its patients in its “Privacy Policy” that the “information collected through cookies *is not linked to any personally identifiable information.*”⁷ But Defendant does not live up to its promises.

⁵ See <https://www.fcionline.com/>.

⁶ See <https://www.fcionline.com/locations/>.

⁷ *Privacy Policy*, <https://www.fcionline.com/privacy-policy/> (emphasis added).

8. Unbeknownst to Plaintiff and Class Members, Defendant installed tracking technologies, including, but not limited to, the Meta Pixel, Google Analytics, and Google Ads, (collectively, the “Tracking Technologies”)⁸ on its Website to collect and disclose the private and confidential information of its patients to unauthorized third parties for its own pecuniary gain. The collection and transmission of this information is instantaneous, invisible and occurs without any notice to—and certainly no consent from—its patients.

9. The Meta Pixel, installed and configured by Defendant, is a piece of code that “tracks the people and [the] type of actions they take”⁹ as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).

10. The Tracking Technologies—which are configured by the website owners, here, Defendant—collect and transmit information from its patients’ browsers to unauthorized third parties, including, but not limited to, Facebook and Google.¹⁰

11. The data sent to Facebook also discloses a patient’s unique and persistent Facebook ID (“Facebook ID” or “FID”) which allows Facebook and other third parties to personally identify those patients and associates their private and confidential information with their Facebook profile.¹¹

⁸ This Complaint contains images and evidence demonstrating the Meta Pixel and Google tracking cookies were used on Defendant’s Website, but Plaintiff (without the benefit of discovery) does not have access to every tracking tool that was previously installed on the Website.

⁹ *Retargeting*, <https://www.facebook.com/business/goals/retargeting>

¹⁰ The pixel itself is a small snippet of code placed on webpages by the website owner. The process of adding the pixel to a webpage is a multi-step process that, as described in detail in *Section D*, must be undertaken by the website owner such as Defendant.

¹¹ The Facebook ID is a unique string of numbers Facebook uses to identify and connect to a

12. Similarly, Google intercepts several identifying pieces of information through its tracking technologies, including a patient's IP address and device information related to the specific computing device a consumer (or patient) is using to access a website. The device information intercepted by Google includes the patient's operating system, operating system version, browser, language, and screen resolution. Additionally, Google uses other tracking features, such as Universal Analytics, which allows Google to track the same user across multiple devices through its addition of the User-ID feature, which "associate[s] a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices."

13. Simply put (and as detailed herein), healthcare providers such as Defendant are *not* permitted to use tracking technology tools (like the Tracking Technologies) in a way that exposes patients' private and confidential information to any third party without express and informed consent from each patient. Neither Plaintiff nor any other Class Members were provided—much less signed—a written authorization permitting Defendant to disclose their private and confidential information to Facebook, Google, or any other third-party data brokers.

14. Plaintiff and Class Members who visited and used Defendant's Website reasonably believed that they were communicating only with their trusted healthcare provider.

patient's Facebook profile via, among other methods, a *c_user* cookie. Facebook creates a Facebook ID automatically, whether or not you choose to create a username. Thus, Facebook, which creates and maintains the Facebook ID directly connected to a patient's Facebook account, utilizes the Facebook ID to personally identify each patient whose private and confidential information is disclosed to it. See *Facebook Cookies Analysis*, <https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbfd8a>; see also https://www.cyberseo.net/blog/how-to-get-facebook-c_user-and-xs/

15. At no point has Defendant, despite intentionally incorporating invisible tracking code from unauthorized third parties into its Website, informed its patients that their personally identifiable information (“PII”) and protected health information (“PHI”) communicated via its Website was intentionally disclosed to a third party—let alone Facebook¹² and Google, who each have a sordid history of privacy violations.^{13,14}

16. As recognized by both the Federal Trade Commission (“FTC”) and the Office for Civil Rights (“OCR”) of HHS, healthcare companies’ use of tracking technologies to collect and divulge their patients’ sensitive and confidential information is an extremely serious data security and privacy issue:

Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.

In today’s surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. **But when companies use consumers’ sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.**¹⁵

¹² Meta Platforms, Inc. is doing business as “Meta” and “Facebook.” The terms “Meta” and “Facebook” are used interchangeably throughout.

¹³ This Court will not have to look far to find evidence of Meta’s violations of privacy laws. Just in May of last year, for instance, the European Union fined Meta “a record-breaking” \$1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record \$1.3 billion EU fine over data privacy*, <https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html>

¹⁴ Google has faced similar penalties and lawsuits. *See* <https://www.reuters.com/legal/google-settles-5-billion-consumer-privacy-lawsuit-2023-12-28/>

¹⁵ *See* Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis added), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases>

17. Similarly, the OCR is clear that “[r]egulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the Health Insurance Portability and Accountability Act (“HIPAA”) Rules.”¹⁶

18. There is no anonymity in the information disclosed to Facebook; that is, the Meta Pixel collects and discloses a substantial “data packet” coupled with the FID so that Defendant can, among other things, send targeted advertisements to patients (and others through Facebook’s Custom Audience features) based on their sensitive and protected PHI and PII. Defendant also uses this impermissibly obtained data for analytics purposes to gain additional insights into how its patients use its Website.

¹⁶ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, Dept. of Health and Human Services, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.htm> (noting that “IIHI collected on a regulated entity’s website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.”).

This guidance was recently vacated *in part* by the Federal District Court for the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited for reference only until the OCR updates its guidance, should it do so in the future. See *American Hosp. Ass’n. v. Becerra*, No. 4:23-cv-01110-P, ECF No. 67 (S.D. Tex., Jun. 20, 2024). Notably, the court’s order found only that the OCR’s guidance regarding covered entities disclosing to third parties users’ *IP addresses* while users navigated *unauthenticated public webpages* (“UPWs”) was improper rulemaking. The Order in no way affects or undermines the OCR’s guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. See *id.* at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the “Proscribed Combination” defined as “circumstances where an online technology connects (1) an individual’s IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers” but stating that “[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document.”). Furthermore, the FTC bulletin on the same topics remains untouched, as do the FTC’s enforcement actions against healthcare providers for committing the same actions alleged herein).

19. The same is true for Google, as it is able to match the IP addresses, device information, and User-IDs it intercepts and links such information to an individual's specific identity.

20. Operating as designed and as implemented by Defendant, the Tracking Technologies disclosed information that allows a third party (*e.g.*, Facebook and Google) to know when and where a specific patient was seeking confidential medical care, the medical condition(s) that patients inquired about, and the precise care the patient sought or received. Facebook and Google both, in turn, sell Plaintiff's and Class Members' PII and PHI to third-party marketers who target Plaintiff and Class Members.

21. For instance, when a patient accesses Defendant's Website where Tracking Technologies are present, the Tracking Technologies transmit the contents of their communications to Facebook and Google, including, but not limited to: (i) information about medical reproductive and fertility services and treatments; (ii) patient status; (iii) searches for specific doctors; (iv) the text of URLs visited by the patient; (v) requests to make an appointment; and (vi) other information that qualifies as PII and PHI under federal and state laws.

22. By installing the Tracking Technologies, Defendant effectively planted a bug on Plaintiff's and Class Members' web browsers and caused them to unknowingly disclose their private, sensitive and confidential health-related communications to Facebook and Google (and other third-party data brokers).

23. The information intercepted by the Tracking Technologies and third-party tracking technologies is used to build incredibly fulsome and robust marketing profiles for individual patients and create targeted advertisements based on the medical conditions and other PII and PHI. Despite the clear and unequivocal prohibition on the disclosure of PII and PHI without consent,

Defendant chose to use the data for it unlawfully disclosed for marketing purposes to bolster its revenue.

24. Simply put, Defendant put its desire for revenue over its patients' privacy rights.

25. As a healthcare provider, Defendant has certain duties and obligations to its patients. Defendant breached those duties and obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure its Website were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patients' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their PII and PHI to Facebook and Google or other third parties; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' PII and PHI through the Tracking Technologies; (v) failing to warn Plaintiff and Class Members about the Tracking Technology present on the Website; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient PII and PHI.

26. Plaintiff and Class Members have suffered injury because of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) compromise and disclosure of PII and PHI; (iv) diminution of value of their PII and PHI; (iv) statutory damages; and (v) the continued and ongoing risk to their PII and PHI.

27. Plaintiff seeks to remedy these harms for herself and a class of all others similarly situated for: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.* (the "ECPA"), Unauthorized Interception, Use and Disclosure; (ii) Negligence; (iii) Unjust Enrichment; and (iv) Violation of the Illinois Eavesdropping Statute, 720 ILCS § 5/14-1, *et. seq.*

PARTIES

28. Plaintiff L.C. is, and has been at all relevant times, a resident of the city of Chicago, Illinois. Plaintiff booked scheduled an appointment for fertility treatment through Defendant's Website on November 11, 2022.

29. Plaintiff attended her appointment and received fertility treatment from Defendant.

30. During the time Plaintiff scheduled an appointment on the Website she maintained an active social media account with Facebook. Plaintiff used the same device to access the Website and her Facebook account. Plaintiff's offsite activity report from her Facebook account confirmed that information related to her use of the Website was intercepted by Facebook.

31. Pursuant to the systemic processes described herein, Defendant assisted Facebook and Google with intercepting Plaintiff's communications, including those that contained personally identifiable information ("PII") and protected health information ("PHI"). This includes information related to the specific fertility treatment she received from Defendant. Defendant assisted Facebook and Google in intercepting this information without Plaintiff's knowledge, consent, or express written authorization.

32. By failing to receive the requisite consent, Defendant breached its duty of confidentiality and aided Facebook and Google in unlawfully intercepting Plaintiff's PII and PHI.

33. Such acts are egregious violations of Plaintiff's right to privacy.

34. Defendant Fertility Centers of Illinois, PLLC is an Illinois professional limited liability company with its principal place of business at 2555 Patriot Blvd, Glenview, IL 60026. Defendant owns and operates the Website and chose to embed the Tracking Technologies on its Website for advertising purposes.

JURISDICTION & VENUE

35. This Court has federal subject matter jurisdiction pursuant to 28 U.S.C. § 1331 over the claims that arise under 18 U.S.C. § 2511. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

36. This Court also 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.

37. The Court has personal jurisdiction over Defendant because its principal place of business and headquarters are located in Glenview, Illinois, it regularly engages in business in the State of Illinois and in Cook County and a substantial portion of the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this county.

38. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant that led to the unauthorized sharing of Plaintiff's and Class Members' PII and PHI; Defendant's principal place of business is located in this District; Defendant collects and redistributes Class Members' PII and PHI in this District and Defendant caused harm to Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Defendant Installed and Configured Facebook Tracking Technologies on its Website.

39. 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.¹⁷

40. 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.

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

42. Specifically, the Meta Pixel "tracks the people and type of actions they take."¹⁸ When a user accesses a webpage hosting the Meta Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers. Notably, this transmission does not occur unless the webpage contains the Meta Pixel.

43. The Meta Pixel is customizable and programmable, meaning that the website owner controls which of its web pages contain the Meta Pixel and which events are tracked and transmitted to Facebook.

44. The process of adding the Meta Pixel to webpages is a multi-step process that must be undertaken by the website owner.¹⁹

¹⁷*Facebook, Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx>

¹⁸ RETARGETING, <https://www.facebook.com/business/goals/retargeting>

¹⁹ Business Help Center: How to set up and install a Meta Pixel, <https://www.facebook.com/business/help/952192354843755?id=1205376682832142>

45. Facebook guides the website owner through setting up the Meta Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a pixel: “(1) Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you, or you can manually add code to your website. (2) Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website.”²⁰

46. Aside from the various steps to embed and activate the Meta Pixel, website owners, like Defendant, must also agree to Facebook’s Business Tools Terms by which Facebook requires website owners using the Meta Pixel to “represent and warrant” that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook’s Business Tools (including the Meta Pixel) and that websites “will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information”²¹

47. Stated differently, Plaintiff’s and Class Members’ PII and PHI would not have been disclosed to Facebook but for Defendant’s decisions to install the Meta Pixel on its Website.

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

²⁰ *Id.*

²¹ *Id.*; see also Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022) <https://www.newsbytesapp.com/news/science/facebook-collects-personaldata-on-abortion-seekers/story> (quoting Facebook spokesman Dale Hogan as saying that it is “against [Facebook’s] policies for websites and apps to send sensitive health data about people through [its] Business Tools”)

B. Defendant Installed and Configured Google Tracking Technologies on its Website.

49. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over \$1 trillion dollars. Google fancies itself a “tech” company, but Google, at its core, is an advertising company.

50. Google “make[s] money” from “advertising products [that] deliver relevant ads at just the right time,” generating “revenues primarily by delivering both performance advertising and brand advertising.”²² In 2020, Google generated \$146.9 billion in advertising revenue, which amounted to more than 80 percent of Google’s total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

Figure 1:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	\$257.6 billion	\$209.5	81.33%
2020	\$182.5 billion	\$146.9 billion	80.49%
2019	\$161.9 billion	\$134.8 billion	83.29%
2018	\$136.8 billion	\$116.5 billion	85.12%

51. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google’s SDK and pixel integrate with Google’s advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google’s ad network and products increasing Google’s overall ad revenue. Products like Google’s SDK and its tracking pixel also improve the company’s advertising network and capabilities by providing more wholesome profiles and data points on individuals.

²² ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm>.

52. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

53. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth information about user behavior. Also, Universal Analytics enabled tracking the same user across multiple devices through its addition of the User-ID feature, which “associate[s] a persistent ID for a single user with that user’s engagement data from one or more sessions initiated from one or more devices.”

54. In 2020, Google launched Google Analytics 4, a platform combining Google Analytics with Firebase to analyze both app and web activity.

55. Since launching Google Analytics, Google has become one of the most popular web analytics platforms on the internet. Indeed, Google had a \$62.6 billion increase in advertising revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

56. Google touts Google Analytics as a marketing platform that offers “a complete understanding of your customers across devices and platforms.”²³ It allows companies and advertisers that utilize it to “understand how your customers interact across your sites and apps, throughout their entire lifestyle,” “uncover new insights and anticipate future customer actions

²³ *Analytics*, GOOGLE, <https://marketingplatform.google.com/about/analytics/>

with Google’s machine learning to get more value out of your data,” “take action to optimize marketing performance with integrations across Google’s advertising and publisher tools,” and “quickly analyze your data and collaborate with an easy-to-use interface and shareable reports.”²⁴

57. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site. This code immediately intercepts a user’s interaction with the webpage every time the user visits it, including what pages they visit and what they click on. The code also collects PII, such as IP addresses and device information related to the specific computing device a consumer (or patient) is using to access a website. The device information intercepted by Google includes the patient’s operating system, operating system version, browser, language, and screen resolution.

58. Once Google’s software code collects the data, it packages the information and sends it to Google Analytics for processing. Google Analytics enables the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google Analytics database and cannot be changed.

59. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on acquisition (e.g., information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (e.g., classify your users by age,

²⁴ *Id.*

location, language, and gender, along with interests they express through their online browsing and purchase activities).

60. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

61. Google Analytics links with Google Ads, so that Google may use the data intercepted by Google Analytics to be utilized for targeted advertising purposes.²⁵ Such practices were in effect on Defendant's Website at all relevant times.

62. The Website utilizes Google's pixel and SDK. As a result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least "Custom Events" and URLs that disclosed the specific fertility treatment being received by the patient. Google also received additional PII, including the patients' IP address, device information, and User-IDs.

63. Google collects vast quantities of consumer data through its tracking technology.

64. Due to the vast network of consumer information held by Google, it is able to match the IP addresses, device information, and User-IDs it intercepts and link such information to an individual's specific identity.

65. Google then utilizes such information through targeted advertising.

C. Defendant Assisted Third Parties in Intercepting Patients' Communications with its Website and Disclosed Their Private Information to Third Parties.

66. Defendant's Website is accessible on mobile devices and desktop computers and allows patients to communicate with Defendant regarding their medical care.

²⁵ <https://support.google.com/analytics/answer/9379420?hl=en#zippy=%2Cin-this-article>

67. Defendant encouraged patients to use its Website to communicate their PII and PHI, schedule appointments, access information about their treatments, pay medical bills and more.

68. Despite this, Defendant purposely installed Tracking Technologies on its Website and programmed specific webpage(s) to surreptitiously share its patients' private and protected communications, including Plaintiff's and Class Members' PHI and/or PII, which was sent to Facebook and Google.

69. The Tracking Technologies followed, recorded and disseminated patients' information as they navigated and communicated with Defendant via the Website, simultaneously transmitting the substance of those communications to unintended and undisclosed third parties.

70. The information disseminated by the Tracking Technologies and/or intercepted by third parties constitutes PII and PHI including medical information patients requested or viewed, the title of any buttons clicked (such as the "Treatments" drop down page which identifies and communicates the specific medical conditions and treatments of a patient), the exact phrases typed into text boxes, selections made from drop-down menus or while using filtering tools and other sensitive and confidential information, the divulgence of which is and was highly offensive to Plaintiff.

71. This is PHI because the webpages have access to "information that relates to any individual's past, present, or future health, health care, or payment for health care."²⁶

72. The information collected and disclosed by Defendant's Tracking Technologies is not anonymous and is viewed and categorized by the intercepting party on receipt.

²⁶ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited June 20, 2024) (vacated by *American Hospital Association, et al. v Xavier Becerra, et al.*, No. 4:23-cv-01110-P, Dkt. No. 67 (N.D. Tex. June 20, 2024)).

73. The information Facebook received via the Tracking Technologies was linked and connected to patients' Facebook profiles (via their Facebook ID or "c_user id"), which includes other PII.

74. Similarly, Google stores users' logged-in identifier on non-Google websites in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses this data to serve personalized ads.²⁷

75. Simply put, the health information that was disclosed via the Tracking Technologies is personally identifiable and was sent alongside other persistent unique identifiers such as the patients' IP address, Facebook ID, User-IDs, and device identifiers.²⁸

D. Defendant's Method of Transmitting Plaintiff's & Class Members' PII and PHI via Tracking Technologies.

76. 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" (computer, tablet or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome, Mozilla's Firefox, Apple's Safari, and/or Microsoft's Edge browsers).

77. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' devices as their web browsers query the server through the internet.

²⁷ See *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) (order denying summary judgment and citing internal evidence from Google employees).

²⁸ See *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1056 (N.D. Cal. 2021) (discussing how Google collects personal information and IP addresses); see also <https://developers.facebook.com/docs/meta-pixel/>

78. Web communications consist of Hypertext Transfer Protocol (“HTTP”) or Hypertext Transfer Protocol Secure (“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:

1. **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 to file a motion to a court.)
2. **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.
3. **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.

79. A patient’s HTTP request essentially asks Defendant’s Website to retrieve certain information (such as a set of health screening questions). 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 participants’ screens as they navigate Defendant’s Website.

80. Every website is comprised of Markup and “Source Code.” Source Code is a simple set of instructions that commands the website user’s browser to take certain actions when the webpage first loads or when a specified event triggers the code.

81. 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.

82. The Tracking Technologies are Source Code that do just that—they surreptitiously transmit a Website User’s communications and inputs to the corresponding user IDs, much like a traditional wiretap.

83. For example, when individuals visit Defendant’s Website via an HTTP request to Defendant’s server, Defendant’s server sends an HTTP response (including the Markup) that displays the webpage visible to the User, along with Source Code (including the Tracking Technologies).

84. Thus, Defendant is, in essence, handing its patients a tapped website and, once a webpage is loaded into the patient’s browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Tracking Technologies, which then intercept those communications—intended only for Defendant—and instantaneously transmit those communications to Facebook and Google or another corresponding user IDs.

85. Third parties like Facebook and Google place 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 identify the specific user associated with the information intercepted (in this case, highly sensitive PII and PHI).

86. For example, Facebook uses cookies named c_user, datr, fr and fbp to identify its account holders. Facebook stores or updates Facebook-specific cookies every time a person accesses their Facebook account from the same web browser.

87. The Meta Pixel can access these cookies and send certain identifying information like the user’s Facebook ID to Facebook along with the other data relating to the user’s website inputs.

88. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

89. A User's Facebook 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, Facebook—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. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

90. The Facebook datr cookie identifies the User's web browser. It is an identifier unique to each person's specific web browser and is another way Facebook can identify Facebook users.

91. The Facebook fr cookie is a combination of the Facebook ID (c_user) and the browser ID (datr) cookie values.

92. A User who accessed Defendant's Website while logged into (or recently having logged into) Facebook would have their browser transmit the c_user, datr and fr cookies to Facebook.

93. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.

94. Google acts in a similar manner, matching the IP addresses, device information, and User-IDs it intercepts and linking such information to an individual's specific identity.

95. For example, Google utilizes a “cid” or “Client ID,” which is a unique identifier utilized by Google and Defendant to “track [a] user[’s] interactions across sessions.” “Its primary purpose is to uniquely identify users across sessions.”²⁹

96. Similarly, Google also utilizes the “auid” or “Advertiser User ID,” and “guid” or “Globally Unique Identifier,” cookies which identify unique users and unique interactions with a website.

97. Defendant sent these identifiers with each patient’s “event” data.

98. Defendant intentionally configured the Tracking Technologies installed on its Website to capture both the “characteristics” of individual patients’ communications with its Website (their IP addresses, Facebook ID, User-IDs, cookie identifiers, device identifiers, emails, and phone numbers) and the “content” of these communications (the buttons, links, pages, and tabs they click and view related to their fertility-related health conditions and services sought from Defendant).

99. This disclosed PHI and PII allows Facebook and Google to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Defendant to target those persons with Defendant’s ads, Facebook and Google also then sells that information to marketers who will target Plaintiff and Class Members.

100. Defendant intercepted and disclosed the following non-public private information to Facebook and Google:

- a. Plaintiff’s and Class Members’ status as medical patients;
- b. Plaintiff’s and Class Members’ communications with Defendant through its Website, including medical conditions for which they sought treatments and treatments sought;

²⁹ [https://www.owox.com/blog/use-cases/google-analytics-client-id#:~:text=The%20Client%20ID%20\(cid\)%20or,unique%20users%20using%20this%20parameter.](https://www.owox.com/blog/use-cases/google-analytics-client-id#:~:text=The%20Client%20ID%20(cid)%20or,unique%20users%20using%20this%20parameter.)

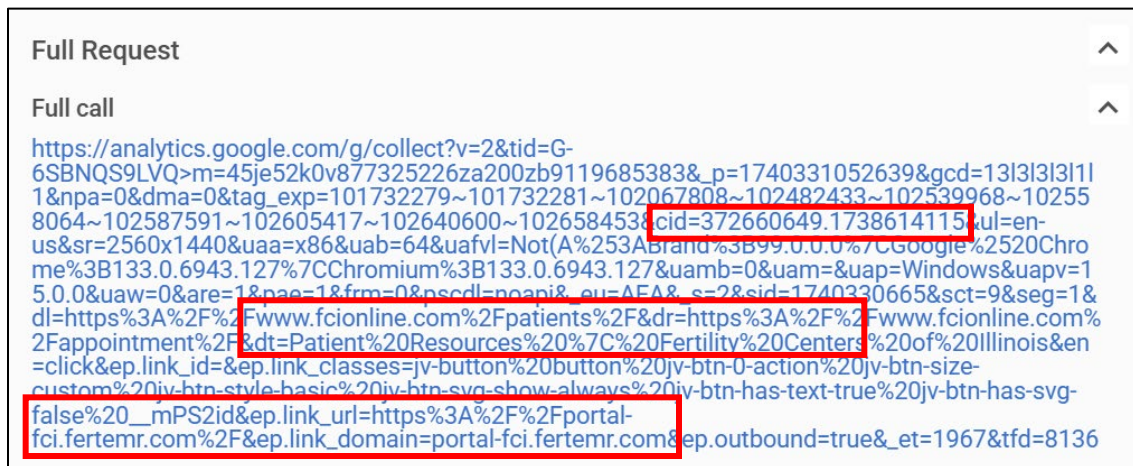
- c. Plaintiff's and Class Members' searches for doctors;
- d. Plaintiff's and Class Members' contacting Defendant and making appointments for medical care; and
- e. PII, including but not limited to patients' locations, IP addresses, device identifiers, individual's unique Facebook ID, user-IDs, and other unique personal identifiers.

101. Through the Website, Defendant shares its patients' identities and online activity, including information and search results related to their private medical treatment.

102. When patients navigate the Website, the Tracking Technologies embedded by Defendant immediately begin intercepting their communications with the Website.

103. For example, when a patient selects the "Patient Portal" link to access their account, Defendant discloses that communication to Google:

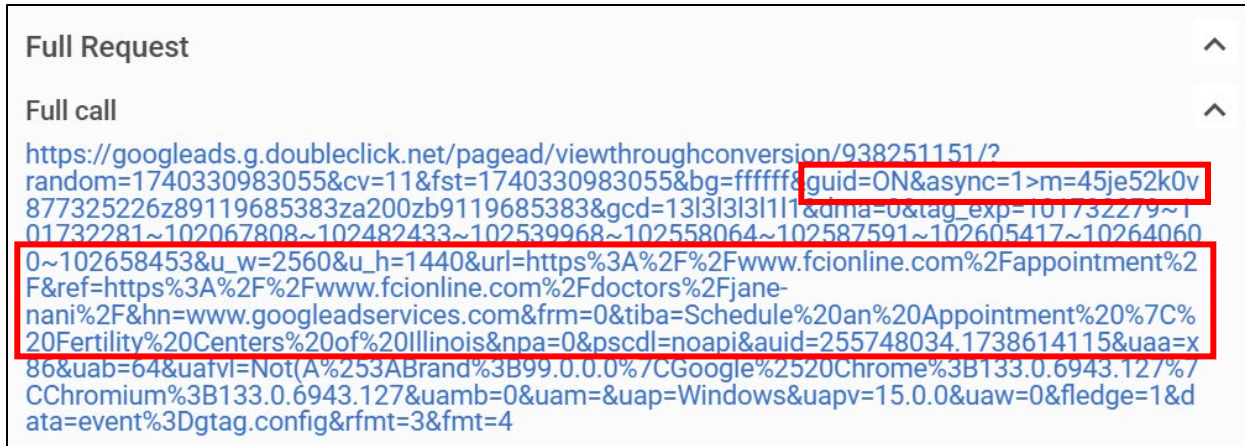
Figure 2:



104. When navigating Defendant's Website, patients can search for the fertility treatments and doctors they are interested in scheduling appointments with, as shown in Figures 3-6:

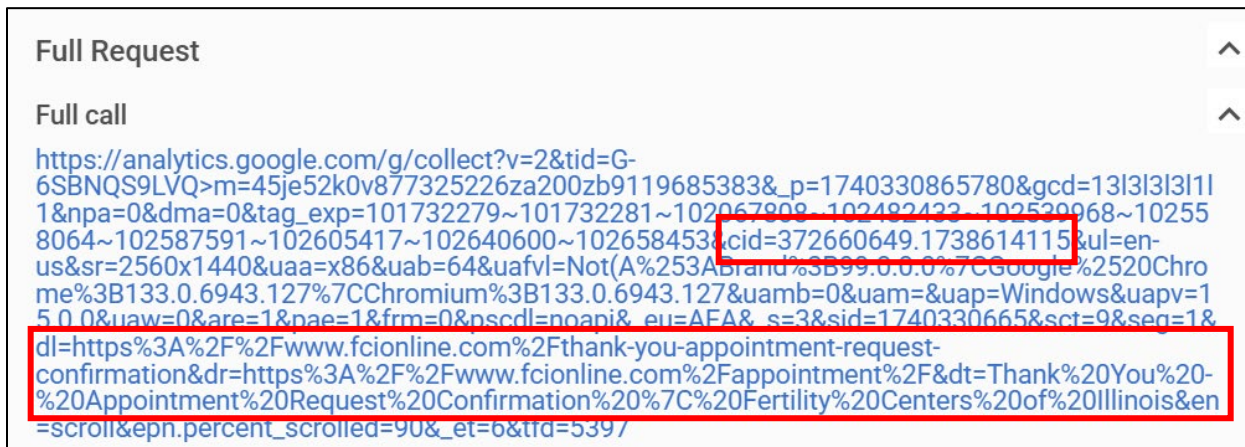
Figures 3-6:

Full Request Full call https://analytics.google.com/g/collect?v=2&tid=G-6SBNQS9LVQ>m=45je52k0v877325226z89119685383za200zb9119685383&_p=1740330668366&gcd=13l3l3l3l1l1&npa=0&dma=0&tag_exp=101732279~101732281~102067808~102482433~102539968~102558064~102587591~102605417~102640600~102658453&cid=372660649.1738614115&ul=en-us&sr=2560x1440&uaa=x86&uab=64&uafvl=Not(A%253ABrand%3B99.0.0.0%7CGoogle%2520Chrome%3B133.0.6943.127%7CChromium%3B133.0.6943.127&uamb=0&uam=&uap=Windows&uapv=15.0.0&uaw=0&are=1&pae=1&frm=0&pscdl=noapi&_s=1&sid=1740330665&sct=9&seg=1&dl=https%3A%2F%2Fwww.fcionline.com%2Ftreatments%2Fin-vitro-fertilization-ivf%2F&dr=https%3A%2F%2Fwww.fcionline.com%2Ftreatments%2F&dt=What%20is%20IVF%3F%20%7C%20In%20Vitro%20Fertilization%20%7C%20Fertility%20Center%20of%20Illinois&en=page_view&tfd=5347	^ ^
Full Request Full call https://googleads.g.doubleclick.net/pagead/viewthroughconversion/938251151/?random=1740330668614&cv=11&fst=1740330668614&bg=ffffff&guid=ON&async=1>m=45je52k0v877325226z89119685383za200zb9119685383&gcd=13l3l3l3l1l1&dma=0&tag_exp=101732279~101732281~102067808~102482433~102539968~102558064~102587591~102605417~102640600~102658453&u_w=2560&u_h=1440&url=https%3A%2F%2Fwww.fcionline.com%2Ftreatments%2Fin-vitro-fertilization-ivf%2F&ref=https%3A%2F%2Fwww.fcionline.com%2Ftreatments%2F&nn=www.googleadservices.com&frm=0&tiba=What%20is%20IVF%3F%20%7C%20In%20Vitro%20Fertilization%20%7C%20Fertility%20Center%20of%20Illinois&npa=0&pscdl=noapi&uid=255748034.1738614115&uaa=x86&uab=64&uafvl=Not(A%253ABrand%3B99.0.0.0%7CGoogle%2520Chrome%3B133.0.6943.127%7CChromium%3B133.0.6943.127&uamb=0&uam=&uap=Windows&uapv=15.0.0&uaw=0&fledge=1&data=event%3Dgtag.config&rfmt=3&fmt=4	^ ^
Full Request Full call https://analytics.google.com/g/collect?v=2&tid=G-6SBNQS9LVQ>m=45je52k0v877325226za200zb9119685383&_p=1740330982981&gcd=13l3l3l3l1l1&npa=0&dma=0&tag_exp=101732279~101732281~102067808~102482433~102539968~102558064~102587591~102605417~102640600~102658453&cid=372660649.1738614115&ul=en-us&sr=2560x1440&uaa=x86&uab=64&uafvl=Not(A%253ABrand%3B99.0.0.0%7CGoogle%2520Chrome%3B133.0.6943.127%7CChromium%3B133.0.6943.127&uamb=0&uam=&uap=Windows&uapv=15.0.0&uaw=0&are=1&pae=1&frm=0&pscdl=noapi&_eu=AEA&_s=2&sid=1740330665&sct=9&seq=1&dl=https%3A%2F%2Fwww.fcionline.com%2Fappointment%2F&dr=https%3A%2F%2Fwww.fcionline.com%2Fdoctors%2Fjane-nani%2F&dt=Schedule%20an%20Appointment%20%7C%20Fertility%20Centers%20of%20Illinois&en=scroll&eph.percent_scrolled=90&_et=44&tfd=5188	^ ^

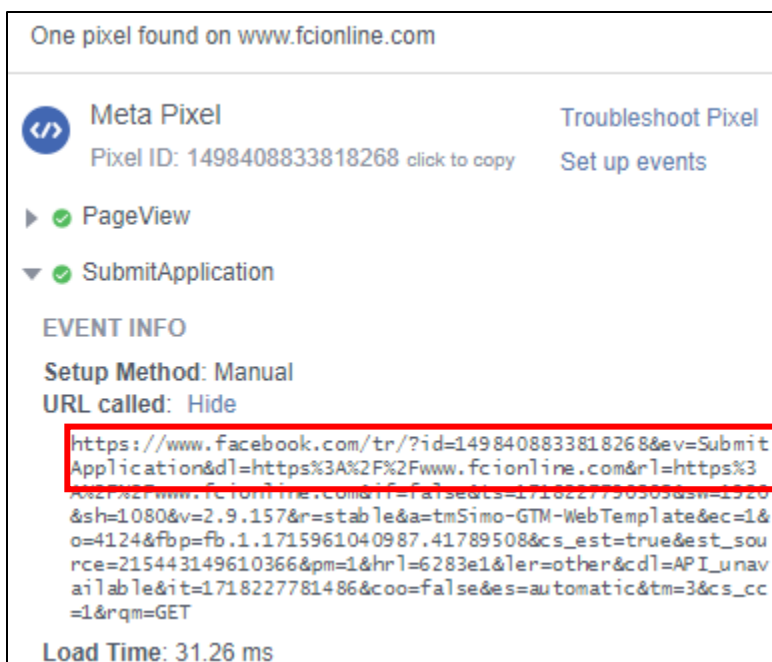


105. When a patient completes the process to schedule an appointment for fertility treatment on Defendant’s Website, Defendant assists Google and Facebook with intercepting that information as well:

Figures 7-8³⁰:



³⁰ Specifically, a “SubmitApplication” event, as shown in Figure 8, indicates to Facebook that a patient “applie[d] for a product, service, or program you offer.” See META, <https://developers.facebook.com/docs/meta-pixel/reference/>. Here, Defendant only offers one service, namely, fertility treatment.



106. The patient's selections and filters are transmitted to Facebook and Google via the Tracking Technologies, even if they contain the patient's treatment, procedures, medical conditions, or related queries, without alerting the patient and the communications Defendant sends to Facebook and Google also contain the patient's PII and personal identifiers, including but not limited to their Facebook ID, IP address, fbp, datr and fr cookies, User-IDs, and device information, along with the search filters the patient selected.

107. In each of the examples above, the patient's website activity and the contents of their communications are sent to Facebook and Google alongside their PII. Several different methods allow marketers and third parties to identify individual consumers, but the examples above demonstrate what happens when the website patient is logged into Facebook on their web browser or device. When this happens, the Users' identity is revealed via third-party cookies that work in conjunction with the Tracking Technologies.

108. Defendant did not seek and did not have Plaintiff's and Class Members' consent to share any of the sensitive PII and PHI described above.

E. Defendant's Use of the Tracking Technologies Violated Its Own Privacy Policies.

109. Defendant's privacy policy represents to patients and visitors to its Website that it will keep their Personal Information, including their PHI, private and secure and that it will only disclose PHI provided to them under certain circumstances, ***none of which apply here.***³¹

110. With respect to tracking technologies and analytics, Defendant's privacy policy does not disclose to its patients that it discloses their PHI and PII to third-parties, including Facebook and Google.

111. For example, when discussing cookies specifically, Defendant's Privacy Policy admits that it collects information about its patients, but that "information collected through cookies is not linked to any personally identifiable information."³²

112. Patients are not informed about and have not consented to the disclosure of their PII and PHI and their Website activity to a third party, including Facebook and Google.

113. This is precisely the type of information for which HIPAA requires healthcare providers to utilize de-identification techniques to protect the privacy of patients.³³

114. Despite a lack of disclosure, Defendant allows Facebook and Google to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information that it promises to keep private.

115. Defendant breached its own privacy policies by unlawfully permitting Facebook and Google and likely other third parties to intercept patients' PII and PHI without obtaining

³¹ See <https://www.fcionline.com/privacy-policy/>

³² See *Id.*

³³ See <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>

patients' consent or authorization. Facebook and Google then read, understood, and used that PII and PHI for its own business purposes—i.e., selling targeted advertising to Defendant (and other companies) which specifically targeted those patients based on their reproductive health conditions.

F. Defendant Violated HIPAA.

116. Defendant's disclosure of Plaintiff's and Class Members' PII and PHI to entities like Facebook and Google also violated HIPAA.

117. Under federal law, a healthcare provider may not disclose PII, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.³⁴

118. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

119. HIPAA's Privacy Rule defines "individually identifiable health information" ("IIHI") as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

³⁴ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

120. The Privacy Rule broadly defines protected health information as IIIHI that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

121. Under the HIPAA de-identification rule, “health information is not individually identifiable only if”: (i) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination” or (ii) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

- A. Names;
- ...
- H. Medical record numbers;
- ...
- J. Account numbers;
- ...
- M. Device identifiers and serial numbers;
- N. Web Universal Resource Locators (URLs);
- O. Internet Protocol (IP) address numbers; ... and
- P. Any other unique identifying number, characteristic, or code... and” the covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”³⁵

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

123. Even the fact that an individual is receiving a medical service, i.e., is a patient of a particular entity, can be PHI.

³⁵ See 45 C.F.R. § 160.514.

124. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, “[i]f 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.”³⁶

125. Consistent with this restriction, HHS has issued marketing guidance that provides, “With limited exceptions, the [Privacy] 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 or enrollees to third parties without obtaining authorization from each person on the list.”³⁷

126. Here, as described *supra*, Defendant provided patient information to third parties in violation of the Privacy Rule—and its own Privacy Policy. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.”

127. The statute states that a “person . . . shall be considered to have obtained or disclosed individually identifiable health information . . . if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320(d)(6).

³⁶ See *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>.

³⁷ *Marketing*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html>

128. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually identifiable health information relating to an individual “shall be fined not more than \$250,000, imprisoned not more than 10 years, or both.” 42 U.S.C. § 1320(d)(6)(b)(1).

129. HIPAA also requires Defendant to “review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information,” 45 C.F.R. § 164.306I, and to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights,” 45 C.F.R. § 164.312(a)(1)—which Defendant failed to do.

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

131. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

- a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained and transmitted in violation of 45 C.F.R. section 164.306(a)(1);
- b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);
- c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation of 45 C.F.R.

section 164.308(a)(6)(ii);

- d) Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);
- e) Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3); and
- f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

132. In disclosing the content of Plaintiff's and Class Members' communications, Defendant had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions, that is, to illegally disclose Plaintiff's and Class Members' PII and PHI to third parties, like Facebook and Google, in violation of HIPAA, including 42 U.S.C. § 1320d-6(a)(3), as well as the torts alleged below.

133. Defendant intercepted the content of Plaintiff's and Class Members' communications, including their PII and PHI, for a criminal and tortious purpose. Defendant would not have been able to obtain the PII and PHI or the marketing services it did if it had complied with the law.

G. Patients' Reasonable Expectation of Privacy.

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

135. Indeed, when Plaintiff and Class Members provided their PII and PHI to Defendant, they each had a reasonable expectation that the information would remain private, and that

Defendant would not share the PII or PHI with third parties for a commercial purpose unrelated to patient care.

136. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

137. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.³⁸

138. Personal data privacy and obtaining consent to share PII and PHI are material to Plaintiff and Class Members.

139. Plaintiff's and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as healthcare providers, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

H. Defendant was Enriched by & Benefitted from the Use of Tracking Technologies.

140. Defendant decided to embed the Tracking Technologies on its Website with the purpose of disclosing Plaintiff's and Class Members's communications to Facebook and Google

³⁸ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/>

in order to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to Defendant and boost its revenue.

141. After receiving individually identifiable patient health information communicated on Defendant's Website, Facebook and Google analyze this data, improve their own technology and businesses (including machine learning), and then forward this data and analysis of this data, to Defendant.

142. Defendant then uses this data and analysis for its own commercial purposes that include understanding how patients utilize its Website.

143. Facebook and Google, as well, use this data and analysis for their own commercial purposes, including to improve their platforms and better understand the individuals that make up the audiences that their clients (advertisers) pay Facebook and Google to target with ads.

144. Defendant also receives an additional commercial benefit from using Facebook and Google's tracking tools in being able to serve more targeted advertisements to existing and prospective patients.

145. Plaintiff's and Class Members' PII and PHI has considerable value as highly monetizable data, especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

146. In exchange for disclosing the PII and PHI of their account holders and patients, Defendant is compensated by Facebook and Google in the form of enhanced advertising services and more cost-efficient marketing on their platforms.

147. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.³⁹

148. For example, Freshpaint, a healthcare marketing vendor, cautioned that “Meta isn’t HIPAA-compliant. They don’t sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers,” and “[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now.”⁴⁰

149. Medico Digital also warns that “retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences.”⁴¹

150. Whether a user has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the pixels’ ability to track comprehensive browsing history is also relevant. *See, e.g., Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).

151. Upon information and good faith belief, Defendant retargeted patients and potential patients, including Plaintiff and Class Members.

³⁹ *See The guide to HIPAA compliance in analytics*, <https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf> (explaining that Google Analytics 4 is not HIPAA-compliant)

⁴⁰ *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra* note 90.

⁴¹ *The complex world of healthcare retargeting*, *supra* note 89.

152. Thus, utilizing the Tracking Technologies directly benefits Defendant by, among other things, reducing the cost of advertising and retargeting.

I. Plaintiff's Private Information has Financial Value.

153. Plaintiff's and Class Members' PII and PHI has value, and Defendant's disclosure and interception harmed Plaintiff and Class Members by not compensating them for the value of their PII and PHI and, in turn, decreasing the value of their PII and PHI.

154. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

155. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

156. The robust market for Internet user data has been analogized to the "oil" of the tech industry.⁴² A 2015 article from TechCrunch accurately noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."⁴³ That article noted that the value of a single Internet user—or really, a single user's data—varied from about \$15 to more than \$40.

157. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data (after costs).⁴⁴ That figure is only due to keep

⁴² See <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

⁴³ See <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>

⁴⁴ See *What Your Data is Really Worth to Facebook* (July 12, 2019), <https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/>

increasing; estimates for 2022 were as high as \$434 per user, for a total of more than \$200 billion industry wide.

158. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: “Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.”⁴⁵

159. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.⁴⁶

160. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

161. Courts recognize the value of personal information and the harm when it is disclosed without consent.⁴⁷

⁴⁵ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

⁴⁶ See *10 Apps for Selling Your Data for Cash*, <https://wallethacks.com/apps-for-selling-your-data/>

⁴⁷ See, e.g., *In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that Plaintiff's allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing “the value that personal identifying information has in our increasingly digital economy”).

162. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

163. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

164. The value of health data is well-known and various reports have been conducted to identify its value.

165. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."⁴⁸

166. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).⁴⁹

167. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a

⁴⁸See

<https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf>

⁴⁹ See <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

Hidden Multi-Billion Dollar Industry,” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.⁵⁰

168. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”⁵¹

169. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

170. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users’ stolen data, surely Internet users can sell their own data.

171. In short, there is a quantifiable economic value to Internet users’ data that is greater than zero. The exact number will be a matter for experts to determine.

172. Defendant shared Plaintiff’s and Class Members’ communications and transactions on its Website without permission.

173. The unauthorized access to Plaintiff’s and Class Members’ PII and PHI has diminished the value of that information, resulting in harm to Defendant’s patients, including Plaintiff and Class Members.

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

⁵⁰ See <https://time.com/4588104/medical-data-industry/>

⁵¹ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html>

TOLLING

175. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of its incorporation of the Tracking Technologies into its Website.

176. The Tracking Technologies on Defendant's Website were and are entirely invisible to a website visitor.

177. Through no fault or lack of diligence, Plaintiff and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

178. Plaintiff was ignorant of the information essential to pursue her claims, without any fault or lack of diligence on her part.

179. Defendant had exclusive knowledge that its Website incorporated the Tracking Technologies and yet failed to disclose to customers, including Plaintiff and Class Members, that by searching for and scheduling fertility treatment, Plaintiff's and Class Members' PII and PHI would be disclosed or released to unauthorized third parties, like Facebook and Google.

180. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its customers' PII and PHI. In fact, to the present Defendant has not conceded, acknowledged, or otherwise indicated to its customers that it has disclosed or released their PII and PHI to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

181. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

182. The earliest that Plaintiff or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of this Complaint.

183. Plaintiff first discovered that Defendant had collected and shared her PII and PHI without her consent on or around June 2024 after contacting undersigned counsel and discussing potential claims against Defendant.

CLASS ACTION ALLEGATIONS

184. **Class Definition:** Plaintiff brings this action individually and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

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

All individuals residing in the United States who used Defendant's Website and had their PII and PHI shared with unauthorized third parties including, but not limited to, Facebook and Google, during the applicable statutory period.

186. The Illinois Sub-Class that Plaintiff seeks to represent is defined as:

All individuals residing in Illinois who used Defendant's Website and had their PII and PHI shared with unauthorized third parties including, but not limited to, Facebook and Google, during the applicable statutory period.

187. Plaintiff reserves the right to modify the class definition or add sub-classes as necessary prior to filing a motion for class certification.

188. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgment.

189. The Nationwide Class, and the Illinois Sub-Class are referred to collectively as the "Classes."

190. Excluded from the proposed Classes are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by

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

191. Plaintiff reserves the right to amend the definitions of the Class or Sub-class and add subclasses if further information and discovery indicate that the definitions should be narrowed, expanded or otherwise modified.

192. Numerosity/Ascertainability. Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff at this time. However, it is estimated that there are at least thousands of individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's records and non-parties Facebook's and Google's records.

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

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

195. Common Questions of Law and Fact. Questions of law and fact common to the Classes predominate over questions that may affect only individual Class Members because

Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Classes:

- a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' PII and PHI;
- b. Whether Defendant had duties not to disclose Plaintiff's and Class Members' PII and PHI to unauthorized third parties;
- c. Whether Defendant violated its privacy policies by disclosing Plaintiff's and Class Members' PII and PHI to Facebook, Google, or other 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 disclosed without their consent;
- f. Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of patient's PII and PHI;
- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII and PHI;
- h. Whether Defendant knowingly made false representations or

omitted material representations as to their data security and/or privacy policy practices;

- i. Whether Defendant knowingly omitted material representations with respect to their data security and/or privacy policy practices;
- j. Whether Defendant's acts and practices violated Plaintiff's and Class Members' privacy rights;
- k. Whether Plaintiff and Class Members are entitled to actual, consequential or nominal damages as a result of Defendant's wrongful conduct; 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 Defendant's disclosure of their PII and PHI.

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

CLAIMS FOR RELIEF

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT

18 U.S.C. § 2511(1), *et seq.*

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

198. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

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

200. 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.

201. The transmissions of Plaintiff’s PII and PHI to Defendant’s Website qualifies as a “communication” under the ECPA’s definition of 18 U.S.C. § 2510(12).

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

203. 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).

204. Interception. The ECPA defines an 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).

205. Electronical, 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).

206. The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies Defendant, Facebook, and Google use to track Plaintiff’s and the Class Members’ communications;
- b. Plaintiff’s and Class Members’ browsers;
- c. Plaintiff’s and Class Members’ computing devices;
- d. Defendant’s web-servers and
- e. The Tracking Technologies deployed by Defendant to effectuate sending and acquiring patients’ sensitive communications.

207. Whenever Plaintiff and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Technologies embedded and operating on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff’s and Class Members’ electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

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

209. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies it embedded and operated on its Website, contemporaneously and intentionally redirected and disclosed the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

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

211. Additionally, through the above-described Tracking Technologies and intercepted communications, this information was, in turn, used by third parties, such as Facebook and Google, to 1) place Plaintiff and Class Members in specific health-related categories based on their past, present and future health conditions and 2) target Plaintiff and Class Members with particular advertising associated with Plaintiff's and Class Members specific health conditions and fertility treatment(s).

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

213. 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).

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

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

216. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Tracking Technologies.

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

218. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State, such as Illinois—namely, violations of HIPAA, among others.

219. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

220. Defendant is a “party to the communication” with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding and/or interception of Plaintiff's and Class Members' PII and PHI does not qualify for the party exemption.

221. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party. HIPAA defines IIHI as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

222. Plaintiff's information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Technologies to intercept and then disclose Plaintiff's and Class Members' PII and PHI for financial gain.

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

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

- a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and
- b. Disclosed IIHI to Facebook and Google without patient authorization.

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

226. Healthcare patients have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause the Tracking Technologies and other tracking codes (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiff's and Class Members' computing devices as "first-party" cookies that are not blocked.

227. The _fbp, auid, cid, and guid cookies, which constitute programs, commanded Plaintiff's and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

228. Defendant knew or had reason to know that the fbp, auid, cid, and guid cookies would command Plaintiff's and Class Members' computing devices to remove, redirect, and disclose their data and the content of their communications with Defendant to Google, Facebook, and others.

229. Defendant's scheme or artifice to defraud in this action consists of: (a) the false and misleading statements and omissions in its privacy policy (HIPAA Notice) set forth above, including the statements and omissions recited in the claims below and (b) the placement of the 'fbp,' 'auid,' 'cid,' and 'guid' cookies on patient computing devices disguised as first-party cookies on Defendant's Website rather than as third-party cookies from Facebook and Google.

230. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property rights (a) to the confidentiality of PII and PHI and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes and (b) to determine who has access to their computing devices.

231. As such, Defendant cannot viably claim any exception to ECPA liability.

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

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their IIHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, treatments, and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' IIHI without providing any value or benefit to Plaintiff or the Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' IIHI, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiff or the Class Members;
- d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and
- e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiff and Class Members intended to remain private no longer private.

233. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II
NEGLIGENCE

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

235. Defendant owed Plaintiff and Class Members a duty to keep their PII and PHI completely confidential, and to safeguard sensitive personal and medical information.

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

237. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Technologies to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including PII and PHI and the contents of such information.

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

239. The third-party recipients included, but may not be limited to, Facebook and/or Google.

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

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Plaintiff and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' PII and PHI; and
- i. Defendant's actions violated the property rights Plaintiff and Class Members have in their PII and PHI.

COUNT III
UNJUST ENRICHMENT

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

242. This claim is pleaded in the alternative to Plaintiff's other causes of action.

243. Defendant benefits from the use of Plaintiff's and Class Members' PII and PHI and

unjustly retained those benefits at their expense.

244. Plaintiff and Class Members conferred a benefit upon Defendant in the form of PII and PHI that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

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

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

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

248. 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.

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

250. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with

reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

251. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts and trade practices alleged in this Complaint.

252. 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 IV
Violation of the Illinois Eavesdropping Statute
720 ILCS § 5/14-1, *et seq.*

253. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count on behalf of herself and the proposed Illinois Subclass.

254. The Illinois Eavesdropping Statute (“IES”), 720 ILCS § 5/14-1, *et seq.*, prohibits the surreptitious interception, recording, or transcription of private electronic communications without the consent of all parties to the conversation and provides a civil cause of action to a person subjected to a violation of the IES against eavesdroppers and their principals.

255. Under 720 ILCS § 5/14-2(a)(3), the IES makes it unlawful for a person to knowingly and intentionally intercept, record, or transcribe, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication.

256. Under 720 ILCS § 5/14-2(a)(5), the IES makes it unlawful for a person to knowingly and intentionally use or disclose any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of the IES, unless he or she does so with the consent of all of the parties.

257. Under 720 ILCS § 5/14-2(a)(4), the IES makes it unlawful for a person to knowingly and intentionally “possesses any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious overhearing, transmitting, or recording of private conversations or the interception, or transcription of private electronic communications and the intended or actual use of the device is contrary to the provisions of” the IES.

258. The IES defines “private electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation.” 720 ILCS § 5/14-1(e).

259. “Surreptitious,” as used in the IES, “means obtained or made by stealth or deception, or executed through secrecy or concealment.” 720 ILCS § 5/14-1(g).

260. An “eavesdropper” means “any person...who operates or participates in the operation of any eavesdropping device contrary to the provisions of [the IES] or who acts as a principal[.]” 720 ILCS § 5/14-1(b).

261. A “principal” includes any person who “[k]nowingly derives any benefit or information from the illegal use of an eavesdropping device by another” or “[d]irects another to use an eavesdropping device illegally on his or her behalf.” 720 ILCS § 5/14-1(c).

262. An “eavesdropping device” is “any device capable of being used to...intercept...electronic communications[.]” 720 ILCS § 5/14-1(a).

263. Plaintiff’s communications with Defendant constituted private electronic communications. Plaintiff transmitted her communications to Defendant from her computer or wire, intended the communications to be private, and reasonably expected the communications to be private under HIPAA, Defendant’s express promises of confidentiality, the physician-patient relationship, and other State and federal laws protecting the confidentiality of Plaintiff’s communications.

264. Facebook and Google were not parties to Plaintiff’s private electronic communications with Defendant. Plaintiff and Class Members believed they were only communicating with Defendant, intended for their communications to be directed at Defendant only, and were unaware of the presence of concealed source code that redirected their communications.

265. Facebook and Google’s interceptions of Plaintiff’s private electronic communications were knowing, intentional, and surreptitious. Facebook and Google intentionally designed their source code so that it could be concealed on websites to secretly intercept private communications. Facebook and Google knew that their source code was capable of, and in fact did, intercept private electronic communications without the consent of all parties to the communications.

266. Facebook and Google used and disclosed Plaintiff’s intercepted communications for advertising purposes.

267. Facebook and Google conduct was done without Plaintiff’s consent, in violation of 720 ILCS § 5/14-2(a)(3) and (a)(5).

268. Defendant acted as Facebook and Google’s “principal” under the IES. By deploying the source code from Facebook and Google on its Website, Defendant directed that Facebook and Google illegally eavesdrop on Plaintiff’s private electronic communications on its behalf and Defendant knowingly derived benefits and information from the illegal eavesdropping in the form of marketing.

269. Defendant further violated 720 ILCS § 5/14-2(a)(4) by possessing the source code, knowing that its design rendered it primarily useful for surreptitiously intercepting private electronic communications contrary to the IES.

270. Defendant’s violation of the IES was wanton, reckless, and/or malicious.

271. For Defendant’s violations of the IES, Plaintiff and Class Members seek actual damages, punitive damages, injunctive relief, and any other relief the Court deems just.

RELIEF REQUESTED

272. Plaintiff, on behalf of herself and the proposed Class and Subclass, respectfully requests that the Court enter an order:

- a. Certifying this action as a class action and appointment of Plaintiff and Plaintiff’s counsel to represent the Class and Subclass defined above;
- b. For equitable relief, enjoining Defendant from engaging in the unlawful practices and illegal acts described herein;
- 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. An award of damages, including but not limited to, (1) actual or statutory damages; (2) punitive damages in an amount to be determined at trial; (3)

prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorney fees and expenses and costs of suit; and (6) such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the proposed Classes, demands a trial by jury for all claims asserted herein and so triable.

DATED: February 27, 2025

Respectfully submitted,

/s/ Alec M. Leslie

BURSOR & FISHER, P.A.

Alec M. Leslie

1330 Avenue of the Americas, 32nd Floor

New York, NY 10019

Telephone: (646) 837-7126

E-Mail: aleslie@bursor.com

BURSOR & FISHER, P.A.

Sarah N. Westcot (*pro hac vice* forthcoming)

Stephen A. Beck

701 Brickell Avenue, Suite 2100

Miami, FL 33131

Telephone: (305) 330-5512

Facsimile: (305) 676-9006

E-Mail: swestcot@bursor.com

sbeck@bursor.com

Attorneys for Plaintiff & the Classes

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

L.C., individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Cook County

(EXCEPT IN U.S. PLAINTIFF CASES)

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

Alec M. Leslie
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
(646) 837-7126

DEFENDANTS

Fertility Centers of Illinois, PLLC,

County of Residence of First Listed Defendant Cook County

(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 | ☐ 1 | ☐ 1 | Incorporated or Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☐ 2 | ☐ 2 | Incorporated and Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

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

VI. CAUSE OF ACTION (Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

18 U.S.C. § 2511- Violation of Privacy

VII. Previous Bankruptcy Matters (For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)**VIII. REQUESTED IN COMPLAINT:**

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

DEMAND \$

\$5,000,000 +

CHECK YES only if demanded in complaint:

JURY DEMAND:

☒ Yes ☐ No

IX. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

X. This case (check one box)

☐ Is not a refile of a previously dismissed action

☐ is a refile of case number _____ previously dismissed by Judge _____

DATE

SIGNATURE OF ATTORNEY OF RECORD

02/27/2025

/s/ Alec M. Leslie