Exhibit A

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

M.H., M.R., and **S.M.**, on behalf of themselves and all others similarly situated, Plaintiffs, vs. **COMPREHENSIVE BREAST CARE CENTER OF TEXAS, INC d/b/a SOLIS MAMMOGRAPHY,** Defendant.	Case No. 0:26-cv-61032 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs M.H., M.R., and S.M. ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Comprehensive Breast Care Center of Texas, Inc. d/b/a Solis Mammography ("Solis" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

INTRODUCTION

1. This class action lawsuit arises out of Solis' unlawful use of third-party tracking technologies by data brokers such as Alphabet, Inc. ("Google") to surreptitiously intercept and disclose its users' private and protected communications, including communications concerning highly sensitive personal health information, to third parties without users' knowledge or consent.

2. By purposely embedding and deploying third party tracking technologies on Solis' website, available at https://www.solismammo.com/ (the "Website"), Solis engages in the

unauthorized disclosure of its users' highly sensitive protected health information ("PHI") and personally identifiable information ("PII" and together with PHI, "Sensitive Health Information") to third parties including, but not limited to, Google. Such disclosures of PHI and PII violate state and federal law.

3. Solis Mammography is a nationwide provider of specialized women's imaging and diagnostic services, focused primarily on breast health.[1] Its offerings include screening and diagnostic mammography, breast ultrasound, and other imaging services.

4. On its Website, Solis encourages patients to research information about their health conditions, including reasons for using Solis to diagnose their medical conditions or otherwise use their imaging services.[2] Solis also encourages its patients to schedule appointments through the Website.[3]

5. However, unbeknownst to users who visited Solis' Website, their communications were intercepted and disclosed to third parties through Solis' use of third-party tracking technologies ("Tracking Tools"). These Tracking Tools track a user's activity on a website and send corresponding data to a third party, including Google.

6. The Tracking Tools embedded on Solis' Website transmitted the following Sensitive Health Information to third parties without Plaintiffs' and each Class Member's authorized consent: (i) their status as patients; (ii) their medical condition; (iii) the specific imaging diagnostics they are using to diagnose and treat that condition; (iv) the location of the center where they receive their imaging diagnostic treatment; (v) that they accessed patient pre-registration forms; (vi) that the accessed information regarding the application of insurance to pay for their

[1] https://www.solismammo.com/why-solis/better-mammogram
[2] *Id.*
[3] *Id.*

treatment; (vi) that they accessed the "contact us" page; and (vii) that they have made a records request.

7. Health information is highly regulated by both state and federal law, including HIPAA, which imposes criminal penalties on disclosing individually identifiable health information ("IIHI") to a third party, including any information that "is created or received by a health care provider" and "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[.]"[4] Accordingly, Solis' disclosure of Plaintiffs' and each Class Member's Sensitive Health Information constitutes a violation of HIPAA.

8. Solis installed the Tracking Tools with the intent to collect and disclose users' Sensitive Health Information for purposes of financial gain.

9. Plaintiffs and Class Members never consented to, authorized, or otherwise agreed to allow Solis to disclose their PHI and PII to anyone other than those reasonably believed to be part of Solis, acting in some healthcare-related capacity. Despite this, Solis knowingly and intentionally disclosed Plaintiffs' and each Class Member's PHI and PII to Google and other third parties.

10. Given the nature of Google's business as one of the world's largest online advertising companies, Plaintiffs' and each Class Member's PHI and PII can and will likely be further used by or exposed to additional third parties.

11. Online advertising giants, like Google, compile as much information as possible about American consumers, including information relating to the most private aspects of their lives

[4] 18 U.S.C. § 1320d-(6).

like their PHI and the diagnostic treatments they use to treat their health conditions. This information is then used as fuel for a massive, targeted advertising enterprise.

12. Thus, any information about a person captured by these online behemoths can be used to stream ads to that person, among other uses. If Google receives information that a person is concerned about their health, it will collect that information and allow its clients to use that information to stream ads related to health treatments and services to that person's computers and smartphones.

13. Google offers its clients' website operators access to its proprietary suites of marketing, advertising, and customer analytics software, including Google Analytics, Google AdSense, and Google Tag Manager (collectively, the "Business Tools").

14. Armed with Google's Business Tools, website operators can leverage Google's enormous database of consumer information for the purposes of deploying targeted advertisements, performing minute analyses of their customer bases, and identifying new market segments that may be exploited.

15. But, in exchange for access to Google's Business Tools, website operators install Tracking Tools, *i.e.*, Google's surveillance software, on their website, including tracking pixels ("Pixels") and third-party cookies that capture sensitive, personally identifiable information provided to the website operator by its website users. This sensitive information can include a unique identifier that Google uses to identify that user called a Client ID ("CID"), regardless of what computer or phone is used to access the website. The Tracking Tools can also capture and share other information like the specific webpages visited by a website user, information entered into an online form by a website user, and the device characteristics of a website user's phone or computer.

16. In essence, when website operators use Google's Business Tools, they choose to participate in Google's mass surveillance network and, in turn, benefit from Google's collection of user data at the expense of their website user's privacy.

17. Solis is one of the companies that has chosen to prioritize its marketing efforts and profits over the privacy of its users and potential patients by installing Google's Tracking Tools on its Website.

18. Plaintiffs and each Class Member used the Website and had their personal Sensitive Health Information tracked by Solis using the Tracking Tools. However, Solis ***never*** obtained authorization from Plaintiffs or Class Members to share their Sensitive Health Information with third parties. At all times relevant to this action, Plaintiffs and Class Members gave no informed consent for information about their Sensitive Health Information to be transmitted to third parties, including Google, the largest advertiser and compiler of user information.

19. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of medical privacy; (ii) lack of trust in communicating with medical providers; (iii) emotional distress and heightened concerns related to the release of Sensitive Health Information to third parties, (iv) loss of benefit of the bargain; (v) diminution of value of the Sensitive Health Information; (vi) statutory damages; and (vii) continued and ongoing risk to their Sensitive Health Information.

20. Therefore, Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and assert the following statutory and common law claims against Defendant: (i) violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq.*; (ii) violation of the Florida Security of Communications Act, Florida Statutes §

934.01, et seq.; (iii) Common Law Invasion of Privacy; (iv) Negligence; (v) Breach of Implied Contract; and (vi) Unjust Enrichment.

PARTIES

Plaintiff M.H.

21. Plaintiff M.H. is a citizen of the State of Florida, residing in Broward County, and brings this action both in an individual capacity and on behalf of all others similarly situated.

22. Plaintiff M.H. utilized the Website on her personal electronic devices to search for information regarding her diagnosis and treatment for breast cancer and to search for information and to schedule her mammogram with Solis at Memorial Hospital in Hollywood, Florida.

23. Unbeknownst to Plaintiff M.H., Defendant transmitted the Sensitive Health Information that she communicated while using the Website, including while searching for information regarding her breast cancer treatment, and scheduling her mammogram. Among the Sensitive Health Information that Plaintiff disclosed to Defendant, and which were disclosed to third parties including Google, were: (i) her status as a patient; (ii) her searches for information related to her breast cancer; (iii) the specific imaging diagnostics she used to treat her medical condition; (iv) the location of the center where she received her imaging diagnostic treatment; (v) that she scheduled a mammogram; and (vi) the location of her mammogram to screen for breast cancer.

24. As a result of Plaintiff M.H. using the Website, Defendant disclosed to third parties including Google, the information she shared with Defendant through the Website. Defendant also disclosed to third parties Plaintiff M.H.'s PII, including the disclosure of her CID to Google.

25. Plaintiff M.H. never authorized Defendant to disclose any aspect of her communications with Defendant through the Website to third parties, including the Sensitive Health Information that she provided to Defendant.

26. On every occasion that she visited the Website, Plaintiff M.H. possessed an account with Google, and she accessed the Website while logged into her Google account on the same device.

27. After providing her Sensitive Health Information to Defendant through the Website, Plaintiff began seeing targeted online advertisements for health services and products related to breast cancer treatment.

Plaintiff M.R.

28. Plaintiff M.R. is a citizen of the State of Florida, residing in Miami-Dade County, and brings this action both in an individual capacity and on behalf of all others similarly situated.

29. Plaintiff M.R. utilized the Website on her personal electronic devices to search for information regarding her breast cancer screening as well as to search for and schedule her mammogram with Solis at the Memorial Hospital Hollywood, Florida location.

30. Unbeknownst to Plaintiff M.R., Defendant transmitted the Sensitive Health Information that she communicated while using the Website, including while searching for information regarding her breast cancer screening and scheduling her mammogram. Among the Sensitive Health Information that Plaintiff disclosed to Defendant, and which were disclosed to third parties including Google, were: (i) her status as a patient; (ii) her searches for information related to her breast cancer screening; (iii) the specific imaging diagnostics she used to screen for breast cancer; (iv) the location of the center where she received her imaging diagnostic treatment; (v) that she scheduled a mammogram; and (vi) the location of her mammogram to screen for breast cancer.

31. As a result of Plaintiff M.R. using the Website, Defendant disclosed to third parties including Google, the information she shared with Defendant through the Website. Defendant also disclosed to third parties Plaintiff M.R.'s PII, including the disclosure of her CID to Google.

32. Plaintiff M.R. never authorized Defendant to disclose any aspect of her communications with Defendant through the Website to third parties, including the Sensitive Health Information that she provided to Defendant.

33. On every occasion that she visited the Website, Plaintiff M.R. possessed an account with Google, and she accessed the Website while logged into her Google account on the same device.

34. After providing her Sensitive Health Information to Defendant through the Website, Plaintiff began seeing targeted online advertisements for health services and products related to breast cancer treatment.

Plaintiff S.M.

35. Plaintiff S.M. is a citizen of the State of Florida, residing in Broward County, and brings this action both in an individual capacity and on behalf of all others similarly situated.

36. Plaintiff S.M. utilized the Website on her personal electronic devices to search for information regarding her breast cancer screening as well as to search for and schedule her mammogram at the Solis location in Plano, Texas.

37. Unbeknownst to Plaintiff S.M., Defendant transmitted the Sensitive Health Information that she communicated while using the Website, including while searching for information regarding her breast cancer screening and scheduling her mammogram. Among the Sensitive Health Information that Plaintiff disclosed to Defendant, and which were disclosed to third parties including Google, were: (i) her status as a patient; (ii) her searches for information

related to her breast cancer screening; (iii) the specific imaging diagnostics she used to screen for breast cancer; (iv) the location of the center where she received her imaging diagnostic treatment; (v) that she scheduled a mammogram; and (vi) the location of her mammogram to screen for breast cancer.

38. As a result of Plaintiff S.M. using the Website, Defendant disclosed to third parties including Google, the information she shared with Defendant through the Website. Defendant also disclosed to third parties Plaintiff S.M.'s PII, including the disclosure of her CID to Google.

39. Plaintiff S.M. never authorized Defendant to disclose any aspect of her communications with Defendant through the Website to third parties, including the Sensitive Health Information that she provided to Defendant.

40. On every occasion that she visited the Website, Plaintiff S.M. possessed an account with Google, and she accessed the Website while logged into her Google account on the same device.

41. After providing her Sensitive Health Information to Defendant through the Website, Plaintiff began seeing targeted online advertisements for health services and products related to breast cancer treatment.

Defendant Solis

42. Defendant Comprehensive Breast Care Center of Texas, Inc. d/b/a Solis Mammography is a for-profit corporation incorporated in the State of Texas with its principal place of business at 15601 Dallas Parkway, STE 300, Addison, TX 75001.

JURISDICTION AND VENUE

43. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and

minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendant.

44. Additionally, this Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint asserts a claim for violation of federal law, specifically, the ECPA, 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.

45. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in the State of Florida, including operating over 300 physical locations in Florida,[5] and because Defendant provided services and in this judicial district.

46. Personal jurisdiction is also proper because Defendants committed tortious acts in the State of Florida and this judicial district and Plaintiffs' claims arise out of such acts, and/or because Defendants have otherwise made or established contacts in the State of Florida and in this judicial district sufficient to permit the exercise of personal jurisdiction.

47. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims in this action occurred in this judicial district.

[Remainder of page intentionally left blank]

[5] https://www.solismammo.com/find-a-center/all-locations

FACTUAL ALLEGATIONS

A. DEFENDANT'S USE OF THIRD-PARTY TRACKING TECHNOLOGIES.

i. Google's Mass Advertising Surveillance Operation.

48. Google is the largest digital advertiser in the country, accounting for 26.8-percent of the total digital advertising revenue generated in the United States.[6] In 2023, Google's advertising revenue of $238 billion accounted for 77-percent of its total revenue for the year.[7]

49. Google advertises Google Analytics and other Business Tools to website operators, like Defendant, claiming they will allow the operator to "[u]nderstand [their] site and app users," "check the performance of [their] marketing," and "[g]et insights only Google can give."[8] But in order for website operators to get information from Google Analytics about their website's visitors, they must allow data collection through installation of Google's Tracking Tools on their website.[9]

50. Indeed, on its *Privacy & Terms* page, Google admits that it collects information from third-party websites, stating that "[m]any websites and apps use Google services to improve their content and keep it free. When they integrate our services, these sites and apps share information with Google."[10]

---

[6] *Share of major ad-selling companies in digital advertising revenue in the United States*, Statista (May 2024), https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/#:~:text=In%202023%2C%20Google%20accounted%20for,21.1%20and%2012.5%20percent%2C%20respectively.

[7] Florian Zandt, *Google's Ad Revenue Dwarfs Competitors*, Statista (Sep. 10, 2024), https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions/#:~:text=Online%20advertising&text=Alphabet%2C%20the%20company%20behind%20the,overall%20revenue%20this%20past%20year.

[8] *Welcome to Google Analytics*, Google, https://analytics.google.com/analytics/web/provision/?authuser=0#/provision.

[9] *See* Aaron Ankin & Surya Matta, *The High Privacy Cost of a "Free" Website*, The Markup, https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites.

51. Google also admits that it uses the information collected from third-party websites, such as the Website, to sell targeted advertising, explaining to users that, "[f]or example, a website that sells mountain bikes might use Google's ad services. After you visit that site, you could see an ad for mountain bikes on a different site that shows ads served by Google."[11]

52. While Google admits that it collects information from third-party websites through the Tracking Tools, it does not provide, nor could it provide, a publicly available list of every webpage on which its Tracking Tools are installed. The vague descriptions of Google's data collection practices referenced above could not give Plaintiffs and Class Members any reason to think that Defendant was part of Google's surveillance network. Moreover, as Defendant does not disclose its use of Google's Tracking Tools, Plaintiffs and Class Members could not have been reasonably expected to review any of Google's privacy statements in connection with their use of the Website.

53. Google aggregates the user information that it collects from third-party websites into "advertising profiles" consisting of all of the data that it has collected about a given user.[12] With these advertising profiles, Google can sell hyper-precise advertising services, allowing its clients to target internet users based on combinations of their location, age, race, interests, hobbies, life events (e.g., recent marriages, graduation, or relocation), political affiliation, education level, home ownership status, marital status, household income, type of employment, use of specific apps or websites, and more.[13]

---

[10] *Privacy & Terms – How Google uses information from sites or apps that use our services*, Google, https://policies.google.com/technologies/partner-sites.

[11] *Id.*

[12] Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (2019), *available online at* https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf.

54. Google's surveillance of individual's internet usage is ubiquitous. In 2017, Scientific American reported that over 70-percent of smartphone apps report "personal data to third-party tracking companies like Google,"[14] and Google trackers are present on 74-percent of all web traffic.

55. Moreover, as in this case, the data collected by Google often pertains to the most personal and sensitive aspects of an individual's life. For example:

a. Twelve of the largest pharmacy providers in the United States send information regarding user's purchases of products such as pregnancy tests, HIV tests, prenatal vitamins, and Plan B to online advertisers.[15] For example, when an online shopper searches for a pregnancy test, views the product page for a pregnancy test, or adds a pregnancy test to their online shopping cart on Kroger's website, that information is transmitted to Google.[16]

b. 81-percent of the most popular mobile apps for managing depression and quitting smoking allowed Facebook and/or Google to access subscriber information, including health diary entries and self-reports about substance abuse.[17]

---

[13] *About audience segments*, Google Ads, https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics.

[14] Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, Scientific American (May 30, 2017), https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/.

[14] Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, Scientific American (May 30, 2017), https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/.

[16] Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You*, The Markup (Feb. 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you.

[17] Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETWORK OPEN (2019), *available online at* https://pubmed.ncbi.nlm.nih.gov/31002321/.

c. 93-percent of pornography websites allow third parties, including Google, to collect their user's browsing habits.[18] In fact, Google advertising trackers were found on 73-percent of pornography websites.[19]

56. This monumental, invasive surveillance of Americans' internet usage and resulting violation of their privacy is not accidental. As Google's then-CEO, Eric Schmit, admitted in 2010: "We know where you are. We know where you've been. We can more or less know what you're thinking about."[20]

57. In fact, Google values user information so highly that it provides its Business Tools to many website operators for free, all to expand its surveillance apparatus.[21]

58. When website operators, like Defendant, make use of Google's Business Tools, they are essentially choosing to participate in Google's mass surveillance network and, in return, they benefit from Google's collection of user data at the expense of their website users' privacy.

59. For example, Google rewards website operators for providing it with user information by granting such website operators access to its Analytics platform, which then leverages demographic data collected by Google to provide detailed analyses of the website's user base.[22]

---

[18] Elena Maris, Timothy Libert & Jennifer R. Henrichsen, *Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites*, NEW MEDIA & SOCIETY (2020), *available online at* https://journals.sagepub.com/doi/10.1177/1461444820924632.
[19] *Id.*

[20] Andrew Orlowski, *Google's Schmidt: We know what you're thinking*, The Register (Oct. 4, 2020), https://www.theregister.com/2010/10/04/google_ericisms/.
[21] *Analytics Overview*, Google, https://marketingplatform.google.com/about/analytics/ ("Google Analytics gives you the tools, free of charge"),

ii. Pixels Can Record Almost Every Interaction Between a User and a Website.

60. In order to use Google's Business Tools, Defendant installed Google's Tracking Tools, including tracking Pixels, onto the Website.

61. Pixels are one of the tools used by website operators to track user behavior. As the Federal Trade Commission ("FTC") explains, a Pixel is:

> [A] small piece of code that will be placed into the website or ad and define [the Pixel operator's] tracking goals such as purchases, clicks, or pageviews…
>
> Pixel tracking can be monetized several ways. One way to monetize pixel tracking is for companies to use the tracking data collected to improve the company's own marketing campaigns…Another is that companies can monetize the data collected by further optimizing their own ad targeting systems and charging other companies to use its advertising offerings.[23]

62. Pixels can collect a remarkable amount of information regarding an individual's online behavior—including the webpages viewed by the user, the amount of time spent by the user on specific webpages, the buttons and hyperlinks that the user clicks while using a website, the items that the user adds to an online shopping cart, the purchases that a user makes through an online retailer, the text entered by the user into a website search bar, and even the information provided by the user on an online form—all transmitted in real-time as the user navigates a website.[24]

63. But most internet users are completely unaware that substantial information about their internet usage is being collected through tracking Pixels. The FTC warns that:

---

[15] Darius Tahir & Simon Fondrie-Teitler, *Need to Get Plan B or an HIV Test Online? Facebook May Know About It*, The Markup (June 30, 2023), https://themarkup.org/pixel-hunt/2023/06/30/need-to-get-plan-b-or-an-hiv-test-online-facebook-may-know-about-it.

> Traditional controls such as blocking third party cookies may not entirely prevent pixels from collecting and sharing information. Additionally, many consumers may not realize that tracking pixels exist because they're invisibly embedded within web pages that users might interact with...Academic and public reporting teams have found that thousands of the most visited webpages have pixels and other methods that leak personal information to third parties.[25]

iii. The Pixels Installed on the Website Transmit Personally Identifiable Information and Protected Health Information to Google.

64. Every website is hosted by a computer "server" that holds the website's contents.

65. To access a website, individuals use "web browsers." Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as computer, tablet, or smartphone) accesses web content through a web browser (such as Google's Chrome, Mozilla's Firefox, Apple's Safari, or Microsoft's Edge).

66. Communications between a website server and web browser consists of Requests and Responses. Any given browsing session may consist of hundreds or even thousands of individual Requests and Responses. A web browser's Request essentially asks the website to provide certain information, such as the contents of a given webpage when the user clicks a link, and the Response from the website sends back the requested information—the web pages' images, words, buttons, and other features that the browser shows on the user's screen as they navigate the website.

---

[27] *See id.*; *How does retargeting on Facebook help your business?*, Meta, https://www.facebook.com/business/goals/retargeting; Tom Kemp, *"Oops! I Did It Again" ... Meta Pixel Still Hoovering Up Our Sensitive Data*, Medium, https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47#_ftn1.

[25] *Lurking Beneath the Surface, supra* note 27.

67. Additionally, on most websites, the Response sent back to the user's web browser directs the browser to create small files known as "cookies" on the user's device.[26] These cookies are saved by the user's web browser, and are used to identify the website user as they browse the website or on subsequent visits to the site.[27] For example, in a more innocuous use case, a cookie may allow the website to remember a user's name and password, language settings, or shopping cart contents.[28]

68. When a Google user logs onto their account, their web browser records a Google tracking cookie.[29] This cookie includes a specific line of code that links the web browser to the user's Google account.[30]

69. Google's Pixels use cookies but operate differently than a cookie. Rather than directing the browser to save a file on the user's device, the Pixels acquire information from the browser without notifying the user. The information can include details about the user, his or her interactions with the website, and information about the user's environment (e.g., type of device, type of browser, and sometimes even the physical location of the device), all relayed contemporaneously as the website user navigates the website.

70. Simultaneously, the Google Pixels, like those installed on the Website, request identifying information from any Google cookies previously installed on the user's web browser.

71. The Pixels then combine the data received from the browser with the data acquired from the cookie and instructs the web browser to transmit the information back to Google. As a

---

[29] *What is a web browser?*, Mozilla, https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/.
[27] *Id.*
[28] *Id.*
[29] Cyphers, *supra*, n. 13.
[30] *Id.*

result, Google can link all of the user information collected by their Pixels to the user's identity, via the user's Google profile. Thus, even if a user never actually logs into a website or fills out a form, the website, along with Google, can know the user's identity.

72. A remarkable number of Americans possess a Google account. Just one of Google's many products, its Gmail e-mail client, is used by over one-third of Americans.[31] When these users visit a website, like those on which the Website has been installed, that utilizes a Google Pixel, any information collected by the Pixel can be linked to the user's identity through the Google cookies installed on the user's web browser.

73. However, it is not only Google account holders that are at risk of having Pixel-collected website data linked to their identities. Rather, Google utilizes sophisticated data tracking methods to identify even those few users who do not have a Google account.[32]

74. Google's Pixels, like those on the Website, can acquire information about the user's device and browser, such as their screen resolution, time zone setting, browser software type and version, operating system type and version, language setting, and IP address.

75. An internet user's combination of such device and browser characteristics, commonly referred to as their "browser fingerprint," is "often unique."[33] By tracking this browser fingerprint, Google is able to compile a user's activity across the internet.[34] And, as Google continuously compiles user data over time, its understanding of the user's browser fingerprint

---

[34] *See* Harsha Kiran, *49 Gmail Statistics To Show How Big It Is In 2024*, TechJury (Jan. 3, 2024), https://techjury.net/blog/gmail-statistics/ ("Gmail accounts for 130.9 million of the total email users in the US"). The United States population is approximately 337.4 million. *See* United States Census Bureau, https://www.census.gov/popclock/.

[35] *See Client ID vs User ID in Google* Analytics, Glide Ad Agency, https://glideagency.com/client-id-vs-user-id-in-google-analytics/.

[33] Cyphers, *supra* note 13.

[34] *Id.*

becomes more sophisticated such that it needs only to collect a single piece of identifying information to identify the user linked to a browser fingerprint.

iv. Defendant Disclosed Plaintiffs' and Class Members' Sensitive Health Information to Google.

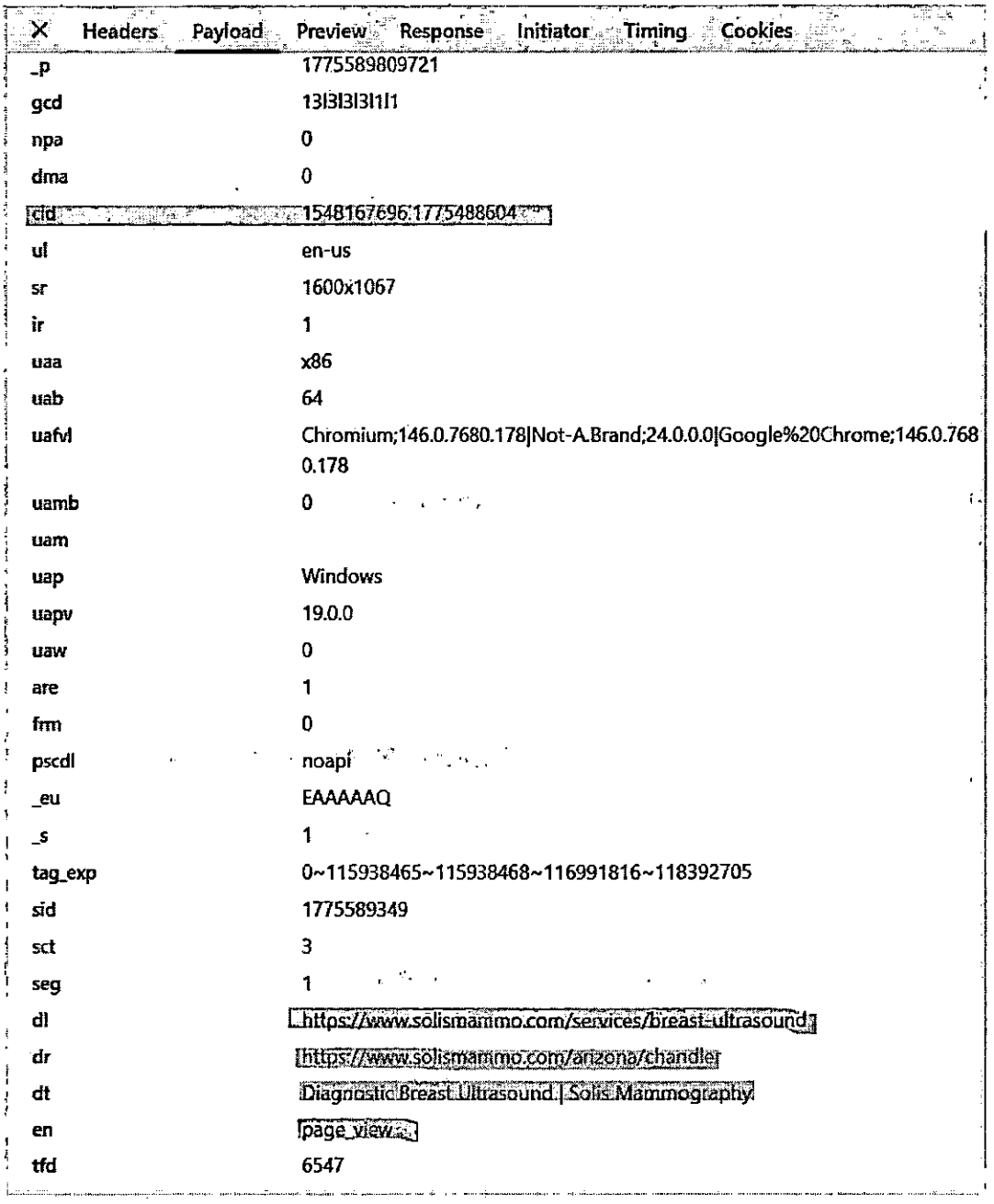
76. Plaintiffs and Class Members used Solis' Website to research and access health treatments and services related to breast cancer screening and other diagnostic imaging. While visiting Solis' Website, Plaintiffs and Class Members each searched for and accessed information regarding available imaging services, selected appointment options, and entered or conveyed health-related information—including the type of diagnostic services sought—thereby transmitting protected health information through the Website.

77. Unbeknownst to Plaintiffs and Class Members, Defendant intentionally configured the Tracking Tools installed on the Website to capture and transmit the Sensitive Health Information that they communicated to Defendant through the Website to third parties, including Google.

78. As Figure 1 shows, when users make a mammography diagnostic appointment on the Website, the Sensitive Health Information requested and contemporaneously transmitted to Google by the Tracking Tools installed on the Website includes the user's Client ID, or CID, as well as their PHI, including that they have scheduled a "Diagnostic Breast Ultrasound" at Solis' "Chandler, Arizona" location.

[Remainder of page intentionally left blank]

Figure 1. Screenshot depicting back-end network traffic from the Website which shows information transmitted to Google when Website users make an appointment for a breast ultrasound.



× Headers	Payload	Preview	Response	Initiator	Timing	Cookies
_p	1775589809721					
gcd	13l3l3l3l1l1					
npa	0					
dma	0					
cid	1548167696.1775488604					
ul	en-us					
sr	1600x1067					
ir	1					
uaa	x86					
uab	64					
uafvl	Chromium;146.0.7680.178|Not-A.Brand;24.0.0.0|Google%20Chrome;146.0.7680.178					
uamb	0					
uam						
uap	Windows					
uapv	19.0.0					
uaw	0					
are	1					
frm	0					
pscdl	noapi					
_eu	EAAAAAQ					
_s	1					
tag_exp	0~115938465~115938468~116991816~118392705					
sid	1775589349					
sct	3					
seg	1					
dl	https://www.solismammo.com/services/breast-ultrasound/					
dr	https://www.solismammo.com/arizona/chandler					
dt	Diagnostic Breast Ultrasound | Solis Mammography					
en	page_view					
tfd	6547					

79. Figure 2 shows, that when a patient uses the Website to make an appointment for a breast biopsy with Solis, the Defendant discloses to Google the patient's Client ID, or CID, as well as the fact that they have are attempting to "schedule" an "Ultrasound & Stereotactic Breast Biopsy."

× Headers	Payload	Preview	Response	Initiator	Timing	Cookies
_p		1775712629999				
gcd		13l3l3l3l1l1				
npa		0				
dma		0				
_eu		EAAAAAQ				
are		1				
cid		1548167696.1775488604				
frm		0				
ir		1				
pscdl		noapi				
sr		1600x1067				
uaa		x86				
uab		64				
uafvl		Chromium;146.0.7680.178|Not-A.Brand;24.0.0.0|Google%20Chrome;146.0.7680.178				
uam						
uamb		0				
uap		Windows				
uapv		19.0.0				
uaw		0				
ul		en-us				
_s		1				
tag_exp		0~115938465~115938468~118131808~118289195				
sid		1775711990				
sct		10				
seg		1				
dl		https://www.solismammo.com/services/breast-biopsy				
dr		https://www.solismammo.com/schedule				
dt		Ultrasound & Stereotactic Breast Biopsy | Solis Mammography				
en		page_view				

Figure 2. Screenshot depicting back-end network traffic from the Website which shows information transmitted to Google when Website users visit the breast biopsy services page and schedule an appointment.

80. As mentioned above, the information that was transmitted to Google was accompanied by specific lines of code linking the Sensitive Health Information provided by Plaintiffs to their identity. The following screenshot shows that the Google Pixel on the Website transmitted the identifier numbers attached to Google's 'cid' cookie, which identifies the user's Google account, along with other information that is commonly used to create a browser fingerprint, such as the user's language selection, screen resolution, IP address, web browser software and version number, and operating system and version number.

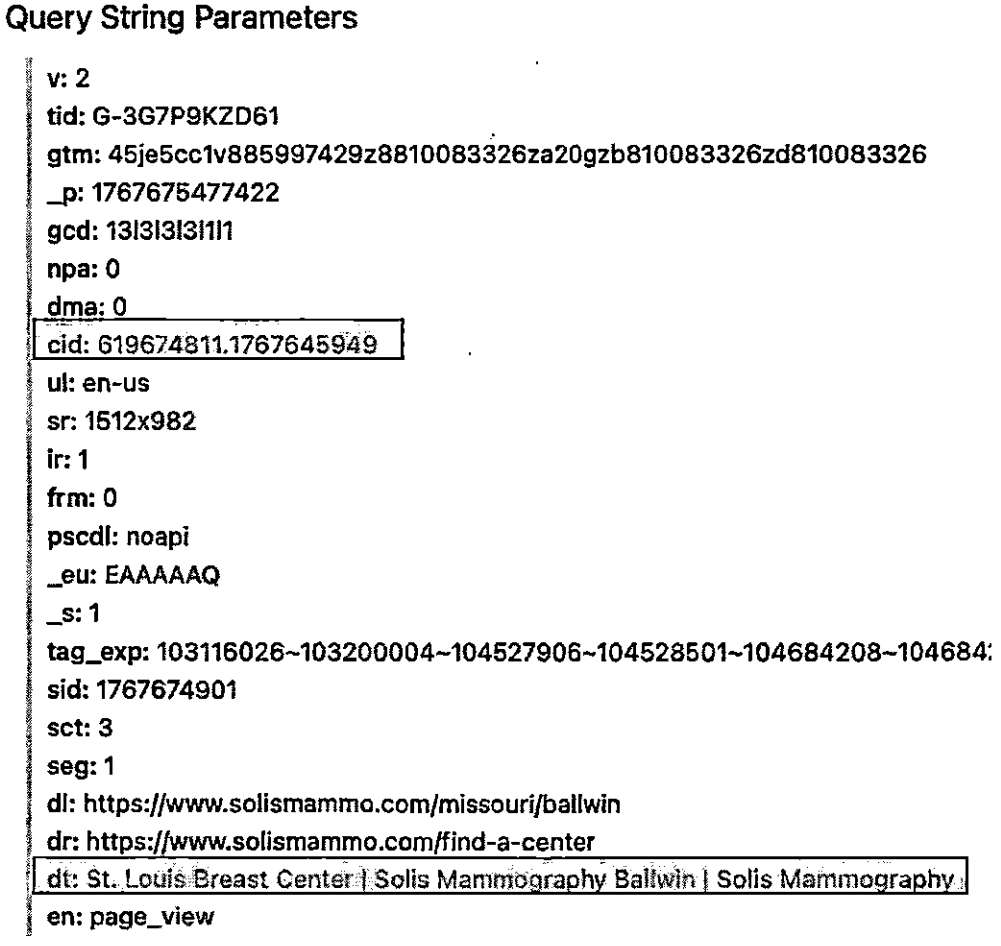


Figure 3. Screenshot depicting back-end network traffic from the Website which shows PII to Google, including the CID, when Website users search for a location to schedule a breast diagnostic screening.

81. In their default state, Google's Pixels record and transmit only "automatic events," consisting largely of routine user behavior, such as the URLs visited by internet users.[35]

82. Defendant purposely configured the Google Pixels on the Website to collect and transmit additional user data, including information related to users' visits to Defendant's breast health services pages, appointment scheduling activity, and breast biopsy and imaging diagnostic information.

B. DEFENDANT DISCLOSED PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES WITHOUT THEIR KNOWLEDGE OR CONSENT.

i. Defendant Failed to Inform Plaintiffs and Class Members of its Disclosure of their Sensitive Health Information.

83. Defendant breached Plaintiffs' and Class Members' right to privacy by unlawfully disclosing their Sensitive Health Information to third parties, including Google.

84. Specifically, Plaintiffs and Class Members had a reasonable expectation of privacy. Defendant did not inform Plaintiffs that it was sharing their Sensitive Health Information with third parties, including Google.

85. By engaging in this improper sharing of information without Plaintiffs' and Class Members' consent, Defendant breached Plaintiffs' and Class Members' right to privacy and unlawfully disclosed their Sensitive Health Information.

86. Despite never telling users like Plaintiffs and Class Members, Defendant allowed third parties such as Google to intercept Plaintiffs' and Class Members' Sensitive Health Information and use it for advertising purposes.

ii. The Tracking Tools Used by Defendant Were Imperceptible to Plaintiffs and Class Members.

87. The Tracking Tools installed on the Website were invisible to Plaintiffs and Class Members. Without analyzing the network information transmitted by the Website through examination of its source code or the use of sophisticated web developer tools, there was no way for a Website user to discover the presence of the Tracking Tools. As a result, typical internet users such as Plaintiffs and Class Members were unable to detect the Tracking Tools on the Website.

88. Plaintiffs and Class Members were shown no disclaimer or warning that their Sensitive Health Information would be disclosed to any unauthorized third party without their express consent.

89. Plaintiffs and Class Members did not know that their Sensitive Health Information was being collected and transmitted to an unauthorized third party.

90. Because Plaintiffs and Class Members were not aware of the Tracking Tools on the Website, or that their Sensitive Health Information would be collected and transmitted to Google, they could not and did not consent to Defendant's conduct.

C. DEFENDANT WAS ENRICHED BY ITS DISCLOSURE OF PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES.

i. Defendant Received Material Benefits in Exchange for Plaintiffs' Sensitive Health Information.

91. As explained, *supra*, users of Google's Business Tools, like Defendant, receive access to advertising and marketing analytics services in exchange for installing Google's Tracking Tools on its website.

92. Upon information and good faith belief, Defendant, as a user of Google's Business Tools, received compensation in the form of advanced advertising services and cost-effective

marketing on third-party platforms in exchange for allowing Google to collect Plaintiffs' and Class Members' Sensitive Health Information.

ii. Plaintiffs' and Class Members' Data Had Financial Value.

93. Plaintiffs' and Class Members' Sensitive Health Information has value, and Defendant's disclosure and interception of that Sensitive Health Information harmed Plaintiffs and the Class.

94. According to the annual reports of Facebook, another major online advertising proprietor, the value it derives from user data has continuously risen. "In 2013, the average American's data was worth about $19 per year in advertising sales to Facebook, according to its financial statements. In 2020, [it] was worth $164 per year."[36]

95. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

96. Moreover, health information is particularly valuable. Healthcare data brokers charge up to $125 per clinical data record, with electronic healthcare databases selling for up to $500,000.[37] In fact, compared to other types of personal data, healthcare data records are by far the most valuable, fetching prices of up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[38]

---

[38] *Automatically Collected Events*, Google Analytics Help, https://support.google.com/analytics/answer/9234069.

[39] Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, The Washington Post (Aug. 29, 2021), https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/.

[37] *The Value of Data*, TRUSTWAVE (2017), *available online at*: https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf.

[38] Todd Zigrang & Jessica Bailey-Wheaton, *Valuing Healthcare Data*, THE VALUE EXAMINER (2023), *available online at*:

97. Several companies have products through which they pay consumers for a license to track certain information. Indeed, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies, in addition to Google, that pay for browsing history information.

98. The unauthorized disclosure of Plaintiffs' and Class Members' private and Sensitive Health Information has diminished the value of that information, resulting in harm to Plaintiffs and Class Members.

D. DEFENDANT'S USE OF THE TRACKING TOOLS VIOLATES HIPAA.

99. The disclosure of Plaintiffs' and Class Members' Sensitive Health Information via the Tracking Tools contravenes the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Sensitive Health Information.[39]

100. The HIPAA Privacy Rule sets forth policies to protect all IIHI that is held or transmitted by a covered entity such as Defendant. These are the 18 HIPAA Identifiers that are considered personally identifiable information because this information can be used to identify, contact, or locate a specific person or can be used with other sources (such as a person's Google account) to identify a single individual. When IIHI is used in conjunction with one's physical or mental health or condition, health care, and/or one's payment for that health care, it becomes PHI.[40]

101. While healthcare entities regulated under HIPAA may use third-party tracking tools, such as the Tracking Tools, they can do so only in a very limited way, to perform analysis

---

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

[42] *The HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

on data key to operations.

102. Simply put, further to the HIPAA Privacy Rule, covered entities such as Defendant are simply ***not*** permitted to use tracking technology tools in a way that exposes Sensitive Health Information to any third party without express and informed consent.

103. Under federal law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[41]

104. The Privacy Rule broadly defines PHI as IIHI that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

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

---

[43] *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/special-topics/de-identification/index.html (HIPAA Identifiers include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

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

106. Under the HIPAA de-identification rule, health information is not considered individually identifiable under only two circumstances: if, (1) an expert has "determine[d] 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 "document[ed] the methods and results of the analysis that justify such determination.'" Or, (2), if all enumerated identifiers of the individual or their family members are removed, including names, medical record numbers, account numbers, device identifiers, device serial numbers, URLs, IP addresses, and "[a]ny other unique identifying number, characteristic, or code," so that the entity does 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." C.F.R. § 160.514.

107. The HIPAA Privacy Rule requires any "covered entity"—which includes healthcare providers like Solis—to maintain appropriate safeguards to protect the privacy of PHI and set limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

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

109. The U.S. Department of Health and Human Services ("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."[42]

110. Consistent with this restriction, the HHS has issued marketing guidance that provides,"[w]ith 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."[43]

111. Here, Defendant provided PHI to third parties in violation of the Privacy Rule.

112. 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. § 164.306(c), 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).

113. 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. § 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. § 164.308(a)(1);

c. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

---

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

d. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to IIHI in violation of 45 C.F.R. § 164.306(a)(3);

e. Failing to effectively train its workforces (including independent contractors) on the policies and procedures for PHI as necessary and appropriate to carry out job functions while maintaining security of PHI beyond using imitation phishing email software in violation of 45 C.F.R. §§ 164.530(b) and 164.308(a)(5); 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. § 164.530(c).

114. In its Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, HHS instructed in 2012:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[44]

115. In its Guidance regarding Marketing, HHS further instructed in 2003:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected

[46] *Marketing*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html.

[44] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (Nov. 26, 2012) at 5, available online at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

> health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (Emphasis added).[45]

116. HHS has repeatedly instructed for years that patient status is protected by the HIPAA Privacy Rule:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002); and

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013).

117. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Tracking Technologies. Courts, including in this District, have found the same under near-identical circumstances.[46]

E. PLAINTIFFS' AND CLASS MEMBERS' Reasonable Expectation of Privacy.

118. At all times when Plaintiffs and Class Members provided their Sensitive Health Information to Defendant, they each had a reasonable expectation that the information would remain confidential and that Defendant would not share the Sensitive Health Information with third parties for a commercial purpose unrelated to providing them with medical care.

---

[48] *Marketing*, HHS, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (April 3, 2003).

[46] *See, e.g., Mekhail v. N. Mem'l Health Care*, 726 F. Supp. 3d 916, 928 (D. Minn. 2024).

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

120. For example, a recent Consumer Reports study shows that 92-percent 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.[47]

121. Moreover, Americans are particularly interested in the safety of their health information. Over 50-percent of Americans believe that "medical-records privacy is not sufficiently protected today by law and organizational practices."[48]

122. And, in a study performed by the National Institutes of Health, nearly 80-percent of respondents reported being "very concerned" or "concerned" about the privacy of medical records.[49]

123. Personal data privacy and obtaining consent to share Sensitive Health Information are material to Plaintiff and Class Members.

---

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

[48] *The Value of Data*, TRUSTWAVE (2017), *available online at*: https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf.

[49] Daniel S Gaylin, Adil Moiduddin, Shamis Mohamoud, Katie Lundeen, Jennifer A Kelly, *Public Attitudes about Health Information Technology, and Its Relationship to Health Care Quality, Costs, and Privacy*, HEALTH SERV. RES. (2011), *available online at* https://pmc.ncbi.nlm.nih.gov/articles/PMC3097409/pdf/hesr0046-0920.pdf.

TOLLING AND ESTOPPEL

124. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of the incorporation of Google's Tracking Tools onto the Website.

125. The Tracking Tools on the Website were and are invisible to the average website visitor.

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

127. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

128. Defendant had exclusive knowledge that the Website incorporated the Pixels and other Tracking Tools and yet failed to disclose to users, including Plaintiffs and Class Members, that by using the Website to make appointments and search for information regarding Solis' diagnostic screening services, Plaintiffs' and Class Members' Sensitive Health Information would be disclosed or released to unauthorized third parties, including Google.

129. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its users' Sensitive Health Information. In fact, to the present, Defendant has not conceded, acknowledged, or otherwise indicated to its users that they have disclosed or released their Sensitive Health Information to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

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

131. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been March 2026, shortly before the filing of this Complaint.

CLASS ALLEGATIONS

132. This action is brought by the named Plaintiffs on their behalf and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

133. The Nationwide Class that Plaintiffs seek to represent is defined, as follows:

> All natural persons residing in the United States who used the Website, and whose Sensitive Health Information was disclosed or transmitted to Google or any other unauthorized third party.

134. The Florida Subclass that Plaintiffs seeks to represent is defined as:

> All natural persons residing in the state of Florida who used the Website, and whose Sensitive Health Information was disclosed or transmitted to Google or any other unauthorized third party.

135. Excluded from the proposed Class are any claims for personal injury, wrongful death, or other property damage sustained by the Class; and any Judge conducting any proceeding in this action and members of their immediate families.

136. Plaintiffs reserve the right to amend the definitions of the Class or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

137. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. Solis has over 300 locations in Florida alone. As such, at least 100—and likely many more—patients and other Website users have been impacted by Defendant's actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

138. **Commonality.** Common questions of law or fact arising from Defendant's conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class Members. These common questions include, but are not limited to, the following:

a) Whether and to what extent Defendant had a duty to protect the Sensitive Health Information of Plaintiffs and Class Members;

b) Whether Defendant had duties not to disclose the Sensitive Health Information of Plaintiffs and Class Members to unauthorized third parties;

c) Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Sensitive Health Information would be disclosed to third parties;

d) Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Sensitive Health Information was being disclosed without their consent;

e) Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of users' Sensitive Health Information;

f) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to keep the Sensitive Health Information belonging to Plaintiffs and Class Members free from unauthorized disclosure;

g) Whether Defendant violated the statutes asserted as claims in this Complaint;

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

i) Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy practices; and

j) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Sensitive Health Information.

139. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Sensitive Health Information, like that of every other Class Member, was compromised as a result of Defendant's incorporation and use of the Tracking Tools.

140. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

141. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was unlawfully stored and disclosed to unauthorized third parties, including Google, in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

142. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

143. Defendant acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

a) Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Sensitive Health Information and not disclosing it to unauthorized third parties;

b) Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Health Information;

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

d) Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Sensitive Health Information would be disclosed to third parties;

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

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

145. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names of each Class Member—each of whom visited Defendant's Website to research

information about their health conditions, schedule mammogram appointments, or otherwise access Defendant's imaging services—affected by the unauthorized disclosures that have taken place.

COUNT I

VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq.*
Unauthorized Interception, Use, and Disclosure
(On Behalf of Plaintiffs and the Class)

146. Plaintiffs repeat and reallege the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

148. 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.

149. The transmissions of Plaintiffs' Sensitive Health Information to the Website qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

150. Electronic Communications. The transmission of Sensitive Health Information between Plaintiffs and Class Members and the 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).

151. 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).

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

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

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel code deployed by Defendant to effectuate the sending and acquisition of user and Website user communications.

154. By utilizing and embedding the Pixels and Tracking Tools on the Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the content of the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

155. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixels and Tracking Tools, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Sensitive Health Information to third parties such as Google.

156. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding their Sensitive Health

Information, including information related to breast cancer screening and other diagnostic imaging.

157. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to third parties, while knowing or having reason to know that such 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).

158. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs 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).

159. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy and the criminal violation of HIPAA, among others.

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

161. Defendant is not a party to the communication based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Sensitive Health Information does not qualify for the party exemption.

162. Defendant's acquisition of sensitive communications that was used and disclosed to Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Invasion of privacy;

b. Breach of confidence;

c. Breach of fiduciary duty;

d. Violations of HIPAA, 42 U.S.C. § 1320d-6(a)(3); and

163. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it used and caused to be used cookie identifiers associated with specific users, including Plaintiffs and Class Members, without user authorization; and disclosed individually identifiable Sensitive Health Information to Google without user authorization.

164. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their Sensitive Health Information on the Website, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' Sensitive Health Information with Google and other third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know were receiving their Sensitive Health Information, and that Plaintiffs and Class Members did not consent to receive their Sensitive Health Information.

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

166. Plaintiffs 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 Sensitive Health Information for commercial purposes has caused Plaintiffs and Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiffs'

and Class Members' Sensitive Health Information without providing any value or benefit to Plaintiffs or Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' Sensitive Health Information, such as understanding how people use the Website and determining what ads people see on the Website, without providing any value or benefit to Plaintiffs or Class Members;

d. Defendant failed to provide Plaintiffs and Class Members with the full value of the services for which they paid, which included a duty to maintain the confidentiality of their Sensitive Health Information; and

e. The diminution in value of Plaintiffs' and Class Members' Sensitive Health Information and/or the loss of privacy due to Defendant making such Sensitive Health Information, which Plaintiffs and Class Members intended to remain private, no longer private.

167. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Tools to track and utilize Plaintiffs' and Class Members' Sensitive Health Information for financial gain.

168. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

169. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the Tracking Tools.

170. Any purported consent that Defendant may claim it received from Plaintiffs and Class Members was not valid.

171. In sending and acquiring the content of Plaintiffs' and Class Members' communications relating to their use of the Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

172. As a result of Defendant's violation of the ECPA, Plaintiffs and the Class 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 attorneys' fees and costs.

COUNT II

VIOLATION OF THE FLORIDA SECURITY OF COMMUNICATIONS ACT
Fla. Stat. § 934.01, et seq.
(On behalf of Plaintiffs and the Florida Subclass)

173. Plaintiffs repeat and reallege the allegations contained in the foregoing paragraphs as if fully set forth herein.

174. The Florida Secretary of Communications Act ("FSCA") is codified at Florida Statutes, § 934.01, et seq. The FSCA begins with legislative findings, including:

> On the basis of its own investigations and of published studies, the Legislature makes the following findings...(4) to safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communications has consented to the interceptions should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.

175. Florida Statutes § 934.10 provides, in pertinent part, as follows:

> Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of §§ 934.04-934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including: (a) [p]reliminary or equitable declaratory relief as may be appropriate; (b) [a]ctual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of the violation or $1,0000, whichever is higher; (c) [p]unitive damages; and (d) [a] reasonable attorney's fee and other litigation costs reasonably incurred.

176. The FCSA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic, or photo-optical systems that affects intrastate, interstate, or foreign commerce." Fla. Stat. § 934.02(12).

177. It further defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Fla. Stat. § 934.02(3).

178. At all relevant times, Defendant aided, employed, agreed with, and conspired with Google to intercept Plaintiffs' and the Florida Subclass Members' internet communications in Florida while accessing the Website, including the contents thereof—i.e., the URLs visited, the medical conditions and types of treatments, and appointment details. Such information not only constitutes protected health information, but it also represents the substance, import, and meaning of the communications between Plaintiffs and other Florida Subclass Members had with Defendant's Website.

179. Plaintiffs and other Florida Subclass Members had a reasonable expectation of privacy in the electronic communications they had with Defendant's Website.

180. Nonetheless, these electronic communications were transmitted to and intercepted by a third party, including Google, during the communication and without knowledge, authorization, or consent of Plaintiffs and Florida Subclass Members. That is because Defendant intentionally inserted an electronic device into its Website that, without the knowledge and consent of Plaintiffs and Florida Subclass Members, recorded and transmitted the substance of their confidential communications with Defendant to a third party.

181. Plaintiffs and other members of the Florida Subclass used Defendant's Website from Florida.

182. Defendant willingly facilitated Google's interception and collection of Plaintiffs' and Florida Subclass Members' Private Information by embedding the Tracking Tools and other third party tracking codes on its Website.

183. Defendant used the following items as a device or apparatus to intercept wire, electronic, or oral communications made by Plaintiffs and other Class Members:

a. The Tracking Tools, Google Analytics, cookies and other tracking codes and programs deployed by Defendant to track Plaintiffs' and Florida Subclass Members' communications while they were navigating Defendant's Website;

b. Plaintiffs' and Florida Subclass Members' browsers;

c. Plaintiffs' and Florida Subclass Members' computing and mobile devices;

d. Defendants' web and ad-servers;

e. The web and ad-servers from which Google and other third parties tracked and intercepted Plaintiffs' and Florida Subclass Members' communications while they accessed and/or navigated Defendant's Website, and

f. The Tracking Tools, Google Analytics, cookies and other computer codes and programs used by Google and other third parties to effectuate its tracking and interception of Plaintiffs' and Florida Subclass Members' communications while they used Defendant's Website.

184. Defendant fails to disclose that it is using the Tracking Tools specifically (and other invisible tracking technologies from third parties) to track and automatically and simultaneously transmit communications to a third party, i.e., Google.

185. To avoid liability under the FCSA, a defendant must show it had the consent of all parties to a communication.

186. The patient communication information that Defendant transmits to Google and other unauthorized third parties while using the Tracking Tools and other tracking codes, such as

appointment booking information, the type of medical diagnosis, including diagnostic screening, and IP addresses and unique personal identifiers such as the CID, constitutes protected health information.

187. As demonstrated hereinabove, Defendant violates the FCSA by intercepting and aiding and permitting third parties such as Google to receive its Users' online communications in real time through its Website without their consent.

COUNT III

COMMON LAW INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Florida Subclass)

188. Plaintiffs repeat and reallege the allegations contained in the foregoing paragraphs as if fully set forth herein.

189. Plaintiffs and the Florida Subclass Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, highly personal Sensitive Health Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to the exfiltration of their communications without Plaintiffs' and Class Members' knowledge or consent.

190. Plaintiffs and the Florida Subclass Members had a reasonable expectation of privacy in their communications with Defendant via the Website and the communications platforms and services therein.

191. Plaintiffs and the Florida Subclass Members communicated Sensitive Health Information that they intended for only Defendant to receive and that they understood Defendant would keep private and secure.

192. Defendant's interception and disclosure of the substance and nature of those communications to third parties without the knowledge and informed consent of Plaintiffs and the Florida Subclass Members is an intentional intrusion on Plaintiffs' and the Florida Subclass Members' solitude or seclusion.

193. Plaintiffs and the Florida Subclass Members have a general expectation that their communications regarding sensitive, highly personal information would be protected from surreptitious disclosure to third parties.

194. Defendant's disclosure and publicization of Plaintiffs' and the Florida Subclass Members' Sensitive Health Information coupled with individually identifying information is highly offensive to the reasonable person.

195. As a result of Defendant's actions, Plaintiffs and the Florida Subclass Members have suffered harm and injury including, but not limited to, an invasion of their privacy rights.

196. Plaintiffs and the Florida Subclass Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to compensatory and/or nominal damages.

197. Plaintiffs and the Florida Subclass Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiffs and the Florida Subclass Members for the harm to their privacy interests as a result of the intrusions upon their privacy.

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

199. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT IV

NEGLIGENCE
(On Behalf of Plaintiffs and the Florida Subclass)

200. Plaintiffs repeat and reallege the allegations contained in the foregoing paragraphs as if fully set forth herein.

201. Through their use of the Website, Plaintiffs and the Florida Subclass Members provided Defendant with their Sensitive Health Information, believing such information would be kept confidential.

202. By collecting and storing this data, Defendant had a duty of care to use reasonable means to secure and safeguard it from unauthorized disclosure to third parties.

203. Defendant negligently failed to take reasonable steps to protect Plaintiffs' and the Florida Subclass Members' Sensitive Health Information from being disclosed to third parties, without their consent, including to Google.

204. Defendant further negligently omitted to inform Plaintiffs and the Florida Subclass Members that it would use their Sensitive Health Information for marketing purposes, and/or that their Sensitive Health Information would be transmitted to third parties.

205. Defendant knew, or reasonably should have known, that Plaintiffs and the Florida Subclass Members would not have provided their Sensitive Health Information to Defendant had they known that Defendant intended to use that information for unlawful purposes.

206. Defendant's conduct has caused Plaintiffs and the Florida Subclass Members to suffer damages by having their highly personal, personally identifiable Sensitive Health Information accessed, stored, and disseminated without their knowledge or consent.

207. Plaintiffs and the Florida Subclass Members are entitled to compensatory, nominal,

and/or punitive damages.

208. Defendant's negligent conduct is ongoing, in that it still holds the Sensitive Health Information of Plaintiffs and the Florida Subclass Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT V

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Florida Subclass)

209. Plaintiffs repeat and reallege the allegations contained in the foregoing paragraphs as if fully set forth herein.

210. When Plaintiffs and Class Members provided their Sensitive Health Information to Defendant in exchange for information and services related to breast cancer screening and mammography, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose the Sensitive Health Information without consent.

211. Plaintiffs and the Florida Subclass Members accepted Defendant's offers and provided their Sensitive Health Information to Defendant.

212. Plaintiffs and the Florida Subclass Members would not have entrusted Defendant with their Sensitive Health Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Sensitive Health Information without consent.

213. Defendant breached these implied contracts by disclosing Plaintiffs' and the Florida Subclass Members' Sensitive Health Information to third parties like Google.

214. As a direct and proximate result of Defendant's breaches of these implied contracts,

Plaintiffs and the Florida Subclass Members sustained damages as alleged herein.

215. Plaintiffs and the Florida Subclass Members would not have used Defendant's services, or would have paid substantially less for those services, had they known their Sensitive Health Information would be disclosed.

216. Plaintiffs and the Florida Subclass Members are entitled to compensatory, consequential, and/or nominal damages as a result of Defendant's breaches of implied contract.

COUNT VI

UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Florida Subclass)

217. Plaintiffs repeat and reallege the allegations contained in the foregoing paragraphs as if fully set forth herein.

218. Plaintiffs plead this claim in the alternative to their breach of implied contract claim.

219. Plaintiffs and the Florida Subclass Members conferred a monetary benefit on Defendant in exchange for information and services related to breast cancer screening and other diagnostic imaging. Specifically, they provided their Sensitive Health Information to Defendant which Defendant then utilized for marketing and advertising purposes, as described, *supra*.

220. Defendant knew that Plaintiffs and the Florida Subclass Members conferred a benefit upon them, which Defendant accepted. Defendant profited from the Sensitive Health Information of Plaintiffs and the Florida Subclass Members by exchanging it for marketing and advertising services.

221. In particular, Defendant enriched itself by obtaining the inherent value of Plaintiffs' and the Florida Subclass Members' Sensitive Health Information, and by saving the costs it reasonably should have expended on marketing and/or data security measures to secure Plaintiffs' and Florida Subclass Members' Sensitive Health Information.

222. Plaintiffs and the Florida Subclass Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the privacy of its users' and Sensitive Health Information.

223. Under the principles of equity and good conscience, Defendant should not be permitted to retain such benefits obtained by its surreptitious collection and transmission of Plaintiff's and Florida Subclass Members' Sensitive Health Information.

224. If Plaintiffs and the Florida Subclass Members knew that Defendant had not reasonably secured their Sensitive Health Information, they would not have agreed to provide their Sensitive Health Information to Defendant.

225. Plaintiffs and the Florida Subclass Members have no adequate remedy at law for this count. An unjust enrichment theory provides the equitable disgorgement of profits even where an individual has not suffered a corresponding loss in the form of money damages.

226. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Florida Subclass Members have suffered and will continue to suffer injury.

227. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Florida Subclass Members, proceeds that they unjustly received from them, or to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and other Class Members, pray for judgment against Defendant as follows:

A. an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

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

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

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

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

F. prejudgment interest on all amounts awarded; and

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

Dated: April 9, 2026

Respectfully submitted,

/s/ Matthew J. Langley

Matthew J. Langley (SBN 97331)
ALMEIDA LAW GROUP LLC
849 W. Webster Ave.
Chicago, Illinois 60614
Tel.: (773) 554-9354
matt@almeidalawgroup.com