

**FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
COURT OF COMMON PLEAS OF PHILADELPHIA**



JOHNATHON MOHR, ANNA GALLINI, SAMUEL BEST, STEPHANIE CISSORSKY, MAYA SHENGOLD, ELI STEIKER-GINZBERG, LUDWIG VANTRIKT, DANIEL WINIKUR, LISA WATT, IAN ZOLITOR, MARKEITA REID, and COLIN POWERS, for themselves and others similarly situated,

Plaintiffs,

v.

THE TRUSTEES OF THE UNIVERSITY OF PENNSYLVANIA AS OWNER AND OPERATOR OF THE UNIVERSITY OF PENNSYLVANIA HEALTH SYSTEM (d/b/a PENN MEDICINE),

Defendant.

NOTICE TO DEFEND

NOTICE

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

You should take this paper to your lawyer at once. If you do not have a lawyer or cannot afford one, go to or telephone the office set forth below to find out where you can get legal help.

**Philadelphia Bar Association
Lawyer Referral
and Information Service
One Reading Center
Philadelphia, Pennsylvania 19107
(215) 238-6333
TTY (215) 451-6197**

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de estas demandas expuestas en las paginas siguientes, usted tiene veinte (20) dias de plazo al partir de la fecha de la demanda y la notificacion. Hace falta ascender una comparencia escrita o en persona o con un abogado y entregar a la corte en forma escrita sus defensas o sus objeciones a las demandas en contra de su persona. Sea avisado que si usted no se defiende, la corte tomara medidas y puede continuar la demanda en contra suya sin previo aviso o notificacion. Ademias, la corte puede decidir a favor del demandante y requiere que usted cumpla con todas las provisiones de esta demanda. Usted puede perder dinero o sus propiedades u otros derechos importantes para usted.

Lleve esta demanda a un abogado inmediatamente. Si no tiene abogado o si no tiene el dinero suficiente de pagar tal servicio. Vaya en persona o llame por telefono a la oficina cuya direccion se encuentra escrita abajo para averiguar donde se puede conseguir asistencia legal.

**Asociacion De Licenciados
De Filadelfia
Servicio De Referencia E
Informacion Legal
One Reading Center
Filadelfia, Pennsylvania 19107
(215) 238-6333
TTY (215) 451-6197**

**CHIMICLES SCHWARTZ KRINER
& DONALD-SMITH LLP**

Steven A. Schwartz (PA I.D. No. 50579)
361 W. Lancaster Avenue
Haverford, PA 19041
Tel: (610) 642-8500
Fax: (610) 649-3633
E-Mail: sas@chimicles.com

Counsel for Plaintiffs

* Additional counsel listed on signature page

JOHNATHON MOHR, ANNA GALLINI,
SAMUEL BEST, STEPHANIE CISSORSKY,
MAYA SHENGOLD, ELI STEIKER-
GINZBERG, LUDWIG VANTRIKT, DANIEL
WINIKUR, LISA WATT, IAN ZOLITOR,
MARKEITA REID, and COLIN POWERS, for
themselves and others similarly situated,

Plaintiffs,

v.

THE TRUSTEES OF THE UNIVERSITY OF
PENNSYLVANIA AS OWNER AND
OPERATOR OF THE UNIVERSITY OF
PENNSYLVANIA HEALTH SYSTEM (d/b/a
PENN MEDICINE),

Defendant.

IN THE COURT OF COMMON
PLEAS OF PHILADELPHIA
COUNTY, PENNSYLVANIA

COMMERCE PROGRAM

Case No. 230102149

**FIRST AMENDED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Johnathon Mohr, Anna Gallini, Samuel Best, Stephanie Cissorsky, Maya Shengold, Eli Steiker-Ginzberg, Ludwig vanTrikt, Daniel Winikur, Lisa Watt, Ian Zolitor, Markeita Reid, and Colin Powers (“Plaintiffs”), on behalf of themselves and all other similarly situated individuals (the “Class Members”) against The Trustees of the University of Pennsylvania as Owner and Operator of the University of Pennsylvania Health System (“Defendant” or “Penn

Medicine”) bring this action based upon personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all Pennsylvania residents who have accessed and used the myPennMedicine app (the “App”) or any medical website owned and operated by Defendant, including but not limited to: pennmedicine.org; pennbehavioralhealth.org; and/or uphs.upenn.edu (collectively, the “Website”).

2. Defendant aids employs, agrees, and conspires with third parties, including Facebook/Meta¹, Google LLC (“Google”), LinkedIn Corporation (“LinkedIn”), Snap Inc. (“Snap”), and Bytedance, also known as TikTok (“TikTok”) to intercept communications sent and received by Plaintiffs and Class Members, including communications containing protected medical information. Plaintiffs bring this action for legal and equitable remedies resulting from these illegal actions.

JURISDICTION AND VENUE

3. The Court has subject matter jurisdiction over this action pursuant to Pa. Cons. Art. 5, §5(b) and 42 Pa. C.S.A. § 931(b).

4. The Court has personal jurisdiction over Defendant pursuant to 42 Pa. C.S.A. 5301(a)(2).

5. Venue is proper pursuant to Pa. R. Civ. P. 2179(a)(1) because Defendant’s principal place of business is located in this County

¹ In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Unless otherwise indicated, Facebook, Inc. and Meta Platforms, Inc. are referenced collectively herein as “Facebook.”

THE PARTIES

Plaintiff Mohr

6. Plaintiff Johnathon Mohr is an adult citizen of the Commonwealth and is domiciled in Norristown, Pennsylvania.

7. From 2020 to 2022, Plaintiff Mohr used the Website, including its patient portal, to schedule an appointment and access medical results. Plaintiff Mohr accessed the Website using a tablet and desktop computer. As described below, each time Plaintiff Mohr booked medical appointments, he disclosed medical information regarding his medical condition, history or treatment.

8. Plaintiff Mohr also has an active Facebook account which he has maintained since 2020. Plaintiff Mohr accesses his Facebook account from multiple devices, including his tablet, smartphone and desktop computer.

Plaintiff Gallini

9. Plaintiff Anna Gallini is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

10. From 2020 through 2024, Plaintiff Gallini used the Website, including its patient portal, schedule an appointment and access medical results. Plaintiff Gallini accessed the Website using a mobile phone and laptop computer. As described below, each time Plaintiff Gallini booked medical appointments, she disclosed medical information regarding her medical condition, history or treatment

11. Plaintiff Gallini also has an active Facebook and/or Google account which she has maintained since at least 2020. Plaintiff Gallini accesses her Facebook and/or Google account from multiple devices, including her mobile phone and laptop computer.

Plaintiff Best

12. Plaintiff Samuel Best is an adult citizen of the Commonwealth and is domiciled in Langhorne, Pennsylvania.

13. From 2021 to 2024, Plaintiff Best used the Website, including its patient portal, to schedule an appointment and access medical results. Plaintiff Best accessed the Website using a mobile phone, iPad, and desktop computer. As described below, each time Plaintiff Best booked medical appointments, he disclosed medical information regarding his medical condition, history or treatment.

14. Plaintiff Best also has an active Facebook and/or Google account which he has maintained since at least 2021. Plaintiff Best accesses his Facebook and/or Google account from multiple devices, including his mobile phone, iPad, and desktop computer.

Plaintiff Cissorsky

15. Plaintiff Stephanie Cissorsky is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

16. From 2020 through 2024, Plaintiff Cissorsky used the Website, including its patient portal, schedule an appointment and access medical results. Plaintiff Cissorsky accessed the Website using a mobile phone, laptop computer, and desktop computer. As described below, each time Plaintiff Cissorsky booked medical appointments, she disclosed medical information regarding her medical condition, history or treatment

17. Plaintiff Cissorsky also has an active Facebook and/or Google account which she has maintained since at least 2020. Plaintiff Cissorsky accesses her Facebook and/or Google account from multiple devices, including her mobile phone, laptop computer, and desktop computer.

Plaintiff Shengold

18. Plaintiff Maya Shengold is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

19. From 2020 through 2024, Plaintiff Shengold used the Website, including its patient portal, schedule an appointment and access medical results. Plaintiff Shengold accessed the Website using a mobile phone and desktop computer. As described below, each time Plaintiff Shengold booked medical appointments, she disclosed medical information regarding her medical condition, history or treatment

20. Plaintiff Shengold also has an active Facebook and/or Google account which she has maintained since at least 2020. Plaintiff Shengold accesses her Facebook and/or Google account from multiple devices, including her mobile phone and desktop computer.

Plaintiff Steiker-Ginzberg

21. Plaintiff Eli Steiker-Ginzberg is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

22. From 2020 to 2024, Plaintiff Steiker-Ginzberg used the Website, including its patient portal, to schedule an appointment and access medical results. Plaintiff Steiker-Ginzberg accessed the Website using a mobile phone and laptop computer. As described below, each time Plaintiff Steiker-Ginzberg booked medical appointments, he disclosed medical information regarding his medical condition, history or treatment.

23. Plaintiff Steiker-Ginzberg also has an active Facebook and/or Google account which he has maintained since at least 2021. Plaintiff Steiker-Ginzberg accesses his Facebook and/or Google account from multiple devices, including his mobile phone and laptop computer.

Plaintiff vanTrikt

24. Plaintiff Ludwig vanTrikt is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

25. From 2020 to 2024, Plaintiff vanTrikt used the Website, including its patient portal, to schedule an appointment and access medical results. Plaintiff vanTrikt accessed the Website using a mobile phone and desktop computer. As described below, each time Plaintiff vanTrikt booked medical appointments, he disclosed medical information regarding his medical condition, history or treatment.

26. Plaintiff vanTrikt also has an active Facebook and/or Google account which he has maintained since at least 2020. Plaintiff vanTrikt accesses his Facebook and/or Google account from multiple devices, including his mobile phone and desktop computer.

Plaintiff Winikur

27. Plaintiff Daniel Winikur is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

28. From 2022 to 2024, Plaintiff Winikur used the Website, including its patient portal, to schedule an appointment and access medical results. Plaintiff Winikur accessed the Website using a mobile phone and laptop computer. As described below, each time Plaintiff Winikur booked medical appointments, he disclosed medical information regarding his medical condition, history or treatment.

29. Plaintiff Winikur also has an active Facebook and/or Google account which he has maintained since at least 2022. Plaintiff Winikur accesses his Facebook and/or Google account from multiple devices, including his mobile phone and laptop computer.

Plaintiff Watt

30. Plaintiff Lisa Watt is an adult citizen of the Commonwealth and is domiciled in Chester Springs, Pennsylvania.

31. From 2020 through 2024, Plaintiff Watt used the Website, including its patient portal, schedule an appointment and access medical results. Plaintiff Watt accessed the Website using a mobile phone and laptop computer. As described below, each time Plaintiff Watt booked medical appointments, she disclosed medical information regarding her medical condition, history or treatment

32. Plaintiff Watt also has an active Facebook and/or Google account which she has maintained since at least 2020. Plaintiff Watt accesses her Facebook and/or Google account from multiple devices, including her mobile phone and laptop computer.

Plaintiff Zolitor

33. Plaintiff Ian Zolitor is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

34. From 2020 to 2024, Plaintiff Zolitor used the Website, including its patient portal, to schedule an appointment and access medical results. Plaintiff Zolitor accessed the Website using a mobile phone and laptop computer. As described below, each time Plaintiff Zolitor booked medical appointments, he disclosed medical information regarding his medical condition, history or treatment.

35. Plaintiff Zolitor also has an active Facebook and/or Google account which he has maintained since at least 2020. Plaintiff Zolitor accesses his Facebook and/or Google account from multiple devices, including his mobile phone and laptop computer.

Plaintiff Reid

36. Plaintiff Markeita Reid is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

37. From 2020 through 2024, Plaintiff Reid used the Website, including its patient portal, schedule an appointment and access medical results. Plaintiff Reid accessed the Website using a mobile phone, laptop computer, and desktop computer. As described below, each time Plaintiff Reid booked medical appointments, she disclosed medical information regarding her medical condition, history or treatment

38. Plaintiff Reid also has an active Facebook and/or Google account which she has maintained since at least 2020. Plaintiff Reid accesses her Facebook and/or Google account from multiple devices, including her mobile phone, laptop computer, and desktop computer.

Plaintiff Powers

39. Plaintiff Colin Powers is an adult citizen of the Commonwealth and is domiciled in Philadelphia, Pennsylvania.

40. From 2020 to 2024, Plaintiff Powers used the Website, including its patient portal, to schedule an appointment and access medical results. Plaintiff Powers accessed the Website using a mobile phone and laptop computer. As described below, each time Plaintiff Powers booked medical appointments, he disclosed medical information regarding his medical condition, history or treatment.

41. Plaintiff Powers also has an active Facebook and/or Google account which he has maintained since at least 2020. Plaintiff Powers accesses his Facebook and/or Google account from multiple devices, including his mobile phone and laptop computer.

Defendant

42. Defendant The Trustees of the University of Pennsylvania is a registered nonprofit entity with its principal place of business in Pennsylvania. Defendant employs approximately 20,433 individuals. As of June 2021, Defendant reported revenue of approximately \$9.3 billion and total assets of approximately \$31 billion. Through Penn Medicine, Defendant offers a full range of medical services, including primary, inpatient and outpatient care, and treats thousands of patients each year.

43. Pursuant to the systematic process described herein, Defendant, through Penn Medicine, assisted third parties, including Facebook, Google, LinkedIn, Snap, and TikTok with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information and related confidential information. Defendant assisted these interceptions without Plaintiff's knowledge, consent or express written authorization.

44. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiffs' personally identifiable information ("PII") and protected health information ("PHI").

FACTUAL ALLEGATIONS

The Pennsylvania Wiretapping and Electronic Surveillance Control Act

45. The Pennsylvania Wiretapping and Electronic Surveillance Control Act (the "Pennsylvania Wiretapping Act") prohibits: (a) the interception or procurement of another to intercept any wire, electronic or oral communication; (b) the intentional disclosure of the contents of any wire, electronic or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication; and (c) the intentional use of the contents of any wire, electronic or oral communication that the discloser

knew or should have known was obtained through the interception of a wire, electronic or oral communication. 18 Pa. Cons. Stat. § 5703.

46. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose or use, a wire, electronic, or oral communication in violation of the Pennsylvania Wiretapping Act is subject to a civil action for: (a) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (b) punitive damages; and (c) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

47. Under the Pennsylvania Wiretapping Act, "intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

48. Under the Pennsylvania Wiretapping Act, "contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

49. Under the Pennsylvania Wiretapping Act, "person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

50. Under the Pennsylvania Wiretapping Act, "electronic communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

51. Pursuant to the Pennsylvania Wiretapping Act, the Commonwealth and any of its officers, officials or employees who may be shielded from liability under the Pennsylvania

Wiretapping Act by the doctrine of sovereign immunity waive such immunity. 18 Pa. Const. Stat. § 5725(b).

Penn Medicine and Its Website

52. Penn Medicine has six acute care hospitals, eight multispecialty centers and hundreds of outpatient locations within the Commonwealth. In fiscal year 2021, Penn Medicine had: (a) approximately 6.5 million outpatient visits; (b) over 337,000 emergency department visits; and (c) over 3,400 hospital beds.

53. Penn Medicine offers a full range of medical services, including primary, inpatient and outpatient care.

54. Penn Medicine has at least three websites – pennmedicine.org; pennbehavioralhealth.org; and uphs.upenn.edu, as well as at least one patient portal that can be accessed via <https://secure.mypennmedicine.org/MyPennMedicine/Authentication/Login?> – that are accessible on mobile devices and desktop computers. Penn Med also offers the App for download on Android and iPhone devices.

Facebook’s Platform and Business Tools

55. Facebook describes itself as a “real identity platform,”² meaning users are allowed only one account and must share “the name they go by in everyday life.”³ To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.⁴

² Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

³ FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

⁴ FACEBOOK, SIGN UP, <https://www.facebook.com/>

56. In 2021, Facebook generated \$117 billion in revenue.⁵ Roughly 97% of that came from selling advertising space.⁶

57. Facebook sells advertising space by highlighting its ability to target users.⁷ Facebook can target users so effectively because it surveils user activity both on and off its site.⁸ This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”⁹ Facebook compiles this information into a generalized dataset called “Core Audiences,” which advertisers use to apply highly specific filters and parameters for their targeted advertisements.¹⁰

58. Advertisers can also build “Custom Audiences.”¹¹ Custom Audiences enables advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”¹² With Custom Audiences, advertisers can target existing customers directly, and they can also build “Lookalike Audiences,” which “leverage[] information such as demographics, interests, and behavior from

⁵ FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx>

⁶ *Id.*

⁷ FACEBOOK, WHY ADVERTISE ON FACEBOOK, <https://www.facebook.com/business/help/205029060038706>.

⁸ FACEBOOK, ABOUT FACEBOOK PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

⁹ FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

¹⁰ FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences>.

¹¹ FACEBOOK, ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

¹² FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

your source audience to find new people who share similar qualities.”¹³ Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. Advertisers can do so through two mechanisms: (a) by manually uploading contact information for customers; or (b) by utilizing Facebook’s “Business Tools.”¹⁴

59. As Facebook puts it, the Business Tools “help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services.”¹⁵ Put more succinctly, Facebook’s Business Tools are bits of code that advertisers can integrate into their websites, mobile applications and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

60. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, the webpage’s Universal Resource Locator (“URL”) and metadata, or when a user downloads a mobile application or makes a purchase.¹⁶ Facebook’s Business Tools can also track other events. Facebook offers a menu of “standard events” from which advertisers

¹³ FACEBOOK, ABOUT LOOKALIKE AUDIENCES, <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

¹⁴ FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494>.

¹⁵ FACEBOOK, THE FACEBOOK BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087>.

¹⁶ See FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>.

can choose, including what content a visitor views or purchases.¹⁷ Advertisers can even create their own tracking parameters by building a “custom event.”¹⁸

61. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their websites. As the name implies, the Facebook Tracking Pixel “tracks the people and type of actions they take.”¹⁹ When a user accesses a website hosting the Facebook Tracking Pixel, Facebook’s software script surreptitiously directs the user’s browser to send a separate message to Facebook’s servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Tracking Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser’s attempt to load and read Defendant’s websites—Defendant’s own code and Facebook’s embedded code.

62. An example illustrates the point. Take an individual who navigates to one of Defendant’s websites and clicks on a tab for allergy information. When that tab is clicked, the individual’s browser sends a GET request to Defendant’s server requesting that server to load the particular webpage. Because Defendant utilizes the Facebook Tracking Pixel, Facebook’s embedded code, written in JavaScript, sends secret instructions back to the individual’s browser, without alerting the individual that this is happening. Facebook causes the browser to secretly and concurrently duplicate the communication with the Penn Medicine website at issue, transmitting

¹⁷ FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

¹⁸ FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; *see also* FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>.

¹⁹ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

63. After collecting and intercepting this information, Facebook processes it, analyzes it and assimilates it into datasets like Core Audiences and Custom Audiences.

Google Analytics

64. Google offers a range of advertising software, one of which is called Google Analytics.

65. "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights" for businesses.²⁰ This is made possible by Google Analytics, a piece of code installed on a website or app that collects information on how website and app users interact with a business's website, including "how many users bought an item . . . by tracking whether they made it to the purchase-confirmation page."²¹

66. Google advertises that this service can "[m]onitor activity on your site as it happens."²²

67. Google's business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners' websites with Google Analytics.

68. Thus, through websites and apps that employ Google's services, Google directly receives the electronic communications of website visitors entered into websites via website and app features like search bars.

²⁰ GOOGLE, HOW GOOGLE ANALYTICS WORKS, https://support.google.com/analytics/answer/12159447?hl=en&ref_topic=14089939&sjid=2827624563183915220-NC.

²¹ *Id.*

²² GOOGLE, THE FINER POINTS, <https://marketingplatform.google.com/about/analytics/features/>.

69. That information is then analyzed by Google before it is provided to any entity that was a party to the conversation (like Defendant). In order to conduct this analysis, Google, on information and belief, views the information.

70. Once Google intercepts website or app communications, it has the capability to use such information for its own purposes. “Google uses the information shared by sites and apps to deliver [] services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on [] partners’ sites and apps.”²³

71. Google’s range of software services is based on Google’s ability to collect and analyze information about consumers’ web behavior and deliver targeted advertising to select consumers based on their web habits. This involves collecting visitor information from thousands of websites and then analyzing that information in order to group web users so they can be targeted for products or services based on their interests.

72. In order to engage in analyzing the collected data to deliver targeted advertising, Google, on information and belief, regularly viewed and used the sensitive health information collected by the Google Analytics code. As such, on information and belief, Google regularly viewed and used Plaintiffs and Class Members’ health information collected and/or intercepted via Google Analytics.

73. Information from websites and apps, like Defendant’s App and Website, is central to Google’s ability to successfully market its advertising capabilities to future clients.

74. In sum, Google has the capability to use website and app communications to: (a) improve its own products and services; (b) develop new Google for Business and Google Analytics

²³ GOOGLE, GOOGLE PRIVACY AND TERMS, <https://policies.google.com/technologies/partner-sites>.

products and services; and (c) analyze website visitors' communications to assist with and data analytics and targeted advertising.

75. Further, Defendant shares information with Google that amounts to PII via its collection of device identifiers and IP addresses. Device identifiers and IP addresses are types of information that the U.S. Department of Health and Human Services lists as information that should be removed to de-identify a patient in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").²⁴ Google uses IP addresses and unique device identifiers to track internet users. Therefore, Defendant is disclosing both PHI and PII to Google as described in the section below.

76. Yet another type of PII obtained from Website users by Google, and subsequently viewed by Google, is what data companies refer to as a "browser-fingerprint." A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

77. These browser-fingerprints provide a wide variety of data and can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked. As Google explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."²⁵

²⁴ U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard>.

²⁵ GOOGLE, BUILDING A MORE PRIVATE WEB, <https://www.blog.google/products/chrome/building-a-more-private-web/>.

The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.²⁶ Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.²⁷

78. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.²⁸

79. Browser-fingerprints are personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

80. Defendant uses and causes the disclosure of data sufficient for third parties, like Google, to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning appointments booked, lab work test results, searches for labs, searches for medical conditions, and searches for doctors.

LinkedIn Platform and its Business Tools

81. Defendant also utilized LinkedIn's Insight Tag on its App and Website. LinkedIn offers its LinkedIn Marketing Solutions so that businesses can "[b]uild long-term relationships with the world's largest professional audience."²⁹

82. LinkedIn Marketing Solutions offers a range of advertising tools to its clients. One of those tools is the Insight Tag.³⁰ The Insight Tag is "[a] simple code snippet added to [a] website

²⁶ Chris Hauk, *What is Browser Fingerprinting? How it Works and How to Stop it*, <https://pixelprivacy.com/resources/browser-fingerprinting/>.

²⁷ *Supra* note 37.

²⁸ Yinzhi Cao, Song Li & Erik Wijmans, *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*, <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/>.

²⁹ <https://business.linkedin.com/marketing-solutions/success/marketing-terms/b2b-vs-b2c>

³⁰ LINKEDIN, INSIGHT TAG, <https://business.linkedin.com/marketing-solutions/insight-tag>.

[that] can help [] optimize [] campaigns, retarget [] website visitors, and learn more about [] audiences.”³¹ When a website owner uses the Insight Tag, LinkedIn tracks conversions by tracking actions website visitors take “such as submitting leads, downloading content,” “page visits and clicks.”³² The Insight Tag also collects data on a website visitor including “the URL, referrer, IP address, [and] device and browser characteristics.”³³ Regarding website users’ direct identifiers, the Insight Tag initially collects this data, and removes it seven days after collection.³⁴

83. Website owners can also define for LinkedIn which actions their users take on their website should be considered conversions.³⁵ Once the Insight Tag begins collecting conversion data, “LinkedIn automatically optimize[s] [] campaigns for even more conversions.”³⁶

84. Further, LinkedIn Marketing Solutions drives conversions by allowing clients to create a target audience “based on members who visited a specific page on [their] site”³⁷ or based on the “actions taken on [their] website.”³⁸

³¹ *Id.*

³² LINKEDIN, CONVERSION TRACKING, <https://business.linkedin.com/marketing-solutions/conversion-tracking>

³³ LINKEDIN, LINKEDIN INSIGHT TAG FAQs, <https://www.linkedin.com/help/lms/answer/a427660>.

³⁴ *Id.*

³⁵ LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy#use>.

³⁶ LINKEDIN, GET STARTED WITH LINKEDIN WEBSITE RETARGETING, <https://www.linkedin.com/help/lms/answer/a420433/>.

³⁷ LINKEDIN, RETARGETING WITH MATCHED AUDIENCES, https://www.linkedin.com/help/lms/answer/a427551/?mcid=7059959449221829914&gclid=Cj0KCQjwvb-zBhCmARIsAAfUI2t90seE9eaMsRB9a_9uU3LxOel1HCiKf3dr8q_sr7DrsMIL2SkVRsWaAmRxEALw_wcB&src=go-pa&veh=null&trk=sem-ga_campid.20065362147_asid.148056420385_crid.657161018051_kw.linkedin%2520tracking%2520pixel_d.c_tid.kwd-808912161273_n.g_mt.e_geo.9032535.

³⁸ LINKEDIN, GET STARTED WITH LINKEDIN WEBSITE RETARGETING, <https://www.linkedin.com/help/lms/answer/a420433/>.

85. LinkedIn also offers its clients Audience Insights which is information about a client's "matched or saved audiences – like job titles, company names and industries" so that clients can "adjust and reach audiences who are most likely to become qualified leads and customers."³⁹

86. Thus, through websites that employ LinkedIn's services, LinkedIn directly receives the electronic communications of website visitors, which can include PII and PHI entered into websites via website features like search bars or through URLs.

87. Information and communications that LinkedIn collects and/or intercepts are analyzed by LinkedIn before being provided to any entity that was a party to the conversation (like Defendant). In order to conduct this analysis, LinkedIn, on information and belief, views the information. As such, on information and belief, LinkedIn viewed and used Plaintiffs and Class Members' sensitive health information, PII and PHI collected in the course of providing targeted advertising for Penn Medicine.

88. Once LinkedIn intercepts website communications, it has the capability to use such information for its own purposes beyond recording the data for the website owner. LinkedIn uses the information collected or intercepted "to conduct research and development for [its] Services in order to provide" LinkedIn users with a "better, more intuitive and personalized experience" and increase "growth and engagement" of its Services.⁴⁰

³⁹ LINKEDIN, AUDIENCE INSIGHTS, <https://business.linkedin.com/marketing-solutions/audience-insights>

⁴⁰ LINKEDIN, PRIVACY POLICY, <https://www.linkedin.com/legal/privacy-policy#use>.

The TikTok Pixel

89. TikTok offers a software-as-a-service (“SaaS”) called “TikTok Pixel,” which “helps businesses track the performance of their ads” by sending information from the business’s website to TikTok, who then uses that information to optimize ad campaigns on TikTok and across the internet.⁴¹

90. The TikTok pixel can be “plugged in” to any website, as the pixel is a piece of code that can be added to any website to capture “events” (*i.e.*, any activity by a user that happens on a website).

91. The TikTok Pixel is part of a package of prebuilt software tools under the “TikTok for Business” product line that allow for the delivery of personalized ads. By employing TikTok to collect user information through the TikTok Pixel, websites that procure TikTok’s services can use the information to deliver more effective targeted advertisements, increasing revenue for the websites.

92. In short, when users interact with a webpage in which the TikTok Pixel is integrated, embedded and/or installed, the TikTok Pixel collects the “Metadata and button clicks” (*i.e.*, information about what the user clicked on—such as the specific URL address visited by the user— or text entered into the webpage), a timestamp for the event, and the visitor’s IP address.⁴² That information is sent automatically to TikTok.

93. The “TikTok for Business” business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners’ websites with the TikTok Pixel.

⁴¹ “TikTok Pixel 101: What It Is & How to Use It,” <https://popupsmart.com/blog/tiktok-pixel>

⁴² “About TikTok Pixel,” <https://ads.tiktok.com/help/article/tiktok-pixel?redirected=2>

94. Thus, through websites that employ TikTok’s services, TikTok directly receives the electronic communications of website visitors in real time.

95. On Defendant’s App and Website, TikTok collected the URL value of the page visited, an identification code TikTok uses to track the user, and the visitor’s browser type and operating system.

96. Once TikTok intercepts website communications, it has the capability to use such information for its own purposes. TikTok’s Commercial Terms of Service grant TikTok “a non-exclusive, royalty-free, worldwide, transferable, sublicensable license to access, use, host, cache, store, display, publish, distribute, modify and adapt [information collected from partner websites] in order to develop, research, provide, promote, and improve TikTok’s products and services.”⁴³

97. In practice, this means the information collected is used to: (a) analyze trends in consumer behavior based on data collected from websites across the internet that TikTok can then use when providing targeted advertising to other companies; (b) create consumer profiles of specific users, allowing TikTok to sell future customers targeted advertising to consumers with specific profile characteristics; and (c) develop new TikTok Business products and services, or improve pre-existing TikTok Business products and services.

98. One of TikTok’s partners was Defendant. The TikTok Pixel was employed on the App and Website in the manner described throughout this Complaint.

⁴³ “TikTok For Business Commercial Terms Of Service” <https://ads.tiktok.com/i18n/official/policy/commercial-terms-of-service> (Last accessed January 17, 2024).

The Snap Pixel

99. Snap offers a SaaS called the “Snap Pixel,” which “helps advertisers measure results, optimize targeting, and build audiences for their ad campaigns.”⁴⁴

100. The Snap Pixel can be plugged into any website, as the pixel is “a piece of JavaScript code that’s either installed on [a] website or integrated with an e-commerce store.”⁴⁵

101. The Snap Pixel is part of a line of prebuilt software tools under Snapchat’s “Business” product line. By employing Snap to collect user information through the Snap Pixel, websites that procure Snap’s services can use the information to deliver personalized advertisements, increasing revenue for the websites.

102. When users interact with a webpage with the Snap Pixel installed, the Snap Pixel “tracks a variety of actions on [a] website, such as page views [*i.e.*, the URLs of webpages visited by users], add-to-cart actions, purchases, and sign-ups,” as well as other “events,” such as answering the Quiz questions.⁴⁶ The information is sent automatically to Snap.

103. The Snap advertising business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners’ websites with the Snap Pixel.

104. Thus, through websites that procure Snap’s services, Snap directly receives the electronic communications of apps and websites visitors in real time.

⁴⁴ “Power Performance With The Snap Pixel” https://forbusiness.snapchat.com/advertising/snap-pixel?_sid=PAID&utm_campaign=US_G_Search_Brand_MKAG-snapchatads&utm_content=whysnapads2&utm_medium=PAIDB2B&utm_source=GoogleSEM&utm_term=US&gclid=CjwKCAiAqNSsBhAvEiwAn_tmxW7cadFAgs3TBhgkWKuamlXzGBYv7RtoECeVCmIQmrEvZDHETtxD_hoCZSQQAvD_BwE (Last accessed January 4, 2024).

⁴⁵ *Id.*

⁴⁶ *Id.*

105. One of Snap’s partners is Defendant. The Snap Pixel was employed on Defendant’s App and Website in the manner described throughout this Complaint.

How Defendant Allowed for the Interception of Plaintiff’s and Class Members’ PII, PHI and Communications

106. Through third-party tracking technologies such as the Facebook Tracking Pixel, Google Analytics, LinkedIn Insight Tag, TikTok Pixel and Snap Pixel, Defendant – via the Website and App – allowed for the interception of the identities and online activity (including information and search results related to their private medical treatment) of Penn Medicine’s patients.

107. For example, an investigation by *The Markup* revealed that thirty-three of the top 100 hospitals in the United States, as ranked by *Newsweek*, had the Facebook Tracking Pixel embedded on the appointment schedule pages of their websites, among other possible places.⁴⁷ The Website was among the websites identified.⁴⁸

108. According to the Markup Investigation, the hospital websites were “collecting patients’ sensitive health information – including details about their medical conditions, prescriptions, and doctor’s appointments – and sending it to Facebook.”⁴⁹

109. The Markup Investigation further revealed that the data sent to Facebook was connected to: (a) the IP address of the computer sending the information, providing Facebook with the ability to connect the sensitive information to specific individual or household; or, worse: (b)

⁴⁷ Todd Feathers, *et al.*, FACEBOOK IS RECEIVING SENSITIVE MEDICAL INFORMATION FROM HOSPITAL WEBSITES, THE MARKUP (“Markup Investigation”) (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

⁴⁸ *Id.*

⁴⁹ *Id.*

a specific Facebook user if the user is logged into their Facebook account when using the websites at issue.⁵⁰

110. The Markup Investigation provided the following examples of the types of information surreptitiously intercepted by Facebook: (a) “clicking the ‘Schedule Online’ button on a doctor’s page [of a specified hospital] prompted the [Facebook Tracking Pixel] to send Facebook the text of the button, the doctor’s name, and the search term we used to find her: ‘pregnancy termination’”; and (b) clicking the “Schedule Online Now’ button on a different website “prompted the [Facebook Tracking Pixel] to send Facebook the text of the button, the doctor’s name, and the condition we selected from the dropdown menu: “Alzheimer’s.”⁵¹

111. The startling information revealed in the Markup Investigation prompted a former senior privacy advisor for the U.S. Department of Health and Human Services’ Office for Civil Rights (“Office for Civil Rights”) to remark on the troubling nature of the conduct: “I am deeply troubled by what [the hospitals] are doing with the capture of [patients’] data and the sharing of it.”⁵²

The Website

112. Penn Medicine allows patients to select options like “Find a Doctor,” “Find a Location,” “Make an Appointment,” and “Pay Your Bill.”

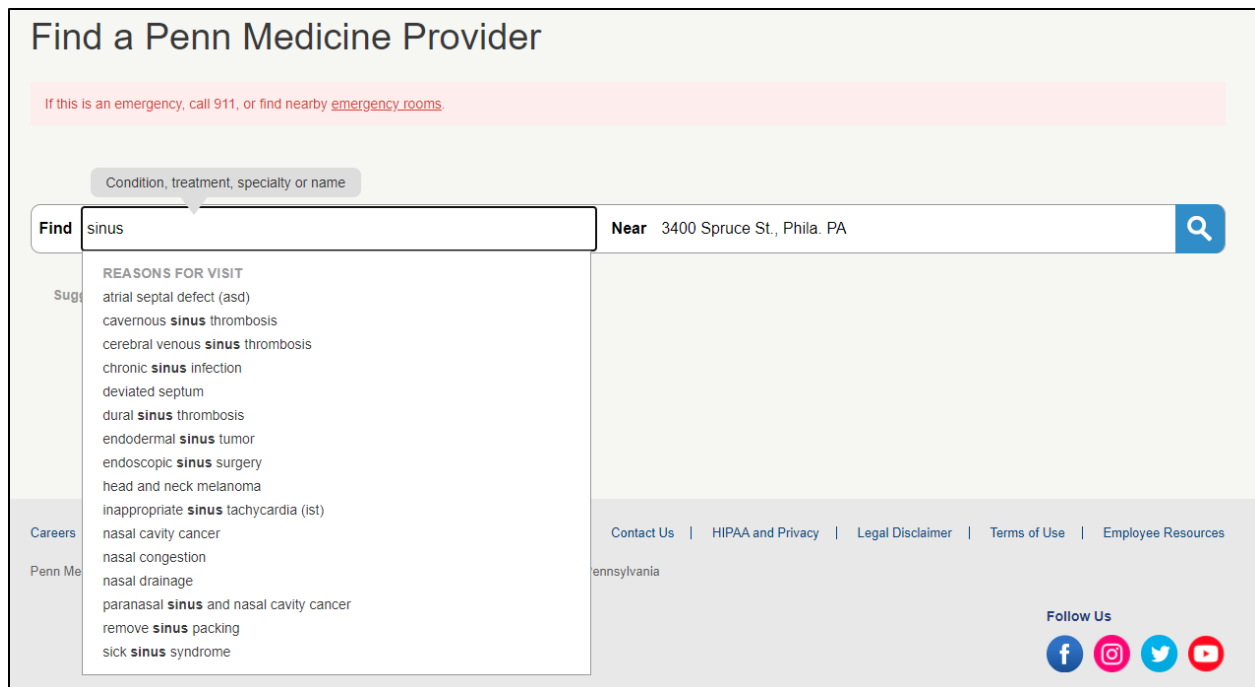
⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*



113. When patients click “Find a Doctor,” they can search by “[c]ondition, treatment, specialty, or name.”



114. When patients click “Make an Appointment,” they can click on an option to schedule an appointment through the “myPennMedicine” portal.

The screenshot shows the 'Make an Appointment at Penn Medicine' web page. At the top, there is a red banner with the text: 'If you have symptoms of an urgent nature, please contact your doctor, call 911 or go to the nearest emergency room immediately.' Below this, there are four main sections arranged in a 2x2 grid. The top-left section is titled 'Schedule with my current provider' and includes the text 'Schedule an in-person or video visit with a provider you have seen in the past 3 years via our patient portal or by phone.' It features a blue button labeled 'Login to myPennMedicine' and the text 'Or call 800-789-7366'. The top-right section is titled 'Schedule with a new provider' and includes the text 'You can request an appointment with a provider you have not seen before by phone or online.' It features a blue button labeled 'Call 800-789-7366' and the text 'Or request an appointment using our online form.' The bottom-left section is titled 'Radiology' and includes the text 'Request a radiology service such as an X-Ray, Mammogram, CAT scan, MRI or ultrasound.' The bottom-right section is titled 'Need Assistance?' and includes the text 'Speak to a member of our team.' It features a blue button labeled 'Call 800-789-7366' and the text 'Or request a callback using our online form.'

115. Upon information and belief, at relevant times, whenever patients searched their treatment or condition, or whenever patients scheduled an appointment, Defendant procured third parties, including Facebook, Google, LinkedIn, TikTok and Snap, to intercept communications that contain PII, PHI and other sensitive information.

116. Among the patient information intercepted by the third parties was PII such as a patient’s Facebook ID (“FID”), IP address and other identifiers by which the patient could be identified. An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user’s Facebook profile and name. Notably, while Facebook can easily identify any individual on its own Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as

much on its website. Indeed, to find a corresponding profile, a person need only attach the FID to the end of the URL for Facebook, typing in Facebook.com/[FID].

117. At relevant times, a user who accessed Defendant's Website while logged into Facebook transmitted what is known as the "c_user cookie" to Facebook, which contained that user's unencrypted Facebook ID.

118. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

119. One such cookie is the "fr cookie" which contains, at least, an unencrypted Facebook ID and browser identifier. Facebook, at a minimum, uses the fr cookie to identify users.⁵³

120. If a visitor has never created an account, an even small set of cookies are transmitted.

121. At relevant times, at each stage, Defendant also utilized the "_fbp cookie," which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.⁵⁴

122. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.⁵⁵ If that happens, the time resets, and another 90 days begins to accrue.⁵⁶

⁵³ FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

⁵⁴ FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

⁵⁵ See FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

⁵⁶ Confirmable through developer tools.

123. The `_fbp` cookie expires after 90 days unless the visitor's browser accesses the same website.⁵⁷ If that happens, the time rests, and another 90 days begins to accrue.⁵⁸

124. The Facebook Pixel uses both first- and third-party cookies. A first-party cookie is “created by the website the user is visiting”—*i.e.*, Penn Medicine.⁵⁹ A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—*i.e.*, Facebook.⁶⁰ The `_fbp` cookie is always transmitted as a first-party cookie. A duplicate `_fbp` cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

125. Facebook, at a minimum, uses the `fr`, `_fbp`, and `c_user` cookies to link to Facebook IDs and corresponding Facebook profiles. Defendant sent these identifiers alongside the event data.

126. Plaintiffs never consented, agreed, or otherwise permitted Defendant to disclose their PII and PHI. Plaintiffs were never provided with any written notice that Defendant disclosed their users' PHI, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiffs' protected health information to the above-mentioned third parties.

127. By law, Plaintiffs are entitled to privacy in their PHI and confidential communications. Defendant deprived Plaintiffs of their privacy rights by procuring third parties,

⁵⁷ See FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

⁵⁸ Also confirmable through developer tools.

⁵⁹ PC MAG, FIRST-PARTY COOKIES, <https://www.pcmag.com/encyclopedia/term/first-party-cookie>. This is confirmable by using developer tools to inspect a website's cookies and track network activity.

⁶⁰ PC MAG, THIRD-PARTY COOKIES, <https://www.pcmag.com/encyclopedia/term/third-party-cookie>. This is also confirmable by tracking network activity.

including Facebook, Google, LinkedIn, TikTok and Snap, to intercept these communications by implementing a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other patients' confidential communications, PII and PHI. Plaintiff Mohr did not discover that Defendant engaged in the conduct alleged herein until January 2023.

The Expectation of Privacy in Healthcare Information

128. An individual's medical records and information are among the most sensitive type of personal information.

129. Indeed, the Commonwealth requires that medical records be treated as confidential. 28 Pa. Code § 115.27.

130. Similarly, the Health Insurance Portability and Accountability Act of 1996 ("HIPPA") imposes strict standards to protect sensitive patient health information from being disclosed without the patients' knowledge and consent. *See* 45 C.F.R. § 160, *et seq.*

131. On December 1, 2022, the Office for Civil Rights issued a bulletin titled *Use of Online Tracking Technologies by HIPPA Covered Entities and Business Associates* (the "Bulletin") in which it addressed the impropriety of healthcare providers utilizing tracking technologies such as the Facebook Tracking Pixel in a manner that impermissibly discloses protected health information ("PHI") in violation of the HIPPA.⁶¹

132. According to the Office for Civil Rights, "[r]egulated entities [those to which HIPPA applies] **are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of [protected health information] to tracking technology**

⁶¹ U.S. Dep't of Health and Human Services – Office for Civil Rights, *Use of Online Tracking Technologies by HIPPA Covered Entities and Business Associates* (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

vendors or any other violations of the HIPPA Rules.”⁶² As set forth in the Bulletin, “disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPPA-compliant authorizations, would constitute impermissible disclosures.”⁶³

133. Outside of HIPPA, the Office for Civil Rights warned that an impermissible disclosure of an individual’s PHI could result in a wide range of additional harms to the individual or others.⁶⁴ “For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or others identified in the individual’s PHI.”⁶⁵

134. The Office for Civil Rights noted the broad range of information that constitutes PHI, including “individually identifiable health information” (“IIHI”) such as “an individual’s medical record number, home or email address, or dates of appointments, as well as an individual’s IP address or geographic location, medical device IDs, or any unique identifying code.”⁶⁶ According to the Bulletin, IIHI can constitute PHI because:

when a regulated entity collects the individual’s IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual’s past, present, or future health or health care or payment for care.⁶⁷

⁶² *Id.* (emphasis in original).

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ *Id.*

135. The Office for Civil Rights concluded that “it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPPA Privacy Rule.”⁶⁸

136. As a result of Defendant’s conduct, as alleged herein, Plaintiffs and Class Members have been exposed to the harms and impending harms described in the Bulletin.

137. Moreover, “courts have recognized the ‘growing trend across courts . . . to recognize the lost property value’ of personal information. *In re Marriott Int’l, Inc., Cust. Data Sec. Breach Litig.*, 440 F.Supp.3d 447, 461 (D. Md. 2020) . . .; *see also In re Facebook Privacy Litigation*, 557 F.App’x. 494, 494 [sic] (9th Cir. 2014).” *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 636 (N.D. Cal. 2021).

CLASS ACTION ALLEGATIONS

138. Plaintiffs, pursuant to Rules 1702, 1708 and 1709 of the Pennsylvania Rules of Civil Procedure, assert this action individually and on behalf of the following Class: All natural persons in the Commonwealth of Pennsylvania who used the App and/or Website while it had third party tracking technology – including the tracking technology of Facebook, Google, LinkedIn, TikTok and Snap – embedded, installed and/or integrated therein.

139. Plaintiffs reserve the right to amend or modify the Class definition with greater specificity or division and/or to add subclasses after having had an opportunity to conduct discovery.

140. Excluded from the Class are: (a) Defendant; (b) any parent, affiliate or subsidiary of Defendant; (c) any entity in which Defendant has a controlling interest; (d) any of Defendant’s officers or directors; (e) any successor or assign of Defendant; (f) any judge or court personnel

⁶⁸ *Id.* (emphasis in original).

assigned to this case and members of their immediate families; and (g) Plaintiffs' counsel and Defendant's counsel and anyone employed by them.

141. **Numerosity.** Consistent with Pennsylvania Rule of Civil Procedure 1702(1), the Class is so numerous that joinder of all members is impracticable. While Plaintiffs do not know the exact number of members of the Class, Plaintiffs believe the Class contains at least hundreds of thousands of individuals, and the members can be identified through Defendant's records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media and/or published notice.

142. **Commonality.** Consistent with Pennsylvania Rule of Civil Procedure 1702(2), common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to the following:

- a. Whether Plaintiffs and Class Members had a reasonable expectation of privacy in their sensitive health information communicated to their healthcare providers;
- b. Whether Defendant violated Plaintiffs' and Class Members' privacy rights;
- c. Whether Defendant intentionally tapped the lines of internet communication between Plaintiffs and Class Members and their medical providers;
- d. Whether Penn Medicine's websites surreptitiously record personally identifiable information, protected health information and related communications and simultaneously, or subsequently, discloses that information to Facebook.
- e. Whether Facebook, Google, Snap, TikTok, or LinkedIn is a third-party eavesdropper;

- f. Whether Defendant's disclosure of personally identifiable information, protected health information and related communications constitutes an affirmative act of communication;
- g. Whether Defendant's actions violated the Pennsylvania Wiretapping Act; and
- h. Whether Plaintiffs' and Class Members are entitled to damages under the Pennsylvania Wiretapping Act.

143. **Typicality.** Consistent with Pennsylvania Rule of Civil Procedure 1702(3), Plaintiffs' claims are typical of the claims of the Class they seek to represent because Plaintiffs and all Class Members have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests to advance adverse to the interests of the other Class Members, and Defendant has no defenses unique to any Plaintiff.

144. **Adequate Representation.** Consistent with Pennsylvania Rule of Civil Procedure 1702(4) and 1709, Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Class and have retained as their counsel attorneys competent and experienced in class actions and complex litigation, including litigation to remedy privacy violations. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of Class Members, and they have the resources to do so.

145. **Predominance.** Consistent with Pennsylvania Rule of Civil Procedure 1708(a)(1), common questions of law and fact predominate over any questions affecting only individual class members. For example, Defendant's liability and the fact of damages is common to all members of the Class.

146. **Superiority and Manageability.** Consistent with Pennsylvania Rule of Civil Procedure 1708(a)(2), a class action is superior to other available means for the fair and efficient

adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, may not be of such magnitude as to make the prosecution of individual actions against Defendant economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer management difficulties and provides the benefit of single adjudication, economy of scale and comprehensive supervision by a single court.

147. **Risk of Inconsistent, Varying, or Prejudicial Adjudications.** Consistent with Pennsylvania Rule of Civil Procedure 1708(a)(3), a class action will minimize the risk of inconsistent, varying or prejudicial adjudications. If Plaintiffs' and Class Members' claims were tried separately, Defendant would be confronted with incompatible standards of conduct and divergent court decisions.

148. **Litigation Already Commenced.** Consistent with Pennsylvania Rule of Civil Procedure 1708(a)(4), to Plaintiffs' knowledge, there are no other cases that have been brought against Defendant, or that are currently pending against Defendant, where Pennsylvania consumers seek to represent a class of Pennsylvania residents based on conduct alleged in this First Amended Class Action Complaint.

149. **Appropriateness of Forum.** Consistent with Pennsylvania Rule of Civil Procedure 1708(a)(5), the most appropriate forum to concentrate the litigation is this County because Defendant is headquartered in this County and a substantial number of Class Members were injured in this County.

150. **Support for Class Certification.** Consistent with Pennsylvania Rule of Civil Procedure 1708(a)(6) and (7), there is support for a class to be certified because of the relatively low amount recoverable by each Class member and the expenses of individual litigation.

151. **The General Applicability of Defendant's Conduct.** Consistent with Pennsylvania Rule of Civil Procedure 1708(b)(2), Defendant's conduct is generally applicable to the class as a whole, making relief appropriate with respect to each Class member.

CLAIMS FOR RELIEF

COUNT I

Violation of the Pennsylvania Wiretapping Act 18 Pa. Cons. Stat. § 5701, *et seq.*

152. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

153. Plaintiffs bring this Count individually and on behalf of the members of the Class.

154. The Pennsylvania Wiretapping Act prohibits: (a) the interception or procurement of another to intercept any wire, electronic, or oral communication; (b) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (c) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

155. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at a rate

of \$100 per day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

156. At all relevant times, Defendant procured third parties, including Facebook, Google, LinkedIn, TikTok and Snap to track and intercept Plaintiffs' and Class Members' internet communications while navigating Defendant's App and/or Website. The third parties intercepted the communications without authorization and consent from Plaintiffs and Class Members.

157. Defendant, when procuring third parties, including Facebook, Google, LinkedIn, TikTok and Snap, to intercept Plaintiffs' communications, intended the third parties to learn the meaning of the content the visitor requested.

158. Plaintiffs and Class Members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

159. Plaintiffs and Class Members were not aware that their electronic communications were being intercepted by third parties, including Facebook, Google, LinkedIn, TikTok and Snap.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- a. Determining that this action is a proper class action;
- b. For an order certifying the Class, naming Plaintiffs as representatives of the Class, and naming Plaintiffs' attorneys as Class Counsel to represent the Class;
- c. For an order declaring that Defendant's conduct violates the statute referenced herein;
- d. For an order finding in favor of Plaintiffs and the Class on the count asserted herein;

- e. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;
- f. For punitive damages, as warranted, in an amount to be determined at trial;
- g. Ordering Defendant to disgorge revenues and profits wrongfully obtained;
- h. For prejudgment interest on all amounts awarded;
- i. For injunctive relief as pleaded or as the Court may deem proper;
- j. For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit; and
- k. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all claims so triable in this action.

Dated: June 3, 2025

Respectfully submitted,

/s/ Steven A. Schwartz

**CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP**

Steven A. Schwartz (PA I.D. No. 50579)

361 W. Lancaster Avenue

Haverford, PA 19041

Tel: (610) 642-8500

Fax: (610) 649-3633

E-Mail: sas@chimicles.com

BURSOR & FISHER, P.A.

Philip L. Fraietta (*pro hac vice*)

Alec M. Leslie (*pro hac vice*)

1330 Avenue of the Americas

New York, NY 10019

Tel: (646) 837-7150

Fax: (212) 989-9163

E-Mail: pfraietta@bursor.com

aleslie@bursor.com

DRURY LEGAL, LLC

Scott R. Drury*

6 Carriage Lane

Highwood, Illinois 60040

Telephone: (312) 358-8225

E-Mail: scott@drurylegal.com

Attorneys for Plaintiffs and the Putative Class