IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

MYSCHELLE TAYLOR and MUHAMMAD UDDIN, individually, and on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

TELADOC HEALTH, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL REQUESTED

Plaintiffs Myschelle Taylor and Muhammad Uddin ("Plaintiffs") bring this class action complaint on behalf of themselves, and all others similarly situated against Defendant Teladoc Health, Inc. ("Teladoc" or "Defendant"). The allegations contained in this class action complaint are based on Plaintiffs' personal knowledge of facts pertaining to themselves and upon information and belief, including further investigation conducted by Plaintiffs' counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought to address Defendant's improper and illegal disclosure of consumers' personally identifiable information ("PII") and/or protected health information ("PHI") (collectively referred to as "Private Information") to Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta") and other third parties as a result of consumers' use of Defendant's website, www.teladochealth.com ("Website").

2. Information about a person's physical, mental, and financial health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences, including discrimination in the workplace or denial of insurance coverage.

3. Defendant owns and controls www.teladochealth.com. Defendant intentionally installed a tracking pixel (the "Facebook Tracking Pixel" or "Pixel") on its website to surreptitiously duplicate and send its customers' private communications to Facebook, the contents of which include Private Information and protected PHI/individually identifiable medical information.

4. By installing, programming, and controlling the Pixel as described herein, Defendant aided, agreed, employed, and conspired with Facebook to intercept Plaintiffs' and Class members' sensitive and private communications without their knowledge or consent.

5. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[1] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

6. The Pixel is programmable, meaning that the Defendant is responsible for determining which communications with the Website are tracked and transmitted to Facebook.

7. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data for marketing and retargeting purposes in an effort to bolster its profits.

8. Correspondingly, Defendant exploits the Private Information Plaintiffs and Class members communicated to Defendant while using its telehealth services and uses this Private

[1] *Retargeting: How to Advertise to Existing Customers with Ads on Facebook*, Facebook, https://www.facebook.com/business/goals/retargeting (last visited Feb. 17, 2023).

Information to create detailed profiles that reflect individual consumer preferences, allowing Facebook and Defendant to deliver targeted advertisements.

9. Defendant's website, and more specifically its source code, manipulated Plaintiffs' and Class members' web browsers so that their communications to Defendant were automatically, contemporaneously, jointly, and surreptitiously sent to Facebook—an unintended third-party recipient.

10. This is the functional equivalent of placing a bug or listening device on a phone line because Defendant's website allows third-parties to "listen in" and receive communications in real time that Plaintiffs intended only for Defendant.

11. Importantly, Facebook would not receive these communications but for Defendant's installation and implementation of the Pixel.

12. In addition to the Facebook Pixel, Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("Conversions API" or "CAPI") on its website servers.[2]

13. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, Conversions API does not cause the user's browser to transmit information directly to Facebook. Instead, Conversions API tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the

[2] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See How to Implement Facebook Conversations API*, Fetch & Funnel, https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited: January 25, 2023).

website owner's servers.[3,4] Indeed, Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[5]

14. Because Conversions API is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

JURISDICTION AND VENUE

15. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendant. The Court also has subject-matter jurisdiction over this matter pursuant to 28 U.S.C. § 1331, as Plaintiffs bring a claim under the federal Electronic Communications Privacy Act ("ECPA"), 18, U.S.C. § 2510, *et seq.* 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.

[3] *What is Facebook Conversations API and How to Use It*, RevealBot, https://revealbot.com/blog/facebook-conversions-api/ (last visited: January 24, 2023).

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

[5] *About Conversations API*, Facebook, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited: January 28, 2023).

16. This Court has personal jurisdiction over Defendant because Defendant is headquartered and maintains its principal place of business in Purchase, New York, within this District.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the acts and omissions giving rise to Plaintiffs' and Class members' claims occurred in this District.

THE PARTIES

Plaintiff Myschelle Taylor

18. Plaintiff Taylor is an adult citizen of the state of Georgia and resides in the city of Hampton.

19. On February 11, 2021, Plaintiff Taylor signed up for a Teladoc account. As part of the registration process, Plaintiff Taylor provided Teladoc with her PII and health information, including her medical history and medical insurance information. Plaintiff Taylor reasonably expected that her communications with Teladoc via its website were confidential, solely between herself and Teladoc, and that such communications would not be transmitted to or intercepted by a third party.

20. Plaintiff Taylor made continuous use of Teladoc's telehealth services to the present day and accessed the platform from her computers and mobile devices.

21. Plaintiff Taylor also has an active Facebook account she regularly accesses using her mobile device and personal computer. As described herein, Teladoc sent Plaintiff Taylor's sensitive and private PII and health information to third parties, including Facebook, when she accessed Teladoc's website. Additionally, the information Teladoc sent to third parties was linked to Plaintiff Taylor's Facebook ID.

22. Pursuant to the systematic process described herein, Teladoc assisted third parties, including Facebook, with intercepting Plaintiff Taylor's communications, including those that contained PII, protected health information, and related confidential information. Teladoc assisted these interceptions without Plaintiff Taylor's knowledge, consent, or express written authorization.

23. By failing to receive the requisite consent, Teladoc breached confidentiality and unlawfully disclosed Plaintiff Taylor's personal, private, and personally identifiable information and protected health information.

Plaintiff Muhammad Uddin

24. Plaintiff Uddin is an adult citizen of the state of Texas and resides in the city of Dallas.

25. In and around June or July of 2017, Plaintiff Uddin signed up for Teladoc through a health plan provided by his employer. As part of the registration process, Plaintiff Uddin provided Teladoc with his PII and health information, including his medical history and medical insurance information. Plaintiff Uddin reasonably expected that his communications with Teladoc via its Website were confidential, were between solely himself and Teladoc, and would not be transmitted to or intercepted by a third party.

26. Plaintiff Uddin accessed Teladoc from his computer and mobile devices and he made extensive use of Teladoc's services until fall 2023, when he stopped utilizing the service.

27. Plaintiff Uddin also has an active Facebook account he regularly accesses using his mobile devices and personal computers. As described herein, Teladoc sent Plaintiff Uddin's sensitive and private PII and health information to third parties, including Facebook, when he

accessed Teladoc's website. Additionally, the information Teladoc sent to third parties was linked to Plaintiff Uddin's Facebook ID.

28. Pursuant to the systematic process described herein, Teladoc assisted third parties, including Facebook, with intercepting Plaintiff Uddin's communications, including those that contained PII, protected health information, and related confidential information. Teladoc assisted these interceptions without Plaintiff Uddin's knowledge, consent, or express written authorization.

29. By failing to receive the requisite consent, Teladoc breached confidentiality and unlawfully disclosed Plaintiffs' personal, private, and personally identifiable information and protected health information.

Defendant Teladoc

30. Defendant Teladoc Health, Inc., is a Delaware corporation with its principal place of business at 2 Manhattanville Road, Purchase, NY 10577.

31. Teladoc Health is a virtual healthcare company. Using its website or mobile application, Teladoc's users can virtually/remotely connect with healthcare service providers. Teladoc has been in continuous operation since 2002 and it operates across 130 countries.

FACTUAL ALLEGATIONS

A. Defendant's Website and The Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiffs' and Class members' Private Information to Facebook.

32. Defendant's Website, www.teladochealth.com, is accessible on mobile devices and computers and provides telehealth services, in large part based on the consumers' personal information and medical information.

33. In order to use Defendant's online services, customers must provide Defendant, at a minimum, the following information:

a. consumers' names, Social Security numbers, and dates of birth;

b. email addresses, residential addresses, and phone numbers;

c. gender and age;

d. health conditions;

e. health insurance information; and

f. medical diagnoses and treatment information.

34. As a result, consumers communicate Private Information via the Website, including private and confidential information regarding their health.

35. Defendant purposely installed the Pixel on its Website and programmed specific webpage(s) to surreptitiously share its users' private and protected communications with Facebook, including Plaintiffs' and Class members' Private Information.

36. The Pixel tracks users as they navigate through the Website and simultaneously transmits to Facebook each users' communications including which pages are visited, which buttons are clicked, and other information including a user's IP address.[6] An IP address is a unique number assigned to an internet-enabled device that informs websites of the device's city, zip code, and physical location.

37. As a result, consumers communicate Private Information via the Website, including private and confidential information regarding their physical and financial health.

38. Notably, while consumers are filling out online forms and selecting options on Teladoc's Website, and supplying the information described above, Teladoc, without the consumers' knowledge or consent, supplies the private and confidential information to non-party Facebook.

[6] *Meta Pixel*, Facebook, https://developers.facebook.com/docs/meta-pixel/

39. If the consumer is also a Facebook user, the information Facebook receives is linked to the user's Facebook profile (via their Facebook ID or "c_user id"), which includes other identifying information.

40. As explained herein, this information is collected not just by Teladoc but also by Facebook because the embedded Pixel simultaneously transmits all the information Teladoc receives, sending it to Facebook. If the consumer is also a Facebook user, Facebook in turn links the information they receive to the visitor's Facebook profile, which includes other identifying information.

41. Plaintiffs and Class members did not and could not anticipate that Defendant would aid and conspire with Facebook to intercept and transmit their communications.

42. And consumers who signed up for Teladoc and provided their private, personal and medical information were not notified that their online communications will be shared with third parties and did not consent to such.

1. Facebook's Business Tools and the Pixel

43. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[7]

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

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

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

46. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[8] Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[9]

47. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[10] When a user accesses webpage(s) hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers. Notably, this transmission does not occur unless the webpage contains the Pixel. Stated differently, each Plaintiffs' and Class member's Private Information would not have been disclosed to Facebook but for the Defendant's decisions to install the Pixel on its Website.

48. As explained in more detail below, this second simultaneous secret transmission is initiated by Defendant's source code concurrently with Plaintiffs' and Class members' communications to their intended recipient, Defendant.

[8] *SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Nov. 14, 2022); *see also FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED*, FACEBOOK, https://developers.facebook.com/docs/facebook-pixel/advanced/; *BEST PRACTICES FOR FACEBOOK PIXEL SETUP*, FACEBOOK, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov. 14, 2022).

[9] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBPAGE(S) 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/. (last visited Nov. 14, 2022)

[10] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

49. An example illustrates the point: An individual navigates to Teladoc's Website and clicks a webpage link to sign up for a Teladoc account. When the link is clicked, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. Because Teladoc utilizes the Facebook 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 duplicate the communication with Teladoc, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

2. Defendant's Pixel, Source Code, and Interception of HTTP Requests

50. Web browsers are software applications that allow consumers to navigate the web and exchange electronic communications over the internet, and every "client device" (computer, tablet, or smart phone) has a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

51. Correspondingly, every website is hosted by a computer "server" which allows the website's owner (Defendant) to exchange communications with the website's visitors (Plaintiffs and Class members) via the visitors' web browser.

52. When a consumer uses Defendant's Website and undertakes various actions, the consumer and Defendant are engaged in an ongoing back-and-forth exchange of electronic communications taking place via the consumer's web browser and Defendant's computer server.

53. These communications are invisible to ordinary consumers because they consist of HTTP Requests and HTTP Responses, and one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.[11]

- **HTTP Request:** an electronic communication sent from the website visitor's browser to the website's corresponding server. In addition to specifying a particular URL (*i.e.*, web address), "GET" HTTP Requests can also send data to the host server, including cookies. A cookie is a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response:** an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

54. A consumer's HTTP Request essentially asks the Defendant's Website to retrieve certain information, and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the user's screen as they navigate Defendant's Website).

55. Every webpage is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

[11] *See* HHS Bulletin § *What is a tracking technology?* ("Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user.")

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

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

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

communications directly from Defendant to Facebook. User devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

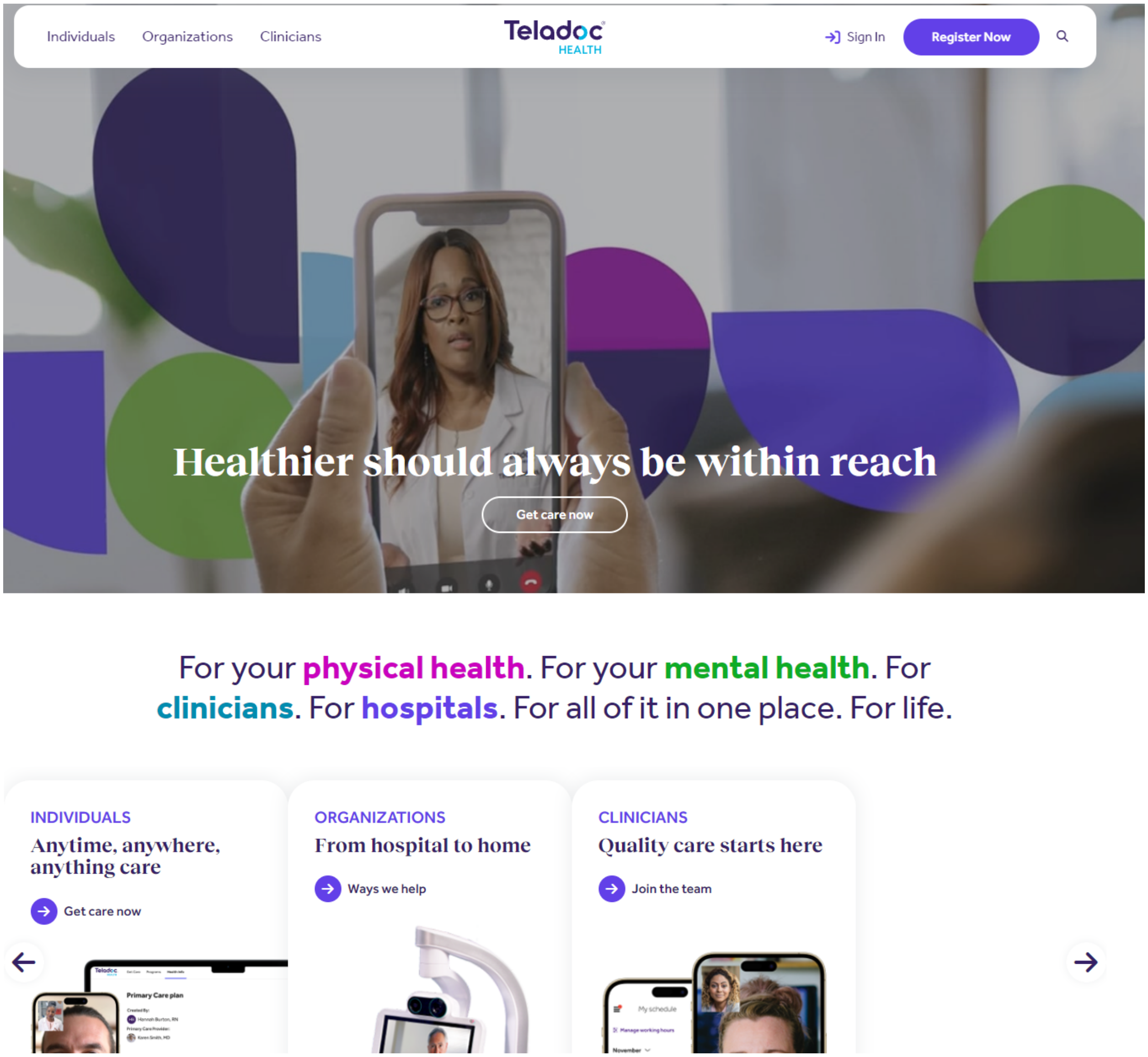
59. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose." Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

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

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

62. In this case, Defendant employed the Tracking Pixel and Conversions API to intercept, duplicate, and re-direct Plaintiffs' and Class members' Private Information to Facebook.

63. For example, when a user visits www.teladochealth.com, and clicks the "Register Now" link, the user's web browser automatically sends an HTTP Request to Defendant's web server. The Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted in the image below.



Healthier should always be within reach

For your **physical health**. For your **mental health**. For **clinicians**. For **hospitals**. For all of it in one place. For life.

INDIVIDUALS

Anytime, anywhere, anything care

Get care now

ORGANIZATIONS

From hospital to home

Ways we help

CLINICIANS

Quality care starts here

Join the team

Figure 1. A consumer starts the process by clicking the "Register Now" button.

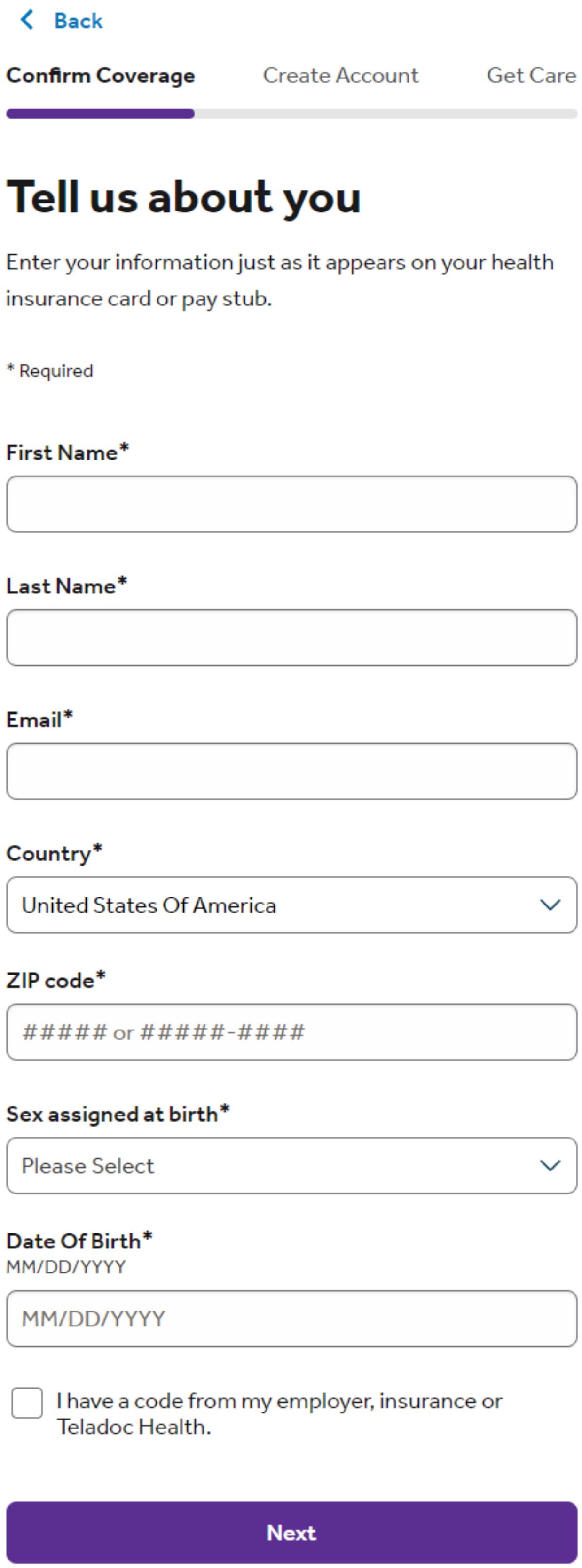
64. The image above represents the Markup for this particular webpage, and it is the only thing the user sees or is aware of when they view and interact with this particular webpage. The user does not see the Defendant's Source Code or any HTTP Requests sent in the "background" while the webpage is operating. In fact, this unseen Source Code manipulated users' browsers by secretly including Pixel code in the webpage's Source Code, which was programmed to silently monitor and report the user's activity. When the webpage loads into the user's browser,

the Pixel code is triggered which sends an HTTP Request to Facebook including the user's c_user id and the URL, informing Facebook that the user is seeking telehealth services.

65. Thereafter, when an event triggers the Pixel code, the code instructs the web browser to duplicate user communications (HTTP Requests) intended for Defendant and to send those communications to Facebook at the same time they are sent to Defendant. This occurs because the Pixel that was embedded in Defendant's Source Code is programmed to automatically track and transmit a user's communications, and this occurs contemporaneously, invisibly, and without the user's knowledge.

66. The images below demonstrate how communications between consumers and Teladoc are collected and sent to third parties, such as Facebook. In Figure 1, above, a consumer visits Teladoc's website and selects the "Register Now" button.

67. Figure 2, below, demonstrates that after selecting the "Register Now" button, users are required to answer multiple questions about their personal, medical, and financial condition.



Tell us about you

Enter your information just as it appears on your health insurance card or pay stub.

* Required

First Name*

Last Name*

Email*

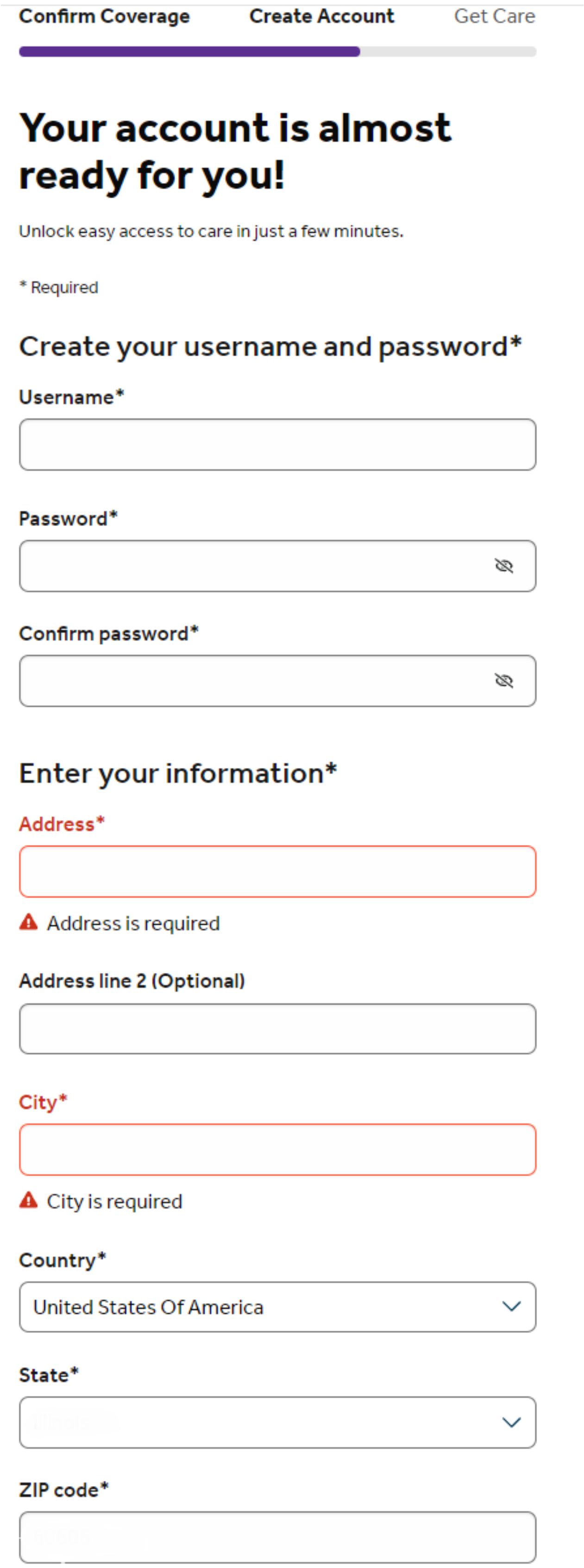
Country*
United States Of America

ZIP code*
or #####-####

Sex assigned at birth*
Please Select

Date Of Birth*
MM/DD/YYYY
MM/DD/YYYY

□ I have a code from my employer, insurance or Teladoc Health.



Your account is almost ready for you!

Unlock easy access to care in just a few minutes.

* Required

Create your username and password*

Username*

Password*

Confirm password*

Enter your information*

Address*

Address is required

Address line 2 (Optional)

City*

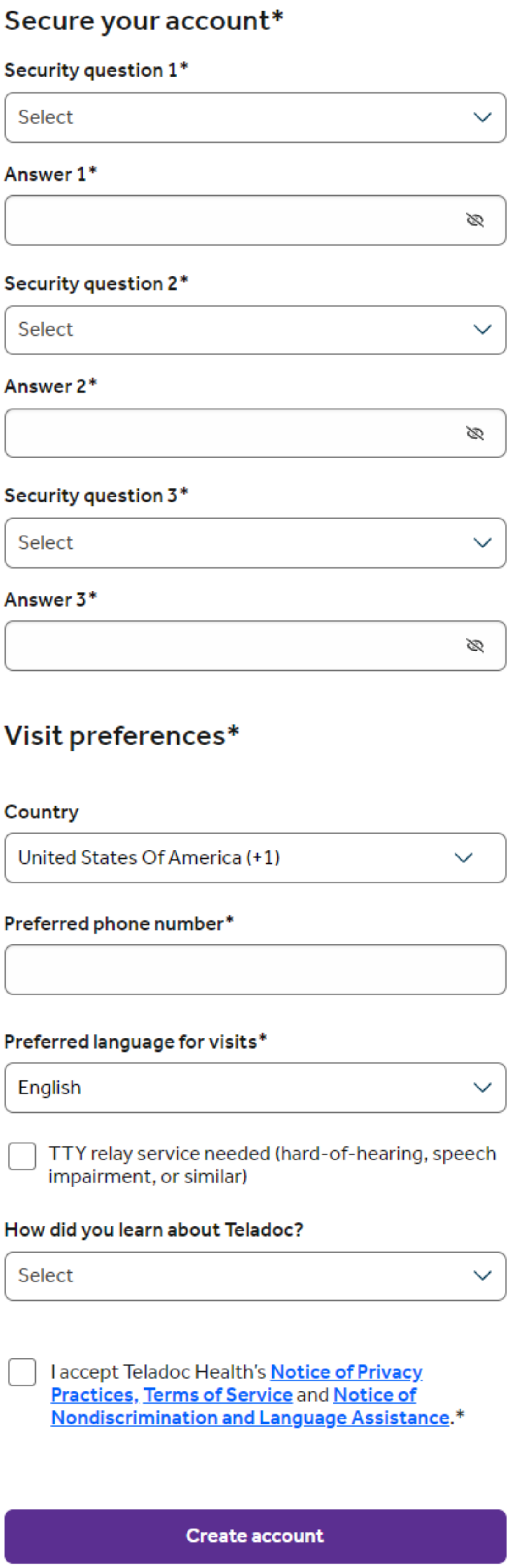
City is required

Country*

United States Of America

State*

ZIP code*



Secure your account*

Security question 1*

Select

Answer 1*

Security question 2*

Select

Answer 2*

Security question 3*

Select

Answer 3*

Visit preferences*

Country

United States Of America (+1)

Preferred phone number*

Preferred language for visits*

English

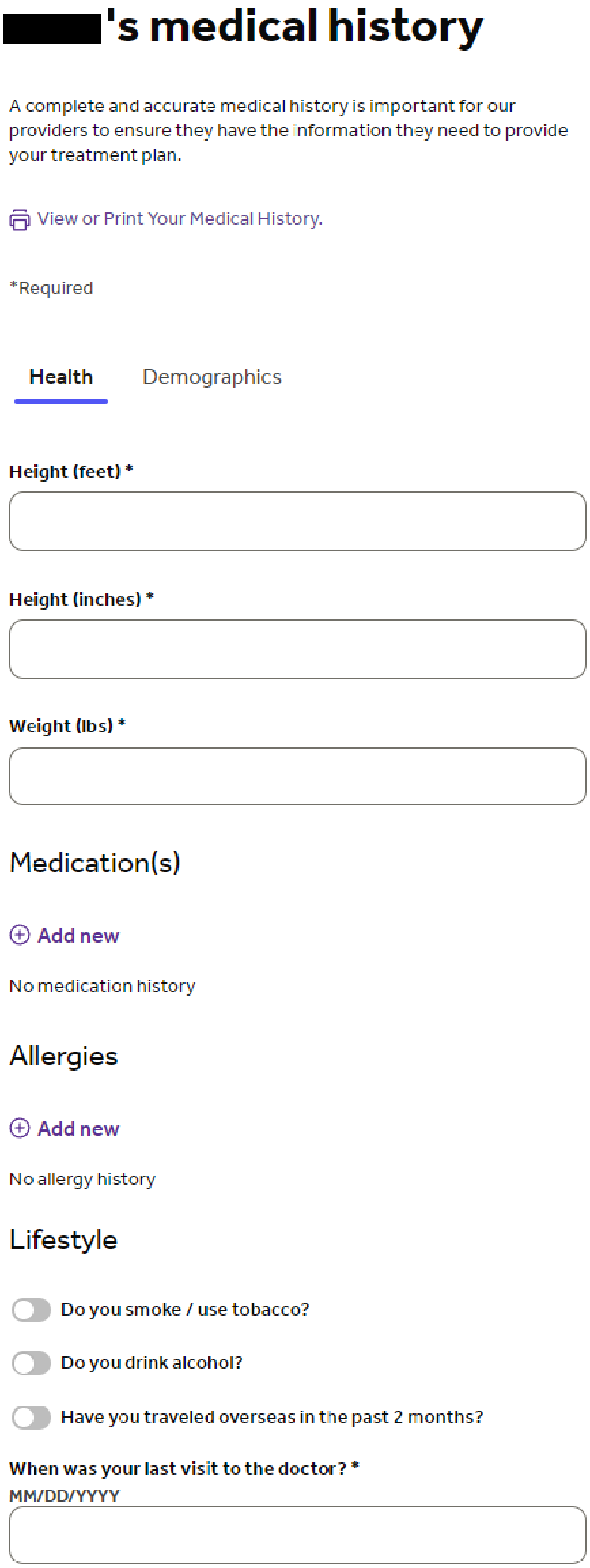
□ TTY relay service needed (hard-of-hearing, speech impairment, or similar)

How did you learn about Teladoc?

Select

□ I accept Teladoc Health's Notice of Privacy Practices, Terms of Service and Notice of Nondiscrimination and Language Assistance.*

Create account



[redacted]'s medical history

A complete and accurate medical history is important for our providers to ensure they have the information they need to provide your treatment plan.

View or Print Your Medical History.

*Required

Health Demographics

Height (feet) *

Height (inches) *

Weight (lbs) *

Medication(s)

⊕ Add new

No medication history

Allergies

⊕ Add new

No allergy history

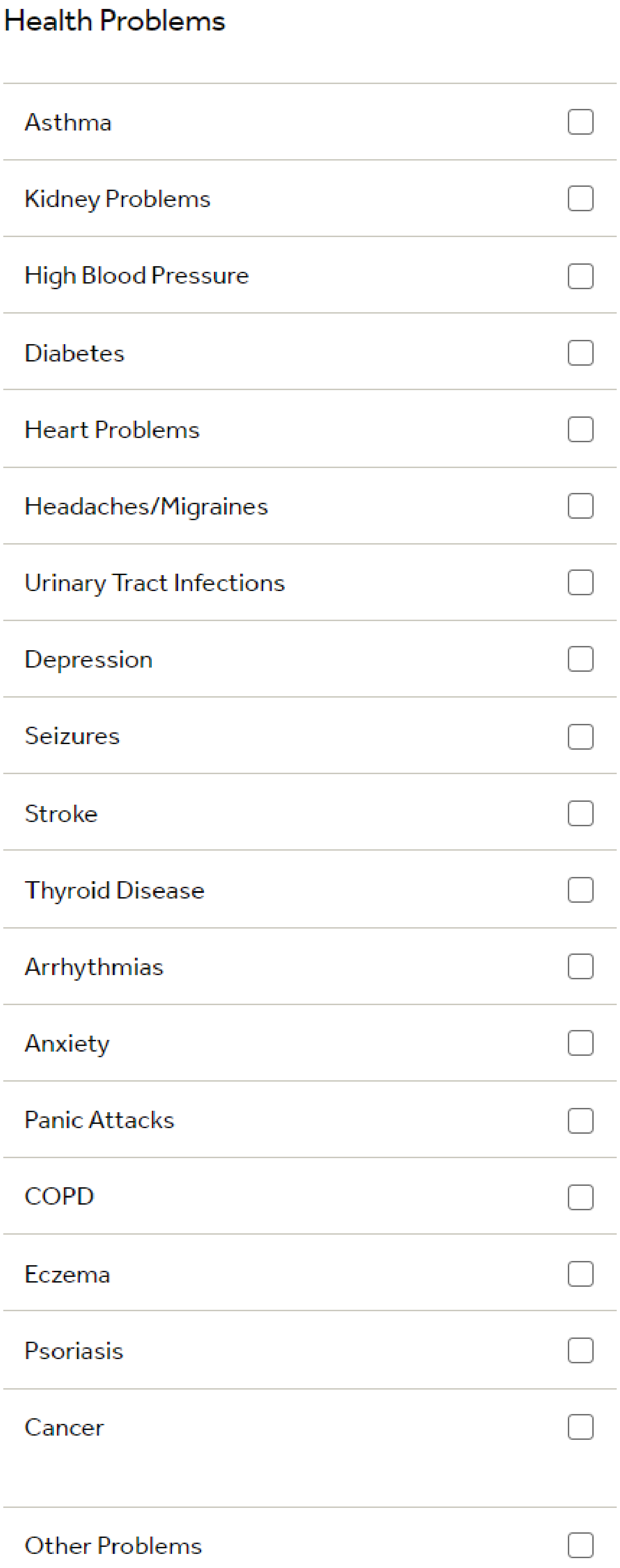
Lifestyle

○ Do you smoke / use tobacco?

○ Do you drink alcohol?

○ Have you traveled overseas in the past 2 months?

When was your last visit to the doctor? *
MM/DD/YYYY



Health Problems

Asthma ☐

Kidney Problems ☐

High Blood Pressure ☐

Diabetes ☐

Heart Problems ☐

Headaches/Migraines ☐

Urinary Tract Infections ☐

Depression ☐

Seizures ☐

Stroke ☐

Thyroid Disease ☐

Arrhythmias ☐

Anxiety ☐

Panic Attacks ☐

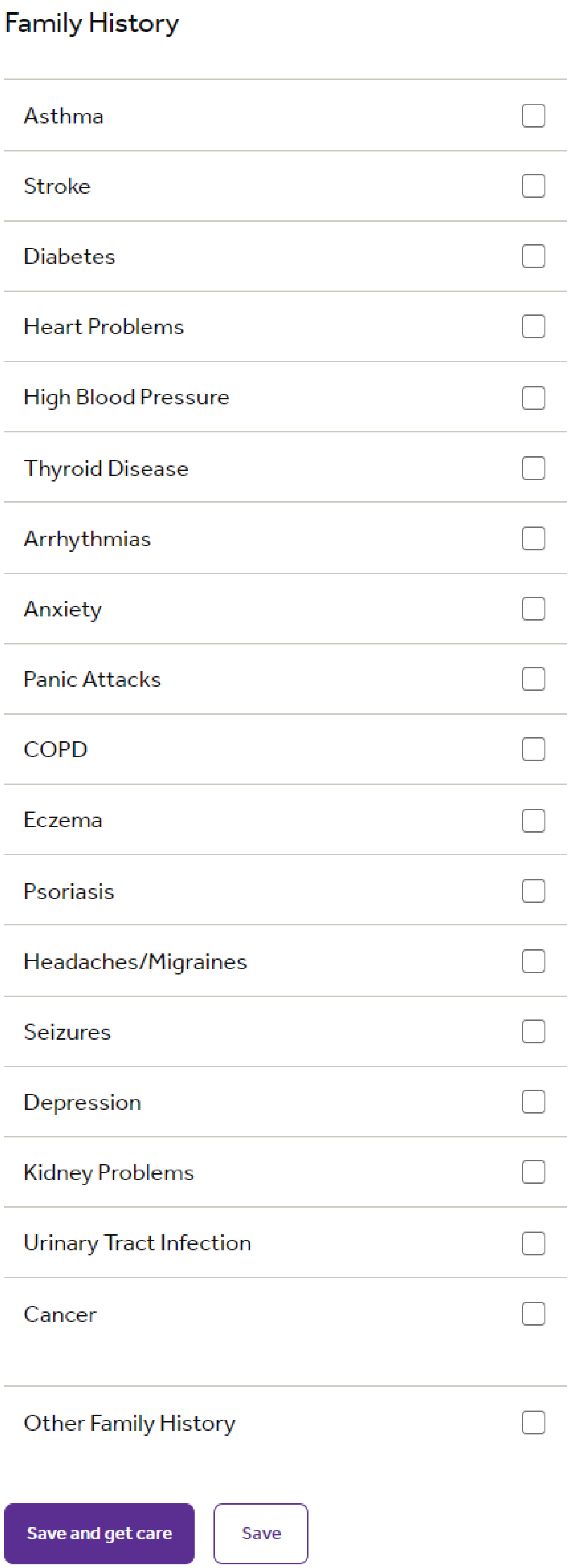
COPD ☐

Eczema ☐

Psoriasis ☐

Cancer ☐

Other Problems ☐



Family History

Asthma □

Stroke □

Diabetes □

Heart Problems □

High Blood Pressure □

Thyroid Disease □

Arrhythmias □

Anxiety □

Panic Attacks □

COPD □

Eczema □

Psoriasis □

Headaches/Migraines □

Seizures □

Depression □

Kidney Problems □

Urinary Tract Infection □

Cancer □

Other Family History □

Figure 2. Consumers are required to answer questions regarding their personal information.

68. Once consumers submit their answers to the questions exemplified above (and other questions), their answers containing Private Information are automatically sent to Facebook.

69. For instance, any information clicked by a consumer on Defendant's Website would be contemporaneously shared with Facebook as that information was being sent to Defendant's servers.

70. At the same time, Conversions API causes the user's communications to be sent to and stored on Defendant's servers, to be later communicated to Facebook from Defendant itself rather than from a Website user's web browser.[12]

71. Thus, without its users' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" its users' computing devices, allowing Facebook and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

72. Consequently, when Plaintiffs and Class members visit Defendant's website and communicate their Private Information, including, but not limited to, button clicks and page visits, that Private Information also is transmitted to Facebook.

3. Users Do Not Provide Informed Consent Before Their Information is Collected and Intercepted.

73. Defendant did not ask users, including Plaintiffs, whether they consent to be wiretapped via the Pixel or to external sharing of their Private Information prior to submitting their Personal Information to Defendant. Users are never told that their electronic communications are being wiretapped via the Pixel.

[12] Facebook has tools to de-duplicate communications sent by the Pixel and Conversions API so that only one copy of any particular communication is sent to it.

74. Defendant's written policies did not adequately disclose the wiretapping.

75. While Teladoc does require users to affirm their acceptance to Teladoc's "Notice of Privacy Practices" these policies do not disclose that Teladoc engages in such extensive sharing of information with third parties, such as Meta/Facebook. The only statement on Teladoc's Notice of Privacy Practices regarding its information sharing practices with third parties is as follows:

> Engage third parties to assist Teladoc Health with our payment and healthcare operations. If any such third party needs access to PHI to perform its services on behalf of Teladoc Health, Teladoc Health will require that third party to enter a written agreement that protects the PHI. We provide only the minimal PHI to accomplish the intended purpose of the use and sharing of the PHI.[13]

This statement would not indicate to reasonable consumers that Teladoc transmits all information provided directly to Meta.

76. As such, users who fill out the questionnaires on Teladoc's website and provide their personally identifiable information, private communications, and protected health information are not informed that Teladoc will track and share their private information and communications with third parties. And users, like Plaintiffs, never agree or are never given the option to agree to any such Privacy Policy when using the website.

77. Furthermore, Teladoc does not provide a link to its Notice of Privacy practices nor require assent until *after* the prospective user has already entered their full name, email, date of birth, sex, email, and country of residence. Thus, these categories of information are transmitted to Meta/Facebook prior to even any attempt at acquiring user consent.

[13] https://www.teladoc.com/notice-of-privacy-practices/ (last upd. February 15, 2023).

4. Plaintiffs' and Class members' Private Communications to Defendant were Linked to their Individual Facebook Profiles and Unique Identifiers.

78. The information that Defendant's Pixel sent to Facebook was transmitted alongside other information that reveals a particular user's identity.

79. Every Facebook user has a unique and persistent Facebook ID ("FID") that is associated with their Facebook profile and individual account, and Facebook places a cookie containing the user's FID ("c_user" cookie) on their device when they log into Facebook. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its 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, ordinary persons who come into possession of the FID can connect it to the corresponding Facebook profile.

80. The FID is categorized as a third-party cookie, and it identifies a particular person and their actions or communications with a website, such as Defendant's Website, if, and only if, the owner of that website has installed the Facebook Pixel.

81. Facebook provides the Pixel code to companies to embed on their own websites, and upon doing so, the Pixel causes the website to operate much like a traditional wiretap that begins "listening in" as soon as the website loads.

82. Thus, the Pixel was triggered each time Plaintiffs and Class members communicated with Defendant via www.Teladoc.com (in the form of HTTP Requests to Defendant's web server). Upon triggering of the Pixel, the Website user's communications were intercepted, duplicated, and secretly transmitted to Facebook at the same time the message is dispatched to Defendant. Thus, two communications originate from a user's browser once the user initiates an action on the webpage: one, as intended, to Defendant, and a second, undetectable to

the user, is simultaneously sent to Facebook. Accordingly, at the same time the user's browser dispatches a GET Request to Defendant, it sends a duplicate to Facebook.

83. Plaintiffs and Class members were unaware this was happening, and Defendant did not inform them that Private Information communicated via Defendant's Website would be shared with Facebook or other third-parties.

84. Teladoc does not share anonymized data with third parties, but instead shares Private Information tied to unique identifiers that are tied to the specific user.

85. Teladoc does not disclose to visitors to its website that it shares their Private Information and related communications with Facebook, or any other third party.

86. Teladoc benefits from the unauthorized sharing with third parties of Plaintiffs' and Class members' personal information, health related information, and private communications. By using the software development kits ("SDK") from Facebook, and providing Plaintiffs' and Class members' personal and private information and communications to Facebook, Teladoc improves its advertising abilities, and benefits financially from advertising its services through third parties.

B. Facebook Exploited and Used Plaintiffs' and Class members' Private Information

87. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"[14] and Facebook has built its more-than $300 billion market capitalization on mining and using that "digital" oil. Thus, the large volumes of personal and sensitive health-related data Defendant provides to Facebook are actively examined, curated, and put to use by Facebook. Facebook acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform

[14] *Data is the New Oil of the Digital Economy*, Wired, https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited Jan. 18, 2023).

it into gasoline. Indeed, Facebook offers the Pixel free of charge[15] and the price that Defendant pays for the Pixel is the data that it allows Facebook to collect.

88. Facebook describes itself as a "real identity platform,"[16] meaning users are allowed only one account and must share "the name they go by in everyday life."[17] To that end, when creating an account, users must provide their first and last name, date of birth, and gender.[18]

89. Facebook sells advertising space by emphasizing its ability to target users.[19] Facebook is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant).[20] This allows Facebook to make inferences about users beyond what they explicitly disclose, including their "interests," "behavior," and "connections."[21] 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.[22]

90. Advertisers can also build "Custom Audiences,"[23] which helps them reach "people who have already shown interest in [their] business, whether they're loyal customers or people

[15] *Facebook's Pixel: What it is and Why you Need it*, SEO Digital Group, https://seodigitalgroup.com/facebook-pixel/

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

[17] *COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY*, FACEBOOK, https://www.facebook.com/communitystandards/integrity_authenticity.

[18] *SIGN UP*, FACEBOOK, https://www.facebook.com/

[19] *WHY ADVERTISE ON FACEBOOK*, FACEBOOK, https://www.facebook.com/business/help/205029060038706.

[20] *ABOUT FACEBOOK PIXEL*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[21] *AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS*, FACEBOOK, https://www.facebook.com/business/ads/ad-targeting.

[22] *EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK*, FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

[23] *ABOUT CUSTOM AUDIENCES*, FACEBOOK, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

who have used [their] app or visited [their] website."[24] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[25] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Facebook. This data can be supplied to Facebook by manually uploading contact information for customers or by utilizing Facebook's "Business Tools."[26]

91. The Facebook Pixel, and the personal data mined and curated with it, is key to this business. 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."[27]

92. Facebook does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever accessing the information. Instead, in accordance with the purpose of the Pixel to allow Facebook to create Core, Custom, and Lookalike Audiences for advertising and marketing purposes, Facebook viewed, processed, and analyzed Plaintiffs' and Class members' confidential Private Information. Upon information and belief, such viewing,

[24] *AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS*, FACEBOOK, https://www.facebook.com/business/ads/ad-targeting.
[25] *About Lookalike Audiences*, Facebook, https://www.facebook.com/business/help/164749007013531?id=401668390442328.
[26] *CREATE A CUSTOMER LIST CUSTOM AUDIENCE*, FACEBOOK, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; *Create a Website Custom Audience*, Facebook, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.
[27] *THE FACEBOOK BUSINESS TOOLS*, FACEBOOK, https://www.facebook.com/help/331509497253087.

processing, and analyzing was performed by computers and/or algorithms programmed and designed by Facebook employees at the direction and behest of Facebook.

93. Facebook receives over 4 petabytes of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data to augment human effort.[28] This process is known as data ingestion and allows "businesses to manage and make sense of large amounts of data."[29]

94. By using these tools, Facebook is able to rapidly translate the information it receives from the Pixel in order to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper's Facebook page.[30] This evidences that Facebook views and categorizes data as they are received from the Pixel.

95. Moreover, even if Facebook eventually deletes or anonymizes sensitive information that it receives, it must first view that information in order to identify it as containing sensitive information suitable for removal. Accordingly, there is a breach of confidentiality once the information is disclosed or received without authorization.

C. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures and Plaintiffs' and Class members' Private Information

96. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiffs' and Class members' Private Information was to commit tortious acts as

[28] Ankusha Sinha Roy, *How Does Facebook Handle the 4+ Petrabyte of Data Generated Per Day? Cambridge Analytica-Facebook Data Scandal*, Medium (Sept. 15, 2020), https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4

[29] Shivang, *Facebook Database [Updated] – A Thorough Insight Into the Databases Used @ Facebook, Scale Your App*, https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/

[30] David Vranlcar, *A Complete Guide to Facebook Tracking For Beginners*, Oberlo (Oct. 5, 2021), https://www.oberlo.com/blog/facebook-pixel

alleged herein, namely, the use of Private Information for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was an invasion of privacy.

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

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

99. Upon information and belief, Defendant was advertising its services on Facebook, and the Pixel was used to help Defendant understand the success of its advertisement efforts on Facebook. Defendant, in coordination with Facebook, associated Plaintiffs' and Class members' Personal Information with preexisting Facebook user profiles.

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

101. Defendant's disclosure of Private Information also injured Plaintiffs and the Class. 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.

102. The value of health data in particular is well-known, and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the

extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[31]

103. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[32]

104. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[33]

105. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

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

[32] *See* Christina Farr, *Hospital Execs Say they are Getting Flooded with Requests for your Health Data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited February 16, 2023).

[33] *How to Collect Emails Addresses on Twitter*, Vero (June 2014), available at https://www.getvero.com/resources/twitter-lead-generation-cards/.

106. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

107. Meta itself has paid users for their digital information, including browsing history. Until 2019, Meta ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

108. Additionally, healthcare data may be valued at up to $250 per record on the black market.[34]

TOLLING OF THE STATUTE OF LIMITATIONS AND DELAYED DISCOVERY

109. All applicable statute(s) of limitations have been tolled by the delayed discovery doctrine. Plaintiffs and Class members could not have reasonably discovered Facebook's practice of tracking and intercepting their activities and communications on Defendant's Website until this class action litigation commenced.

110. Plaintiffs did not learn of Facebook's intercepting their activities and communications on Defendant's Website until being informed by the undersigned counsel of record shortly before this complaint was filed.

111. Plaintiffs had no reason to believe their Private Information was being intercepted through Defendant's Website at all, let alone in real time while Plaintiffs were inputting information into Defendant's Website but before Plaintiffs submitted their application. As detailed above, Defendant's privacy policy did not disclose that Defendant was sharing their information

[34] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SecureLink (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

with Meta/Facebook. Furthermore, the technologies Defendant embedded on its Website are not visible to the reasonable user—they are invisible and work in the background.

112. As a result, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

CLASS ACTION ALLEGATIONS

113. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), the following classes:

> **Nationwide Class:** All persons in the United States who, during the class period, provided their personally identifiable information and/or health information to Teladoc using www.teladochealth.com (the "Class").

Excluded from the Class is Teladoc; any affiliate, parent, or subsidiary of Teladoc; any entity in which Teladoc has a controlling interest; any officer director, or employee of Teladoc; any successor or assign of Teladoc; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

114. Plaintiff Taylor also brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), the following subclass:

> **Georgia Subclass:** All persons in Georgia who, during the class period, provided their personally identifiable information and/or health information to Teladoc using www.teladochealth.com.

Excluded from the Subclass is Teladoc; any affiliate, parent, or subsidiary of Teladoc; any entity in which Teladoc has a controlling interest; any officer director, or employee of Teladoc; any successor or assign of Teladoc; anyone employed by counsel in this action; any judge to whom this case is assigned, her or her spouse and immediate family members; and members of the judge's staff.

115. Plaintiff Uddin also brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), the following subclass:

> **Texas Subclass:** All persons in Texas who, during the class period, provided their personally identifiable information and/or health information to Teladoc using www.teladochealth.com.

Excluded from the Subclass is Teladoc; any affiliate, parent, or subsidiary of Teladoc; any entity in which Teladoc has a controlling interest; any officer director, or employee of Teladoc; any successor or assign of Teladoc; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

116. This action is also brought on behalf of the following subclass:

> **New York Subclass:** All persons in New York who, during the class period, provided their personally identifiable information and/or health information to Teladoc using www.teladochealth.com.

Excluded from the Subclass is Teladoc; any affiliate, parent, or subsidiary of Teladoc; any entity in which Teladoc has a controlling interest; any officer director, or employee of Teladoc; any successor or assign of Teladoc; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

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

118. Plaintiffs reserve the right to modify the Class and/or Subclass definitions, or add additional sub-classes, as necessary prior to filing a motion for class certification, at class certification, or at any later time as the Court permits.

119. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class members is unknown to Plaintiffs at this time. However, it is estimated that there are hundreds of thousands of

individuals in the Class. The identity of such membership is readily ascertainable from Teladoc's records and non-parties' records.

120. Typicality. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs used www.teladochealth.com and had their Private Information disclosed to third parties without their express written authorization or knowledge. Plaintiffs' claims are based on the same legal theories as the claims of other Class members.

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

122. Common Questions of Law and Fact Predominate. Questions of law and fact common to the Class members predominate over questions that may affect only individual Class members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

a) Whether Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances;

b) Whether Defendant's Website surreptitiously records personally identifiable information, protected health information, financial information, and related communications and subsequently, or simultaneously, discloses that information to third parties;

c) Whether Defendant disseminated Class members' confidential communications to third parties;

d) Whether Teladoc's conduct resulted in a breach of confidentiality;

e) Whether Teladoc violated Plaintiffs' and Class members' privacy rights by using software to record and communicate website visitor's personally identifiable information, including unique identifies and FIDs, alongside confidential medical communications;

f) Whether Plaintiffs and Class members are entitled to damages under the ECPA, or any other relevant statute;

g) Whether Defendant's actions violate Plaintiffs' and Class members' privacy rights;

h) Whether Defendant's actions violated New York General Business Law § 349 by, *inter alia*, surreptitiously recording personally identifiable information, protected health information, financial information, and related communications and subsequently, or simultaneously, disclosing that information to third parties.

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

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Intrusion Upon Seclusion
(On Behalf of the Class)

124. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

125. Plaintiffs and Class members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communications platforms and services therein.

126. Plaintiffs and Class members communicated sensitive and protected medical information and personally identifiable information that they intended for only Defendant to receive and that they believed Defendant would keep private.

127. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class members is an intentional intrusion on Plaintiffs' and Class members' solitude or seclusion.

128. Plaintiffs and Class members had a reasonable expectation of privacy based on the sensitive nature of their communications. Plaintiffs and Class members have a general expectation that their communications regarding health and finances will be kept confidential. Defendant's disclosure of Private Information coupled with individually identifying information is highly offensive to the reasonable person.

129. As a result of Defendant's actions, Plaintiffs and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

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

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

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

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

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Class)

134. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

135. Plaintiffs and the Class provided Defendant with their Private Information.

136. By providing their Private Information and upon Defendant's acceptance of this information, Plaintiffs and the Class members (as one set of parties) and Defendant (as the other party) entered into implied-in-fact contracts to keep the provided information private and confidential.

137. This obligation was described in the terms that Defendant itself represented on its own Notice of Privacy Practices, which Defendant itself required Plaintiffs and Class members assent to prior to proceeding with registration. Therefore, Defendant expressly assented to this obligation in these implied contracts.

138. Defendant breached this obligation in the implied contracts by intercepting (or facilitating the interception of), disclosing, and sharing with third-parties the Private Information belonging to Plaintiffs and Class members without their consent.

139. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and the Class have been injured and damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to equitable relief and damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Class)

140. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

141. This Cause of Action is brought in the alternative to the Second Cause of Action – Breach of Implied Contract.

142. By intercepting (or facilitating the interception of), disclosing, and sharing with third-parties the Private Information belonging to Plaintiffs and Class members without their consent, Defendant benefitted (and/or was enriched) through, *inter alia*, receiving revenues from this conduct from parties that received and used this info such as Meta/Facebook.

143. This benefit was received at the expense of Plaintiffs and Class members since they suffered a gross violation of their privacy rights through the disclosure of such sensitive information.

144. This benefit was received at the expense of Plaintiffs and Class members since their Private Information has diminished in value because of this disclosure.

145. This benefit was received at the expense of Plaintiffs and Class members since they gave been placed at a greater risk of further exposure of Private Information, and are entitled to equitable relief and damages in an amount to be proven at trial.

146. It would be inequitable and unconscionable for Defendant to retain the profit, benefit, and other compensation it obtained from using Plaintiffs' and Class members' Private Information

147. Plaintiffs and the Class members seek an order from this Court creating a constructive trust requiring Defendant to provide restitution and disgorge all proceeds, profits, benefits, and other compensation obtained by Defendant from its improper and unlawful

interception (and facilitating interception), disclosure, and use of their Private Information for targeted advertising.

148. Plaintiffs and Class members seek this equitable remedy because their legal remedies are inadequate. 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.

FOURTH CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1)) ("ECPA")
(On Behalf of the Class)

149. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

150. The Electronic Communications Privacy Act ("ECPA"), 18, U.S.C. § 2510, *et seq.*, protects both the sending and receipt of communications.

151. The ECPA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted. 18 U.S.C. § 2520(a).

152. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

153. "Intercept" means "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." 18 U.S.C. § 2510(4).

154. "Electronic communication" means "any 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 that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

155. "Contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

156. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class members, in violation of 18 U.S.C. § 2511(1)(a). Whenever Plaintiffs and Class members interacted with Defendant's Website, Defendant, through the Pixel source code it embedded and ran on its Website, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiffs' and Class members' electronic communications without authorization or consent.

157. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class members to Facebook, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

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. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class members' Private Information for financial gain.

160. Defendant was not acting under color of law to intercept Plaintiffs' and the Class members' wire or electronic communication.

161. Plaintiffs and Class members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code.

162. Any purported consent that Defendant received from Plaintiffs and Class members was not valid.

163. 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. The ECPA provides that a "party to the communication" may 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).

164. Defendant is not a party to the communications, as its duplication and transmission of communications from Plaintiffs and Class members was unauthorized. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (an entity's simultaneous, unknown duplication and forwarding of GET requests made to a web page's server does not qualify for the party exemption, because holding otherwise "would render permissible the most common methods of intrusion, allowing the exception to swallow the rule"). However, even assuming Defendant is

a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class members' Private Information does not qualify for the party exemption.

165. 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 the Class members' communications about their Private Information on its Website, because it used its participation in these communications to improperly share Plaintiffs' and the Class members' information with Facebook, a third-party that did not participate in these communications, that Plaintiffs and the Class members did not know was receiving their Private Information, and that Plaintiffs and the Class members did not consent to receive this information.

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

FIFTH CAUSE OF ACTION
Violation of New York General Business Law § 349
(On Behalf of the Class, or, in the alternative, the New York Subclass)

167. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

168. Plaintiffs bring this action on behalf of the Class, or, in the alternative, the New York Subclass.

169. New York General Business Law § 349 broadly prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in this state.

170. Defendant engaged in (and continues to engage in) a deceptive (and/or prohibited) practice under Section 349 by intercepting (or facilitating the interception of), disclosing, and sharing with third-parties the Private Information belonging to Plaintiffs and Class members

without their consent in direct contravention of affirmative representations it made on its public Notice of Privacy Practices.

171. Defendant's actions as set forth above were consumer-oriented conduct occurred in the conduct of trade or commerce. Defendant published the Notice of Privacy Policy publicly on its Website. The Privacy Policy advises that Defendant will keep consumers' information and communications confidential and explain the extent of any disclosures.

172. The Privacy Policy was posted on the Website, the same location where consumers, including Plaintiffs and Class members, provide Defendant with their Private Information. Further, Defendant required all of its users to assent to the terms of the Notice of Privacy Practices as part of their sign-up process. As such, Defendant's representations in the Privacy Policy are directed at consumers.

173. Defendant's conduct renders its Notice of Privacy Practices deceptive and the representations contained therein regarding the confidentiality of user data false and misleading.

174. The facts Defendant misrepresented, and concealed or failed to disclose, to Plaintiffs and the Class are material in that a reasonable consumer would have considered them important in deciding whether to provide their Private Information to Defendant. This deception was material as the promise of confidentiality of data was a key factor in a reasonable consumer's decision to utilize Defendant's services. And, as reasonable consumers, had Plaintiffs and Class members known that Defendant would not abide by the terms of its own privacy policies, and share their sensitive Private Information with third parties, they would not have signed up for Defendant's services.

175. Plaintiffs and Class members reasonably relied on Defendant's representations on its Notice of Privacy Practices, as the Notice of Privacy Practices actually induced Plaintiffs and Class members to sign up for Defendant's services.

176. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered damages. Defendant shares Plaintiffs' and Class members' Private Information, without their knowledge or consent. Plaintiffs and Class members were damaged by a gross intrusion into their privacy, by the diminution in the value of their Private Information, and by being placed at a risk of further exposure of Private Information.

177. Defendant created the Website and the Notice of Privacy Practices therein in the State of New York. Decisions concerning the use of the Pixel on Defendant's Website occurred in the State of New York. The acts and omissions complained of—including the transactions that deceived and caused harm to Plaintiffs and other consumers—occurred in and emanated from the State of New York.

178. Under General Business Law § 349(h), Plaintiffs are entitled to damages in an amount to be proven at trial, costs and reasonable attorney's fees, and other further relief.

RELIEF REQUESTED

Plaintiffs, on behalf of themselves and the proposed Class and Subclasses, respectfully request that the Court enter an Order:

A. Determining that the claims alleged herein may be maintained as a class action and issue an order certifying the Class and Subclasses defined above;

B. Appointing Plaintiffs as Class representatives, and their counsel as Class counsel;

C. Enjoining Defendant from engaging in the unlawful practices and illegal acts described herein;

D. Awarding Plaintiffs the Class and Subclasses: (1) actual or statutory damages; (2) punitive damages—as warranted—in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) equitable disgorgement and injunctive relief as pleaded or as the Court may deem proper; and (5) reasonable attorneys' fees and expenses and costs of suit; and

E. For other such and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, demand a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: January 30, 2024

Respectfully submitted,

TUSA P.C.

/s/ Joseph S. Tusa
Joseph S. Tusa
joseph.tusapc@gmail.com
P.O. Box 566
55000 Main Road, 2nd Floor
Southold, NY 11971
Telephone: (631) 407-5100

Daniel O. Herrera*
Nickolas J. Hagman*
Alex Lee*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
alee@caffertyclobes.com

**Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiffs and Proposed Counsel for the Putative Class