Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

THOMAS HODGES, HALEYRAE CANNELL, DANIELLE BENEDICT, CHRISTOPHER BRITTON, XE DAVIS, AND EMILY HOZA, individually and on behalf of all others similarly situated, Plaintiffs, v. GOODRX HOLDINGS, INC., Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Thomas Hodges, HaleyRae Cannell, Danielle Benedict, Christopher Britton, Xe Davis, and Emily Hoza (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, hereby file this class action complaint against Defendant GoodRx Holdings, Inc. ("Defendant" or GoodRx"), and in support thereof allege the following:

INTRODUCTION

1. This is a class action brought against GoodRx for alleged violations of state and federal wiretapping statutes, consumer protection laws, common law privacy rights, in connection with its interception of the electronic communications and contents of visitors to both its website, https://www.goodrx.com, and the GoodRx mobile application (the "GoodRx Platform" or "Platform"). GoodRx embeds tracking software and business analytical tools, which disclose personally identifiable information to some of the largest advertising companies in the country such as Meta Platforms, Inc. ("Meta"), Criteo Corp. ("Criteo"), and Google LLC, ("Google").

2. For example, GoodRx utilized a piece of code from Meta on the GoodRx platform, commonly referred to as the Meta Pixel ("Meta Tracking Pixel" or "Pixel"), which enabled it to track GoodRx users. The Pixel then deploys on the Internet browser of each GoodRx platform user for the purpose of watching, intercepting, and recording the GoodRx platform user's electronic communications with GoodRx, including their mouse movements, clicks, keystrokes (such as substantive information being entered into an information field or text box), URLs of web pages visited, and other electronic communications in real-time ("Communications").

3. Likewise, Criteo is the creator of its own software development kit pixel ("SDK"). Criteo also provided GoodRx with its SDK technology, which GoodRx incorporated into the GoodRx Platform via GoodRx's mobile application.

4. Additionally, Google offers its own tracking and analytics products and created its own SDK that GoodRx also integrated into the GoodRx Platform.

5. Through GoodRx's improper and illegal conduct, Plaintiffs and putative Class Members' private information was collected and disclosed for advertising and analytics purposes to third parties, including Meta, Criteo, and Google. This information includes personally identifying information ("PII") and/or personally identifiable health information ("PHI").

6. Information about a person's physical and mental 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.

7. Significantly, Defendant has already admitted to this misconduct, publicly stating on February 28, 2020, that, "we found in the case of Facebook advertising, we were not living up to our own standards. For this we are truly sorry, and we will do better." Subsequently, during a

March 2020 GoodRx board meeting presentation, the company acknowledged it has been sharing "information that could be linked to user's interest in certain drugs … with Facebook." Further, Facebook investigated and determined that GoodRx had violated Facebook's advertising policy terms, which prohibit the sharing of health information with Facebook.

8. The tracking pixels and SDKs are 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 a website (such as a general search bar, chat feature, or text box), among other things.

9. This tracking technology is programmable, meaning that Defendant is responsible for determining exactly what information was tracked and collected from Plaintiffs and Class Members during their visits to the GoodRx Platform, and subsequently transmitted to Meta, Google, and/or Criteo – the intended third-party recipients.

10. Pixels and SDKs 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 via Facebook to bolster its profits.

11. Correspondingly, Defendant exploited the PII and/or PHI that Plaintiffs and putative Class Members input and searched via the GoodRx Platform and used this PII to assist with the creation of detailed profiles that reflect individual GoodRx Platform users' PII and/or PHI, including personal and sensitive health information, which allowed Meta and other third parties to deliver targeted advertisements to Plaintiffs and putative Class Members.

[1] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Feb. 17, 2023).

12. The above-described practice is the functional equivalent of placing a bug or listening device on a phone line because Defendant's Platform essentially allowed third parties to "listen in" and receive private information, including PII and/or PHI, that Plaintiffs and putative Class Members did not intend to be shared with Meta, Google, Criteo or any other third parties.

13. Importantly, these third parties would never have received Plaintiffs and putative Class Members' private information but for Defendant's installation and implementation of the Pixel and other tracking and analytical tools (the "Tracking Tools").

14. By installing, programming, and controlling the Tracking Tools as described herein, Defendant aided, agreed, employed, and conspired with third-party companies to intercept Plaintiffs and putative Class Members' private information without their knowledge or consent.

15. GoodRx's interception of this highly sensitive information without the consent of Plaintiffs and Class Members constitutes an egregious and extreme invasion of privacy.

16. The actions taken by Defendant to spy on its GoodRx Platform users violate numerous state wiretapping and privacy laws.

17. Plaintiffs are citizens of California, Florida, Illinois, New Jersey, New York, and Pennsylvania, and bring this action individually and on behalf of a nationwide class consisting of consumers whose GoodRx Platform Communications were surveilled in real-time and intercepted through Defendant's procurement and use of tracking technology embedded on the GoodRx Platform, causing them injuries, including violations of their substantive legal privacy rights under their respective states' wiretapping laws, invasion of their privacy, and exposure of their PII and PHI (collectively, the "Class").

18. Plaintiffs and putative Class Members seek all civil remedies provided under the causes of action listed below, including but not limited to compensatory, statutory, and punitive damages, and attorneys' fees and costs.

19. Plaintiffs and putative Class Members seek injunctive relief that will halt Defendant's ongoing unlawful conduct.

THE PARTIES

20. Plaintiff Thomas Hodges is a citizen of the State of California, and at all times relevant to this action, resided and was domiciled in Sacramento County, California, had a Facebook account, and visited and utilized the GoodRx Platform.

21. Plaintiff HaleyRae Cannell is a citizen of the State of Florida, and at all times relevant to this action, resided and was domiciled in Orange County, Florida, had a Facebook account, and visited and utilized the GoodRx Platform.

22. Plaintiff Danielle Benedict is a citizen of the State of Illinois, and at all times relevant to this action, resided and was domiciled in Kendall County, Illinois, had a Facebook account, and visited and utilized the GoodRx Platform.

23. Plaintiff Christopher Britton is a citizen of the State of New Jersey, and at all times relevant to this action, resided and was domiciled in Salem County, New Jersey, had a Facebook account, and visited and utilized the GoodRx Platform.

24. Plaintiff Xe Davis is a citizen of the State of New York, and at all times relevant to this action, resided and was domiciled in Ulster County, New York, had a Facebook account, and visited and utilized the GoodRx Platform.

25. Plaintiff Emily Hoza is a citizen of the State of Pennsylvania, and at all times relevant to this action, resided and was domiciled in Westmoreland County, Pennsylvania, had a Facebook account, and visited and utilized the GoodRx Platform.

26. Class Members are adult U.S. citizens who visited GoodRx's Platform from their computers and/or mobile devices. At all relevant times, putative Class Members maintained Facebook accounts. During the relevant time period, putative Class Members visited GoodRx's Platform to search for personal, health-related information, telehealth treatments, and medications.

27. Defendant, GoodRx Holdings, Inc., is a public company with its principal place of business located at 2701 Olympic Blvd., West Building Suite 200, Santa Monica, CA 90404. GoodRx employs approximately 800 individuals and generated annual revenue in the amount of $765 million in 2022. The GoodRx Platform facilitates consumer searches for medications and discounts on those medications, as well as research regarding symptoms, illnesses and health conditions, and scheduling telehealth appointments with licensed healthcare providers.

JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all putative Class Members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more Members of the proposed Class, and at least one Member of the proposed Class, including Plaintiffs are citizens of states different than Defendant.

29. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the Electronic Communications Privacy Act, 18 U.S.C. § 2511, *et seq*.

30. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in Florida. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Florida while they were located within Florida. At all relevant times, Defendant knew that its practices would directly result in the real-time viewing and collecting of information from Florida citizens while those citizens browse www.goodrx.com. Defendant chose to avail itself of the business opportunities of marketing and selling its services in Florida and viewing real-time data from GoodRx Platform visit sessions initiated by Florida citizens while located in Florida, and the claims alleged herein arise from those activities.

31. Defendant also knows that many GoodRx Platform users visit and interact with Defendant's Platform while they are physically present in Florida. Defendant's Platform allows users to search for nearby stores by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (i.e., without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Defendant is continuously made aware that its GoodRx Platform is being visited by users located in Florida, and that such GoodRx Platform visitors are being wiretapped in violation of Florida statutory and common law.

32. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. GoodRx Platform User and Usage Data Have Immense Economic Value.

33. The "world's most valuable resource is no longer oil, but data."[2]

34. Earlier this year, Business News Daily reported that some businesses collect personal data (i.e., gender, web browser cookies, IP addresses, and device IDs), engagement data (i.e., how consumers interact with a business's website, applications, and emails), behavioral data (i.e., customers' purchase histories and product usage information), and attitudinal data (i.e., data on consumer satisfaction) from consumers.[3] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[4]

35. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[5]

36. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of

---

[2] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

[3] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing with It)*, Business News Daily (updated Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[4] *Id.*

[5] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

Methodologies for Measuring Monetary Value."[6] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[7]

37. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military are estimated to cost USD 55."[8]

B. GoodRx Platform Users Have a Reasonable Expectation of Privacy in Their Interactions with the GoodRx Platform.

38. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the Defendants said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[9]

39. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[10] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[11]

---

[6] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[7] *Id.* at 25.

[8] *Id*.

[9] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

[10] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[11] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

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

41. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[12]

42. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[13]

43. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[14]

C. Meta's Tracking Pixel

44. Meta operates the world's largest social media company and generated $116 billion in revenue in 2022, roughly 98% of which was derived from selling advertising space.[15]

---

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

[13] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/.

[14] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[15] 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

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

46. Meta's Business Tools, including the Pixel, 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.

47. 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.16 Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[17]

48. One such Business Tool is the Pixel, which "tracks the people and type of actions they take."[18] When a user accesses platform hosting the Pixel, private information provided to the host platform is surreptitiously sent to Meta. Notably, this transmission does not occur unless the platform contains the Meta Pixel. Stated differently, each putative Class Member's private information would not have been disclosed to Meta but for Defendant's decisions to install the Pixel on the GoodRx Platform.

---

[16] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Sep. 1, 2023); *see* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Sep. 1, 2023).

[17] 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 last visited Sep. 1, 2023)

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

49. At the time of accessing the GoodRx Platform, Plaintiffs maintained active social media accounts on Facebook and/or Instagram.

50. This secret transmission was initiated by Defendant's source code in order to share Plaintiffs and Class Members' private information, which was intended exclusively for Defendant, with Meta.

D. Google's Tracking Pixel

51. Google, one of the most recognized companies in the world, is also one of the largest advertising companies in the world.

52. Google "make[s] money" from "advertising products [that] deliver relevant ads at just the right time," and generates "revenues primarily by delivering both performance advertising and brand advertising."[19] In 2020, Google generated $146.9 billion in advertising revenue, which amounted to more than 80 percent of Google's total revenues for the year.

53. In 2020, Google began its Google Analytics 4 to analyze users web and mobile app activity.

54. Following this new product, Google saw a $62.6 billion increase in advertising revenues.

55. Google Analytics offers "a complete understanding of your customers across devices and platforms."[20]

56. Third-party platforms like GoodRx can utilize Google Analytics by placing a code on each page of the website or application. The software immediately intercepts the user's

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

[20] *Analytics*, GOOGLE, https://marketingplatform.google.com/about/analytics/ (last visited Jan. 10, 2023).

communications with the web page and also collects identifiable information such as a user's IP address or other information.

57. The Code collects this data to Google Analytics where the information is utilized to generate reports to analyze the user's activity on the web page.

58. GoodRx utilizes Google's technology and disclosed users' PII and PHI to Google without the consent and notification to the users.

E. Criteo's Tracking Pixel

59. Criteo is a digital advertising company targeting personal advertising. In 2021, Criteo generated $2.2 billion in revenue.

60. Criteo offers its Criteo One Tag, which is tracking code like the Meta Pixel.

61. GoodRx utilizes Criteo's technology on the GoodRx Platform to track its users' communications and information on the site.

62. GoodRx disclosed users PII and PHI to Criteo without users' consent or knowledge of this disclosure of private information.

F. Other Tracking Technologies

63. GoodRx incorporated several other third parties' Tracking Tools onto its GoodRx Platform.

64. Upon information and belief, GoodRx incorporated tracking technologies from nearly 20 third parties onto its GoodRx Platform to intercept users' data without their consent.

G. Statutory Background

The California Invasion of Privacy Act

65. The California Invasion of Privacy Act ("CIPA") prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or

learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

66. To establish liability under CIPA Section 637.1(a), Plaintiff Hodges and putative California Subclass Members need only establish that Defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system; or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

67. Violations of CIPA are not limited to phone lines, but also apply to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of

consumers' internet browsing history). Indeed, the Meta Pixel was recently examined by the Northern District of California with the district court concluding that the plaintiffs were likely to succeed on the merits with respect to both CIPA and the analogous Federal Wiretap Act. *See In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *11, 13 (N.D. Cal. Dec. 22, 2022).

68. CIPA affords a private right of action to any person who has been subjected to a violation of the statute to seek injunctive relief and statutory damages of $5,000 per violation, regardless as to whether they suffered actual damages. Cal. Penal Code § 637.2.

The California Constitution

69. The California Constitution, Art. 1, § 1, provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." The California Constitution provides a private right of action against private entities for violations of the right to privacy.

70. A claim for invasion of privacy under the California Constitution requires allegations of (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms. Available relief for such violations may include, but is not limited to, reasonable compensation for the harm to Plaintiff Hodges and putative California Subclass Members' privacy interests as well as disgorgement of any profits made by GoodRx as a result of its intrusions upon Plaintiff Hodges and putative California Subclass Members' privacy, and punitive damages resulting from the malicious, willful, and intentional nature of GoodRx's

actions, directed at injuring Plaintiff Hodges and putative California Subclass Members in conscious disregard of their rights. Such damages are warranted here.

71. Putative Class Members who are citizens of California satisfy each of the three requirements for an invasion of privacy claim under the California Constitution.

The Confidentiality of Medical Information Act

72. The Confidentiality of Medical Information Act (CMIA) is a California law that protects the confidentiality of individually identifiable medical information obtained by health care providers, health insurers, and their contractors. Among other things, the CMIA (1) prohibits covered health care providers from disclosing medical information regarding a patient, enrollee, or subscriber without first obtaining authorization, and (2) requires covered health care providers that create, maintain, store or destroy medical information to do so in a manner that preserves the confidentiality of such information. Cal. Civ. Code § 56 (West)

73. In *Vigil c. Muir Medical Group IPA, Inc.*, a California Appellate Court further analyzed the meaning of CMIA. "The common or ordinary dictionary definition of "confidential" is "private" or "secret." (See, e.g., Black's Law Dict. (11th ed. 2019) p. 373, col. 1 ["meant to be kept secret]; Webster's Third New International Dict. (1961) p. 158, col. 1 ["private, secret"].) Thus, under the ordinary meaning of "confidential," the confidential nature of information is not breached unless the information is reviewed by unauthorized parties. This construction is consistent with the purpose of the CMIA to protect patients' privacy. (*See Brown v. Mortensen* (2011) 51 Cal.4th 1052, 1071, 126 Cal.Rptr.3d 428, 253 P.3d 522 ["[T]he interest protected by [the CMIA] is an interest in informational privacy"].)" *Vigil v. Muir Med. Group IPA, Inc.*, 300 Cal. Rptr. 3d 32 (Ct. App. 2022), review denied (Jan. 25, 2023)(emphasis added).

74. Class Members who are citizens of California satisfy the requirements CMIA claim as their confidential medical information was disclosed to a third party without their consent, and the personal information stored by GoodRx in a manner that did not protect the confidentiality of the information.

The Pennsylvania Wiretapping and Electronic Surveillance Control Act

75. The Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18. Pa. C.S. § 5725 ("WESCA"), provides for a civil cause of action against any person who intercepts, discloses, or uses Plaintiff Hoza and putative Pennsylvania Subclass Members' wire, electronic, or oral communication and entitles Plaintiff Hoza and putative Pennsylvania Subclass Members to recover actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000, whichever is higher, as well as punitive damages and reasonable attorneys' fees and other litigation costs reasonably incurred.

76. To establish liability under the WESCA, Plaintiff Hoza and putative Pennsylvania Subclass Members need only establish that (1) they engaged in communications, (2) they possessed an expectation that the communication would not be intercepted, (3) their expectation was justifiable under the circumstances, and (4) the other party attempted to, or successfully intercepted the conversation, or encouraged another to do so. *Kelly v. Borough of Carlisle*, 622 F.3d 248, 257 (3d Cir. 2010). Plaintiff Hoza and putative Pennsylvania Subclass Members satisfy each of these elements, as discussed below.

The Florida Security of Communications Act

77. The Florida Security of Communications Act, Fla. Stat. §§ 934.01, et seq. ("FSCA"), provides for a civil cause of action against any person who intercepts, discloses, or uses another person's wire, oral, or electronic communication in violation of §§ 934.03-934.09.

Available relief for such violations may include preliminary or equitable declaratory relief, actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher, punitive damages, and reasonable attorneys' fees and other litigation costs reasonably incurred.

78. To establish liability under the FSCA, Plaintiff Cannell and putative Florida Subclass Members need only establish that (1) they are or were Florida residents, or that the interceptions occurred in Florida, (2) they had a subjective expectation of privacy in the intercepted communication, and (3) that society recognizes the expectation of privacy as reasonable. *Denarii Sys., LLC v. Arab*, No. 12-24239-CIV, 2013 WL 6162825, at *2 (S.D. Fla. Nov. 25, 2013). Florida Subclass Members satisfy each of these elements, as discussed below.

The New Jersey Constitution

79. The New Jersey Constitution, Art. 1, ¶ 1, provides that "All persons are by nature free and independent, and have certain natural and unalienable rights, among which are those of enjoying and defending life and liberty, of acquiring, possessing, and protecting property…". The New Jersey Supreme Court has ruled that the right to privacy is one of the "natural and unalienable" rights recognized by the New Jersey Constitution. *Hennessey v. Coastal Eagle Point Oil Co.*, 129 N.J. 81, 609 A.2d 11 (1992). The New Jersey Supreme Court has "recognized a constitution-based privacy right in many contexts…" including "disclosure of confidential personal information." *Id.* (citing *Application of Martin*, 90 N.J. 295, 447 A.2d 1290 (1982)); *See also Burnett v. Cnty. of Bergen*, 198 N.J. 408, 968 A.2d 1151 (2009) (citing *State v. Reid*, 194 N.J. 386, 389, 945 A.2d 26 (2008) ("recognizing reasonable expectation of privacy in subscriber information under State Constitution, notwithstanding disclosure to Internet service providers")).

80. Additionally, New Jersey's Supreme Court made it clear that although users voluntarily enter personal information into online databases and websites to use services, they are not relinquishing their privacy rights by doing so. "[I]t is well-settled under New Jersey law that disclosure to a third-party provider, as an essential step to obtaining service altogether, does not upend the privacy interest at stake. *See McAllister, supra*, 184 N.J. at 31, 875 A.2d 866; *Hunt, supra*, 91 N.J. at 347, 450 A.2d 952. In the world of the Internet, the nature of the technology requires individuals to obtain an IP address to access the Web. Users make disclosures to ISPs for the limited goal of using that technology and not to promote the release of personal information to others. Under our precedents, users are entitled to expect confidentiality under these circumstances." *State v. Reid*, 194 N.J. 386, 945 A.2d 26 (2008)(emphasis added). "We find that Article I, Paragraph 7, of the New Jersey Constitution protects an individual's privacy interest in the subscriber information…" *Id*.

81. Plaintiff Britton and putative New Jersey Subclass Members had their privacy rights violated when their PII and PHI were compromised due to GoodRx utilizing the third-party tracking technology to share this constitutionally protected information with third parties.

New York Security Breach and Notification Act (SHIELD Act)

82. The SHIELD Act, which became effective on October 23, 2019, amended certain of New York's existing data privacy and security laws and introduced substantive data security requirements for regulated entities. The SHIELD Act applies to any business that owns or licenses computerized data that includes the "private information" of New York residents (including employees), regardless of whether the business otherwise operates in New York state. N.Y. Gen. Bus. Law § 899-aa (McKinney).

83. Under the SHIELD Act, (a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person; (b) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

> (1) social security number;
> (2) driver's license number or non-driver identification card number;
> (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;
> (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
> (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity;
> or
> (ii) **a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.**

Id. (emphasis added).

84. Under the SHIELD Act, "Breach of the security of the system" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. Good faith access to, or acquisition of, private information by an employee or agent of the business for the purposes of the business is not a breach of the

security of the system, provided that the private information is not used or subject to unauthorized disclosure. *Id*.

85. "In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person:

> (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
> (2) indications that the information has been downloaded or copied; or
> (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
> (d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.

Id. (emphasis added).

86. "Any person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization." *Id.*

87. Plaintiff Davis and New York Subclass Members did not authorize Meta, Facebook, or any third party other than GoodRx to view their PII and/or PHI. Meta, Google, and Criteo were unauthorized entities viewing the Plaintiff and Class Members' personal confidential information. GoodRx did not disclose this to Plaintiff Davis; therefore, GoodRx is in violation of the SHIELD Act and are liable for that violation to New York Subclass Members and Plaintiff Davis.

88. Plaintiff Davis and putative New York Subclass Members had their privacy rights violated when their PII and PHI were compromised without their knowledge due to GoodRx utilizing third-party tracking pixels to share this information with third parties.

Other Applicable Statutes

89. The Electronic Communications Privacy Act ("ECPA") is the federal analog to CIPA and, among other things, prohibits the intentional interception of the contents of any electronic communication. 18 U.S.C. § 2511. The elements of an ECPA claim are:

> (1) Except as otherwise specifically provided in this chapter any person who—
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511 (1)(a) and (c)-(d). As discussed below, Plaintiffs and Putative Class Members satisfy each of these elements.

H. Defendant's Platform and the Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiffs and Class Members' private information to Third Parties.

90. Defendant's Platform is accessible on mobile devices and desktop computers and gives users the option to search for and obtain information about prescription drugs, including discounts on those drugs, as well as symptoms, illnesses and health conditions, and to schedule telehealth appointments.

91. In order to use Defendant's Platform, users must provide Defendant with certain sensitive and personal information. For example, when looking for discounts on prescription drugs, customers must enter the names of their prescription medications and their locations. If users do not specify their location, the Platform independently determines users' locations. And when scheduling telehealth appointments, users must provide their email addresses, phone numbers, dates of birth, biological sex, mailing address, and identify their specific, sensitive, and private health issues, such as depression, a urinary tract infection, or erectile dysfunction.

92. As a result, users share and communicate private information, including PII and/or PHI, with Defendant via its Platform.

93. Defendant purposely installed third-party Tracking Tools on the GoodRx Platform and programmed specific webpage(s) to surreptitiously share its users' private information with third parties, including PII and/or PHI.

94. The tracking software tracks users as they navigate through the GoodRx Platform and transmits to third parties each users' communications, including which pages are visited, which buttons are clicked, specific information users enter into search bars and text boxes, and other

information, including users' IP addresses.[21] An IP address is a unique number assigned to a user's internet-enabled device that informs websites of the device's city, zip code, and physical location.

95. Notably, after users provide their private information via Defendant's Platform, GoodRx, without the users' knowledge or consent, supplies this private information to third parties via the Tracking Tools.

96. If the user is also a Facebook user, the private information that Meta receives from Defendant is linked to the user's Facebook profile (via their Facebook ID or "c_user id"), which includes other identifying information, including the identity of the person that is transmitting the private information.

97. Plaintiffs and putative Class Members did not and could not anticipate that Defendant would aid and conspire with third parties to intercept and transmit their communications, which include private information.

98. However, users who provided their private information, as described above, were not notified of GoodRx's Privacy Policy or about its use of cookies and other tracking technologies, or that their private information would be shared with third parties.

I. Defendant's Use of the Pixel and Other Tracking Technologies

99. Web browsers are software applications that allow users 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).

[21] FACEBOOK, META PIXEL, https://developers.facebook.com/docs/meta-pixel/(last visited Sep. 1, 2023).

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

101. When a user visits Defendant's Platform and undertakes various actions, the user and Defendant are engaged in an ongoing back-and-forth exchange of electronic communications taking place via the user's web browser and Defendant's computer server.

102. These communications are invisible to ordinary users because they consist of HTTP Requests and HTTP Responses, and one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.[22]

> **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.

103. A user's HTTP Request essentially asks Defendant's Platform 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 Platform).

[22] 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.")

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

105. When a user visits www.GoodRx.com, clicks any link or enters search terms, the user's web browser automatically sends an HTTP Request to Defendant's web server. Then, the Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage.

106. The user does not see Defendant's Source Code, or any HTTP Requests sent in the "background" while the webpage is operating. In fact, this unseen Source Code manipulates 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.

107. Thereafter, when an event triggers the Pixel code, the code instructs the web browser to duplicate users' private information intended for Defendant and then sends that information to Meta at the same time it is 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 private information. This occurs invisibly and without the user's knowledge.

108. A similar process occurs via the other Tracking Tools that are embedded on the GoodRx Platform. In other words, private information intended solely for Defendant is intercepted via the Tracking Tools and conveyed to other third parties such as Google and Criteo.

J. Users Do Not Provide Informed Consent Before Their Information Is Collected and Intercepted.

109. Defendant did not ask users, including Plaintiffs and putative Class Members, whether they consented to be wiretapped via Tracking Tools or to external sharing of their private information. In fact, users were never told that their electronic communications are being wiretapped or shared through Tracking Tools.

110. Defendant's written policies did not adequately disclose the wiretapping and privacy invasion for multiple reasons. In fact, for a substantial period of time, Defendant's privacy policy explicitly stated:

> However, we never provide advertisers or any other third parties any information that reveals a personal health condition or personal health information.

111. Significantly, in or around March 2019, Defendant quietly removed the phrase "or any third parties" from its privacy policy. Then, one month later, in April 2019, Defendant deleted this sentence altogether without providing any notice of this revision to users, including Plaintiffs and Class Members.

112. As such, users who provide their private information and any PII and/or PHI were not informed that Defendant would track and share their private information and communications with third parties. Further users, including Plaintiffs and Class Members, never agreed nor were given the option to agree to any such privacy policy when using the GoodRx Platform.

K. Plaintiffs and Putative Class Members' Private Information Was Linked to Their Individual Facebook Profiles and Unique Identifiers.

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

114. 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 people who come into possession of the FID can connect it to the corresponding Facebook profile.

115. 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 Platform, if, and only if, the owner of that website has installed the Meta Pixel.

116. Meta 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.

117. Thus, the Pixel was triggered each time Plaintiffs and putative Class Members communicated with Defendant via www.GoodRx.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 originated from a user's browser once the user initiated an action on the GoodRx Platform: one, as intended, to Defendant, and a second, undetectable to the user, was sent to Facebook. Accordingly, at the same time the user's browser dispatched a GET Request to Defendant, it sent a duplicate to Facebook.

118. Plaintiffs and putative Class Members were unaware this was happening, and Defendant did not inform Plaintiffs and Class Members that private information communicated via Defendant's Platform would be shared with Meta or other third parties.

119. Defendant did not share anonymized data with Meta, but instead shared private information containing PII and/or PHI tied to unique identifiers connected to specific users.

120. On information and belief, Defendant shared other identifiers of Plaintiffs and Class Members via the Tracking Tools to third parties such an IP address, which is a unique address that identifies a device on the internet or a local network and is linked to a particular user.

121. Defendant failed to disclose to users of its Platform that it shared their private information with Meta or any other third party.

122. Defendant benefitted from the unauthorized sharing with third parties of Plaintiffs and putative Class Members' private information. By using the Tracking Tools from Meta and other third-parties and providing Plaintiffs and Class Members' private information to Meta and other third-parties, GoodRx improved its advertising abilities, business analytics, and benefitted financially from advertising through third parties.

L. Meta, Google, Criteo and other Third Parties Exploited and Used Plaintiffs and Class Members' Private Information

123. Third parties such as Meta, Google and Criteo exploit and benefit from the private information they intercept from Plaintiffs and Class Members via the GoodRx Platform.

124. "Data is the new oil of the digital economy,"[23] and Meta, for example, 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 Meta and other third-

[23] DATA IS THE NEW OIL OF THE DIGITAL ECONOMY https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited Sep. 1, 2023).

parties are actively examined, curated, and put to use by the company. Meta acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Meta offers the Pixel free of charge[24] and the price that Defendant pays for the pixel is the data that it allows Meta to collect.

125. Meta describes itself as a "real identity platform,"[25] meaning users are allowed only one account and must share "the name they go by in everyday life."[26] To that end, when creating an account, users must provide their first and last name, date of birth, and gender.[27]

126. Meta sells advertising space by emphasizing its ability to target users.[28] Meta is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant).[29] This allows Meta to make inferences about users beyond what they explicitly disclose, including their "interests," "behavior," and "connections."[30] Meta compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[31]

---

[24] FACEBOOK PIXEL: WHAT IT IS AND WHY YOU NEED IT https://seodigitalgroup.com/facebook-pixel/(last visited Sep. 1, 2023).

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

[26] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity. (last visited Sep. 1, 2023).

[27] FACEBOOK, SIGN UP, https://www.facebook.com/ (last visited Sep. 1, 2023).

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

[29] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142. (last visited Sep. 1, 2023).

[30] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting. (last visited Sep. 1, 2023).

[31] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences. (last visited Sep. 1, 2023).

127. Advertisers can also build "Custom Audiences,"[32] which helps them 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."[33] 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."[34] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Meta. This data can be supplied to Meta by manually uploading contact information for customers or by utilizing Meta's "Business Tools."[35]

128. The Meta Pixel, and the private information mined and curated with it, is key to this business. As Meta puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Meta, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[36]

129. Meta 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 Meta to create Core, Custom, and Lookalike Audiences for

---

[32] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494. (last visited Sep. 1, 2023).

[33] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting. (last visited Sep. 1, 2023).

[34] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328. (last visited Sep. 1, 2023).

[35] 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. (last visited Sep. 1, 2023).

[36] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087. (last visited Sep. 1, 2023).

advertising and marketing purposes, Meta viewed, processed, and analyzed Plaintiffs and putative Class Members' private information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Meta employees at the direction and behest of Meta, which 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.[37] This process is known as data ingestion and allows "businesses to manage and make sense of large amounts of data."[38]

130. By using these tools, Meta can 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.[39] This illustrates how Meta views and categorizes data as the data is received from the Pixel.

131. Moreover, even if Meta 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.

132. Additionally, Google has already been publicly admonished for collecting sensitive information without users' consent. In 2019, the *Wall Street Journal* reported that Google was

[37] HOW DOES FACEBOOK HANDLE THE 4+ PETABYTE OF DATA GENERATED PER DAY? CAMBRIDGE ANALYTICA-FACEBOOK DATA SCANDAL https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4. (last visited Sep. 1, 2023).

[38] FACEBOOK DATABASE- A THOROUGH INSIGHT INTO THE DATABASES USED @ FACEBOOK https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/(last visited Sep. 1, 2023).

[39] A COMPLETE GUIDE TO FACEBOOK TRACKING FOR BEGINNERS https://www.oberlo.com/blog/facebook-pixel/(last visited Sep. 1, 2023).

collecting sensitive information from a popular women's menstruation app and Google collected the same personal health information as Meta did, as revealed by an FTC investigation.

133. Further, in 2019, the *Financial Times* reported that Google received prescription drug information that users input on drug.com. Google still used this information for advertising to the users and utilized the same technology on the GoodRx Platform.

134. Similarly, Criteo incorporated its tracking technology into the GoodRx Platform for it's personal gain and took no steps to safeguard or ask for consent of users who's information Criteo unlawfully received.

M. Defendant Was Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures and Plaintiffs and Putative Class Members' Private Information Had Financial Value

135. 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 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.

136. In exchange for disclosing the private information of its users, Defendant is compensated by third parties in the form of enhanced advertising services and more cost-efficient marketing and business analytics on its platform.

137. 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 users and potential users.

138. For example, 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 Meta, associated Plaintiffs and Class Members' private information with preexisting Facebook user profiles.

139. On information and belief, the Tracking Tools were utilized in a similar fashion for other third-parties such as Google and Criteo.

140. By utilizing tracking technology, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

141. Defendant's disclosure of private information also hurt Plaintiffs and Class Members. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure will only increase to a total of more than $200 billion industry wide.

142. The value of health data is well known and has been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Bil lion 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.[40]

143. 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."[41]

144. 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

[40] HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY https://time.com/4588104/medical-data-industry/ (last visited Sep. 1, 2023).

[41] https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited February 16, 2023).

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."[42]

145. 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.").

146. 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 historical information.

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

148. Additionally, healthcare data is extremely valuable to bad actors and on the black market.

CLASS ACTION ALLEGATIONS

149. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

[42] VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER https://www.getvero.com/resources/twitter-lead-generation-cards/. (last visited Sep. 1, 2023).

> All natural persons in the United States who used any website, app, or service made available by or through GoodRx at any point prior to the execution date of this Agreement (the "Class").

150. Plaintiff Thomas Hodges brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following subclass:

> All natural persons in California who used any website, app, or service made available by or through GoodRx at any point prior to the execution date of this Agreement (the "California Subclass").

151. Plaintiff HaleyRae Cannell brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following subclass:

> All natural persons in Florida who used any website, app, or service made available by or through GoodRx at any point prior to the execution date of this Agreement (the "Florida Subclass").

152. Plaintiff Danielle Benedict brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following subclass:

> All natural persons in Illinois who used any website, app, or service made available by or through GoodRx at any point prior to the execution date of this Agreement (the "Illinois Subclass").

153. Plaintiff Christopher Britton brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following subclass:

> All natural persons in New Jersey who used any website, app, or service made available by or through GoodRx at any point prior to the execution date of this Agreement (the "New Jersey Subclass").

154. Plaintiff Xe Davis brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following subclass:

> All natural persons in New York who used any website, app, or service made available by or through GoodRx at any point prior to the execution date of this Agreement (the "New York Subclass").

155. Plaintiff Emily Hoza brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following subclass:

> All natural persons in Pennsylvania who used any website, app, or service made available by or through GoodRx at any point prior to the execution date of this Agreement (the "Pennsylvania Subclass").

156. Excluded from the Class and Subclasses are Defendant and its affiliates, parents, subsidiaries, officers, and directors, all persons who make a timely election to be excluded from the Class and Subclasses, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearances in this action. Plaintiffs reserve the right to modify or amend the Class or Subclass definitions, as appropriate, during the course of this litigation.

157. **Numerosity:** The Members of the Class are so numerous that individual joinder of all Class Members is impracticable. The precise number of Class Members and their identities may be obtained from the books and records of Defendant.

158. **Commonality:** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to: (a) whether Defendant utilizes the Meta Pixel, Google Pixel, or the Criteo SDK and Pixel to watch in real time and intercept Defendant's Platform visitors' PII and PHI; (b) whether Defendant intentionally discloses the intercepted PII and PHI of its GoodRx Platform users; (c) whether Defendant acquires the contents of GoodRx Platform users' PII and PHI without their consent; (d) whether Defendant's conduct violates state or federal privacy statutes, as cited in this Complaint; (e) whether Plaintiffs and Class Members are entitled to equitable relief; and (f) whether Plaintiffs and Class Members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

159. Typicality: Plaintiffs' claims are typical of the other Class Members' claims because, among other things, all Class Members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiffs and each Member of the Class had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiffs and the Members of the Class typical of one another.

160. **Adequacy of Representation**: Plaintiffs have fairly and adequately represented and protected the interests of the Class and will continue to do so. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Members of the Class, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of the other Members of the Class.

161. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

162. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business

practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each Member of the Class. If Defendant intercepted Plaintiffs and Class Members' Communications, then Plaintiffs and each Class Member suffered damages by that conduct.

163. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through GoodRx's records or the Facebook Meta Pixel, Google Pixel, or the Criteo SDK and Pixel records.

CLAIMS FOR RELIEF

COUNT I
Violations of Electronic Communications Privacy Act ("ECPA")
18 U.S.C. §§ 2511(1), *et seq*.
Unauthorized Interception, Use, and Disclosure
(All Class Members)

164. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 163 of this Complaint as if fully set forth herein.

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

166. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

167. The transmissions of Plaintiffs and Class Members' private information to Defendant via GoodRx's Platform qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

168. **Electronic Communications**. The transmission of private information between Plaintiff and Class Members on the one hand and Defendant on the other via its Platform with

which they chose to exchange communications are "transfer[s] of signs, signals, writing,... data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

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

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

a. Plaintiffs and Class Members' browsers;

b. Plaintiffs and Class Members' computing devices;

c. Defendant's webservers; and

d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications

172. Whenever Plaintiffs and Class Members interacted with the GoodRx Platform, Defendant, through the various third-party tracking pixels imbedded and ran on its platform, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of

Plaintiffs and Class Members' electronic communications to third parties, including Meta and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 251 l(l)(c).

173. Whenever Plaintiffs and Class Members interacted with Defendant's Platform, Defendant, through the Tracking Pixel embedded on its Platform, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs and Class Members' electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 251 l(l)(d).

174. Whenever Plaintiffs and Class Members interacted with Defendant's Platform, Defendant, through the source code embedded on its Platform, contemporaneously and intentionally redirected the contents of Plaintiffs and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication.

175. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiffs and Class Members regarding PII and PHI, treatment, medication, and scheduling.

176. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 25ll(l)(a), Defendant violated 18 U.S.C. § 251 l(l)(c).

177. 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. § 251 l(l)(a), Defendant violated 18 U.S.C. § 251 l(l)(d).

178. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the tracking pixels to track and utilize Plaintiffs and Class Members' PII and PHI for financial gain.

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

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

181. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

182. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiffs and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

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

184. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs and Class Members' private information does not qualify for the party exemption.

185. Defendant's acquisition of patient communications that were used and disclosed to Criteo, Meta, and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and New York, New Jersey, California, Florida, Pennsylvania, and Illinois.

186. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person ... without authorization" from the patient.

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

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

a) Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and
b) Disclosed individually identifiable health information to Facebook and Google without patient authorization.

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

190. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs and Class Members' communications about their individually-identifiable patient health information on its Platform, because it used its participation in these communications to improperly share Plaintiffs and Class Members' individually identifiable patient health information with third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know were receiving their

individually-identifiable patient health information, and that Plaintiffs and Class Members did not consent to receive this information.

191. Defendant accessed, obtained, and disclosed Plaintiffs and Class Members' private information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

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

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

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

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

COUNT II
Violation of Common Law Invasion of Privacy- Intrusion Upon Seclusion
(All Class Members)

194. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 163 as if set forth herein.

195. A plaintiff asserting claims for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which plaintiff has a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

196. GoodRx's disclosure of Plaintiffs and Class Members' sensitive data, including PII and PHI to third parties like Google, Meta, and Criteo constitutes an intentional intrusion upon Plaintiffs and Class Members' solitude or seclusion.

197. Plaintiffs and Class Members had a reasonable expectation of privacy in the health information and other personal data that GoodRx disclosed to third parties.

198. Plaintiffs and Class Members' interactions with the GoodRx Platform are inherently sensitive in nature. Plaintiffs and Class Members reasonably expected this information would remain private and confidential and would not be disclosed to third parties without their consent.

199. This expectation is especially heightened given GoodRx's consistent representations to users that this information would be safeguarded and not disclosed to third parties like Meta, Google, and Criteo.

200. In March of 2019, GoodRx promised it adheres to the Digital Advertising Alliance principles. These principles state that entities "should not collect and use . . . pharmaceutical prescriptions, or medical records about a specific individual for Online Behavioral Advertising without Consent."

201. GoodRx's Co-CEO publicly made similar statements, tweeting "People can use GoodRx without giving us any information. Any information we do receive is stored under the same guidelines as any health entity."

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

203. 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 well as a disgorgement of profits made by GoodRx as a result of its intrusions upon Plaintiffs and Class Members' privacy.

204. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of GoodRx's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights.

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

COUNT III
Violation of the California Invasion of Privacy Act
Cal. Penal Code, §§ 631, *et seq.*
(California Subclass Members)

206. Plaintiff Hodges repeats and incorporates by reference paragraphs 1 through 163 as if set forth herein.

207. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society. Cal. Penal Code § 630.

208. California Penal Code § 631(a) provides, in pertinent part: Any person who, by means of any machine, instrument, or contrivance, or in any other manner … [ii] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; [iii] or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [iv] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

209. A Defendant must show it had the consent of all parties to a communication.

210. Plaintiff Hodges and California Subclass Members' specific user input events and choices communicated with Defendant's GoodRx Platform are tracked and collected by Defendant using the SDK provided by third parties, such as Meta, Google, or Criteo. The user's affirmative actions, such as inputting information, selecting options, or relaying a response, constitute communications within the scope of CIPA.

211. At all relevant times, Defendant aided, agreed with, and conspired with Meta, Google and/or Criteo to track and intercept Plaintiff Hodges and California Subclass Members' Internet communications while accessing the Platform. These communications were intercepted without the authorization and consent of Plaintiff Hodges and California Subclass Members. Defendant intentionally inserted an electronic device into its GoodRx Platform that, without the knowledge and consent of Plaintiff Hodges and California Subclass Members, tracked and transmitted the substance of their confidential communications with Defendant to a third party.

212. Defendant willingly facilitated third parties' interception and collection of Plaintiff Hodges and California Subclass Members' private information by embedding the various tracking Pixels on its GoodRx Platform.

213. Defendant intended to share Plaintiff Hodges and California Subclass Members' private information and communications to help a third party learn some meaning of the content of the communications.

214. Plaintiff Hodges and California Subclass Members are residents of California and used their devices within California. As such, Defendant records and disseminates California Subclass Members' data, communications, and private information in California.

215. Plaintiff Hodges and California Subclass Members did not consent to any of Defendant's actions in implementing the tracking software. Nor have Plaintiff Hodges and

California Subclass Members consented to Defendant's intentional collection and sharing of their electronic communications and private information.

216. At all relevant times, Plaintiff Hodges and California Subclass Members did not know Defendant was engaging in such recording and sharing of information, and therefore could not provide consent to have any part of their private and confidential communications and private information intercepted and recorded by Defendant and thereafter transmitted to others.

217. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the software and SDK in the source code of Defendant's GoodRx Platform, such as Google Pixel, falls under the broad catch-all category of "any other manner":

218. The computer codes and programs third parties, such as Criteo, used to track Plaintiffs and Class Members' communications while they were navigating www.GoodRx.com, as well as their browsers, computing and mobile devices, third parties' web and ad servers; the web and ad-servers from which third parties, including Google, Meta and/or Criteo, tracked and intercepted Plaintiff Hodges and California Subclass Members' communications while they were using a web browser to access or navigate the Platform, and the computer codes and programs used by third parties to effectuate its tracking and interception of Plaintiff Hodges and California Subclass Members' communications while they were using a browser to visit the GoodRx Platform.

219. Defendant fails to disclose that it used software from third parties specifically to track and automatically transmit communications and private information to a third party, e.g., Meta, Google, Criteo. Through its since-deleted promise to never provide advertisers or any other third parties any information that reveals a personal health condition or personal health information, Defendant acknowledged that Plaintiff Hodges and California Subclass Members'

communications and private information were and are personal, sensitive, and meant to remain confidential. Yet, Defendant failed to disclose to GoodRx Platform users that Defendant will capture and share their PII and PHI with third parties.

220. The private information that Defendant transmits while using third-party software, including personal information that users enter into the GoodRx Platform, health information, medication information, IP addresses, phone numbers, home addresses, email addresses, and dates of birth, constitute confidential information, as well as PII and PHI.

221. The Pixel is designed such that it transmits each of Plaintiff Hodges and California Subclass Members' actions taken on the GoodRx Platform and private information to a third party alongside and contemporaneously with the user initiating the communication. Thus, the communication is intercepted in transit to the intended recipient, Defendant, and before it reaches Defendant's server.

222. As demonstrated herein above, Defendant violates CIPA by aiding and permitting third parties to receive its users' online communications through its GoodRx Platform without their consent.

223. As a direct and proximate result of Defendant's violation of the CIPA, Plaintiff Hodges and California Subclass Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

224. By disclosing Plaintiff Hodges and California Subclass Members' private information, Defendant violated their statutorily protected right to privacy.

225. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiff Hodges and California Subclass Members for the greater of treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory

damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

226. Under the statute, Defendant is also liable for reasonable attorneys' fees, litigation costs, and injunctive and declaratory relief.

COUNT IV
Invasion of Privacy Under California's Constitution
(California Subclass Members)

227. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

228. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

229. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

230. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy from both the government and private entities alike: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information." Ballot Pamp., Proposed Stats. and Amends.

to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*, 530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one's home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994), 7 Cal.4th 1, 81, (Mosk, J., dissenting)(emphasis added).

231. Plaintiff Hodges and California Subclass Members have a legally protected privacy interest, as recognized by the California Constitution, CIPA, common law and the 4th Amendment to the United States Constitution.

232. Plaintiff Hodges and California Subclass Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal privacy laws. Plaintiff Hodges and California Subclass Members were not aware and could not have reasonably expected that Defendant would surreptitiously install software on its GoodRx Platform to automatically track and transmit to third parties each California Subclass Member's private information.

233. Plaintiff Hodges and California Subclass Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information and financial information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff Hodges and California Subclass Members' knowledge or consent.

234. At all relevant times, by using software to capture and communicate Plaintiff Hodges and California Subclass Members' private information, including unique identifiers and FIDs, Defendant intentionally invaded Plaintiff Hodges and California Subclass Members' privacy rights under the California Constitution.

235. Plaintiff Hodges and California Subclass Members did not authorize Defendant to capture and transmit to third parties their private information, including PII and/or PHI.

236. This invasion of privacy is serious in nature, scope, and impact because it relates to Plaintiff Hodges and California Subclass Members' private communications, personally identifiable information, and/or health information. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right.

237. As a result of Defendant's actions, Plaintiff Hodges and California Subclass Members have suffered harm and injury, including, but not limited to, an invasion of their privacy rights.

238. Plaintiff Hodges and California Subclass 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.

239. Plaintiff Hodges and California Subclass Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests as a result of its intrusions upon Plaintiff Hodges and California Subclass Members' privacy.

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

241. Plaintiff Hodges and California Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT V
California Common Law Invasion of Privacy – Intrusion Upon Seclusion
(California Subclass Members)

242. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

243. Plaintiff Hodges and California Subclass Members had a reasonable expectation of privacy in their communications with Defendant via its GoodRx Platform and the communications platforms and services therein.

244. Plaintiff Hodges and California Subclass Members communicated private information, including PII and/or PHI, that they intended for only Defendant to receive and that they believed Defendant would keep private.

245. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff Hodges and California Subclass Members is an intentional intrusion on their solitude or seclusion.

246. Plaintiff Hodges and California Subclass Members had a reasonable expectation of privacy based on the sensitive nature of their communications. Plaintiff Hodges and California Subclass Members have a general expectation that their communications regarding private information will be kept confidential. Defendant's disclosure of private information, coupled with individually identifying information, is highly offensive to the reasonable person.

247. As a result of Defendant's actions, Plaintiff Hodges and California Subclass Members have suffered harm and injury, including, but not limited to, an invasion of their privacy rights.

248. Plaintiff Hodges and California Subclass 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.

249. Plaintiff Hodges and California Subclass Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests as a result of its intrusions upon their privacy.

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

251. Plaintiff Hodges and California Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT VI
Violation of the Unfair Competition Law – Unfair and Unlawful
(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)
(California Subclass Members)

252. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

253. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

254. Defendant engaged in unlawful business practices in connection with its collection and disclosure of Plaintiff Hodges and California Subclass Members' private information to unrelated third parties in violation of the UCL.

255. The acts, omissions, and conduct of Defendant, as alleged herein, constitute "business practices" within the meaning of the UCL.

256. Defendant violated the "unlawful" prong of the UCL by violating Plaintiff Hodges and California Subclass Members' constitutional rights to privacy and California Penal Code § 631(a).

257. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy (including the aforementioned state privacy statutes and laws) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff Hodges and California Subclass Members.

258. The harm caused by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests other than Defendant's conduct described herein. There is no business justification for aiding and enabling the interception of private information without adequately informing users in advance.

259. As result of Defendant's violations of the UCL, Plaintiff Hodges and California Subclass Members have suffered injury in fact and lost money or property. The unauthorized access to Plaintiff Hodges and California Subclass Members' private and personal data has diminished the value of that information. Plaintiff Hodges and California Subclass Members also derive economic value from their PII and would not have provided it to Defendant or any third party for marketing purposes in the absence of consideration for that use. Thus, Defendant prevented Plaintiff Hodges and California Subclass Members from capturing the full value of their Personal Information for themselves.

260. In the alternative to those claims seeking remedies at law, Plaintiff Hodges and California Subclass Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices. The legal remedies available to Plaintiff Hodges and California Subclass Members are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also United States v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("The mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief."); *Quist v. Empire Water Co*., 2014 Cal. 646, 643 (1928) ("The mere fact that there may be a remedy at law does not oust the jurisdiction of a court of equity. To have this effect, the remedy must also be speedy, adequate, and efficacious to the end in view … It must reach the whole mischief and secure the whole right of the party in a perfect manner at the present time and not in the future."). Additionally, unlike damages, the discretion in fashioning equitable relief is very broad and can be awarded in situations where the entitlement to damages may prove difficult. *Cortez v. Purolator Air Filtration Products Co*., 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can be awarded "even absent individualized proof that the Plaintiff Hodges and California Subclass Members lacked knowledge of the overcharge when the transaction occurred."). Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc*., 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available). Furthermore, the standard for a violation of the UCL "unfair" prong is different from the standard that governs legal claims.

261. Additionally, Defendant violated the "fraudulent" prong of the UCL by disclosing sensitive personal information, PII, and PHI to the third-party advertising and analytics companies without the consent or knowledge of the users.

262. These actions were likely to deceive members of the public including Plaintiff Hodges and California Subclass Members.

263. Plaintiff Hodges and California Subclass Members were deceived into believing their private data would be kept confidential and not shared with third parties.

264. GoodRx previously stated to users that it "never provide[s] advertisers or any other third parties any information that reveals a personal health condition or personal health information."

265. GoodRx did not state that it would provide this information to third parties, in fact, it assured the complete opposite — that this information would be kept confidential.

266. However, GoodRx did share users' confidential PII and PHI with third parties, despite the explicit assurance that it would not.

267. Therefore, Plaintiff Hodges and California Subclass Members are entitled to equitable relief to restore them to the position they would have been in had Defendant not engaged in unfair competition, including an order providing for restitution, and restitutionary disgorgement of all profits paid to Defendant as a result of its unlawful and unfair practices.

COUNT VII
Violation of the Confidentiality of Medical Information Act
Cal. Civ. Code § 56.06 (West)
(California Subclass Members)

268. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

269. The Confidentiality of Medical Information Act (CMIA) is a California law that protects the confidentiality of individually identifiable medical information obtained by health care providers, health insurers, and their contractors. Among other things, the CMIA **(1) prohibits covered health care providers from disclosing medical information regarding a patient, enrollee, or subscriber without first obtaining authorization, and (2) requires covered health care providers that create, maintain, store or destroy medical information to do so in a manner that preserves the confidentiality of such information**. Cal. Civ. Code § 56 (West)(emphasis added).

270. Defendant collected medical information regarding subscriber information from Plaintiff Hodges and California Subclass Members.

271. Defendant did not seek authorization from Plaintiff Hodges and California Subclass Members to disclose said medical information to any other third-party entity.

272. Defendant then disclosed Plaintiff Hodges and California Subclass Members' private medical information to third parties via tracking technology.

273. Under the Confidentiality of Medical Information Act (CMIA), a breach of confidentiality can occur whether or not the information remains in the actual possession of the health care provider. *Vigil v. Muir Medical Group IPA, Inc*. (App. 1 Dist. 2022) 300 Cal.Rptr.3d 32, review denied.

274. GoodRx is a provider of healthcare under Cal. Civ. Code Section 56.06, subdivisions (a) and (b). The GoodRx Platform maintains various user medical information and offers software to users that maintains medical information for the purposes of allowing its users to manage their information or make the information available to a heath care provider. The

software also allows the information to be used for the diagnosis, treatment, or management of a medical condition.

275. At all relevant times, by using tracking software provided by third parties to capture and communicate Plaintiff Hodges and California Subclass Members' private information, including unique identifiers and FIDs, Defendant intentionally disclosed Plaintiff Hodges and California Subclass Members' medical information.

276. Plaintiff Hodges and California Subclass Members did not authorize Defendant to capture and transmit to third parties their private information, including PII and/or PHI.

277. Defendant breached Section 56.06(e) of CMIA by disclosing Plaintiff Hodges and California Subclass Members confidential medical information to a third party without their consent, and the personal information stored by GoodRx in a manner that did not protect the confidentiality of the information.

278. As a result of Defendant's actions, Plaintiff Hodges and Class Members have suffered harm and injury.

279. Plaintiff Hodges and California Subclass Members have been damaged as a direct and proximate result of Defendant's disclosure of their confidential medical information and are entitled to just compensation, including monetary damages.

280. Plaintiff Hodges and California Subclass Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm caused by the disclosure of their private medical information.

281. Plaintiff Hodges and California Subclass Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff Hodges and California Subclass Members in conscious disregard of

their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

282. Plaintiff Hodges and California Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT VIII
Violation of the Confidentiality of Medical Information Act
Cal. Civ. Code § 56.10 (West)
(California Subclass Members)

283. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

284. Cal. Civ. Code Section 56.10 (a) prohibits a health care provider from disclosing medical information without first obtaining an authorization unless a statutory exception applies.

285. GoodRx disclosed PII and PHI without first obtaining authorization when it disclosed Plaintiff Hodges and California Subclass Members' data to third parties and no statutory exception applies.

286. As a result of Defendant's actions, Plaintiff Hodges and California Subclass Members have suffered harm and injury.

287. Plaintiff Hodges and California Subclass Members have been damaged as a direct and proximate result of Defendant's disclosure of their confidential medical information and are entitled to just compensation, including monetary damages.

288. Plaintiff Hodges and California Subclass Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm caused by the disclosure of their private medical information.

289. Plaintiff Hodges and California Subclass Members are entitled to: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3)

statutory damages pursuant to Cal. Civ. Code Section 56.35; and reasonable attorneys' fees and other litigation costs reasonably incurred.

290. Plaintiff Hodges and California Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT IX
Violation of the Confidentiality of Medical Information Act
Cal. Civ. Code § 56.101 (West)
California Subclass Members)

291. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

292. Cal. Civ. Code Section 56.101 (a) requires that every provider of health care "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."

293. GoodRx is a provider of health care who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information.

294. GoodRx failed to maintain, preserve, and/or store medical information in a manner that preserved the confidentiality of the information because it disclosed the information to third party advertising companies, such as Google, Meta, and Criteo through tracking technology embedded on its Platform.

295. This failure to maintain preserve and/or store medical information preserving the confidentiality of such information results in a violation of Cal. Civ. Code Section 56.101(a).

296. Plaintiff Hodges and California Subclass Members are entitled to: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to Cal. Civ. Code Section 56.35; and reasonable attorneys' fees and other litigation costs reasonably incurred.

297. Plaintiff Hodges and California Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT X
Violation of the Confidentiality of Medical Information Act
Cal. Civ. Code § 56.36 (West)
(California Subclass Members)

298. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

299. Cal. Civ. Code Section 56.36(B)(3)(A) prohibits any person of entity other than a licensed health care professional from knowingly or willfully obtaining medical information for financial gain.

300. Cal. Civ. Code Section 56.36(B)(3)(B) prohibits any healthcare professional from "knowingly discloses… medical information in violation of this section…"

301. GoodRx allowed the third-party advertisers to obtain health information in violation of CMIA § 56.36 by knowingly and willfully disclosing Plaintiff Hodges and California Subclass Members' PHI to these third parties using the embedded pixels and tracking technology within the GoodRx Platform.

302. Through this knowing disclosure of health information to unauthorized third parties, GoodRx violated CMIA § 56.36.

303. Pursuant to Cal. Civ. Code Section 56.36(B)(3)(B) "[a]ny licensed health care professional, **who knowingly and willfully** obtains, **discloses**, or uses medical information in violation of this part for financial gain **shall be liable on a first violation**, for an administrative fine or civil penalty not to exceed **five thousand dollars ($5,000) per violation. (emphasis added).**

304. Plaintiff Hodges and California Subclass Members are entitled to: (1) damages of $5,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to Cal. Civ. Code Section 56.35; and reasonable attorneys' fees and other litigation costs reasonably incurred.

305. Plaintiff Hodges and California Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT XI
Violation of the California Consumers Legal Remedies Act ("CLRA")
Cal. Civ. Code §§ 1750, *et seq.*
(California Subclass Members)

306. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

307. GoodRx engaged in "unfair methods of competition and unfair or deceptive acts . . . in a transaction . . . that result[ed] . . . in the sale . . . of goods" to Plaintiffs and Class Members in violation of Cal. Civ. Code § 1750 and Cal. Civ. Code § 1770(a)(5), (7), (9), (14), (16).

308. GoodRx stated that it would protect Plaintiff Hodges and California Subclass Members' privacy interest, including pledging that it would "never provide advertisers or any other third parties any information that reveals a personal health condition or personal health information."

309. GoodRx represented that it would only use "personal medical data" such as prescription drug information in "limited cases" as necessary to fulfill the user's request.

310. Additionally, GoodRx failed to disclose it secretly allowed third parties to intercept Plaintiffs and Class Members' PII and PHI.

311. Plaintiff Hodges and California Subclass Members relied on these statements and would not have purchased GoodRx services and products had GoodRx not made these false representations.

312. Additionally, GoodRx profited directly from these sales, including through payment for these services and products, and from the data disclosed and intercepted.

313. Plaintiff Hodges and California Subclass Members are entitled to: (1) damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to Cal. Civ. Code Section 1750; and reasonable attorneys' fees and other litigation costs reasonably incurred.

314. Plaintiff Hodges and California Subclass Members seek such relief as this Court may deem just and proper.

COUNT XII
Violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act
18. Pa. C.S. § 5725 ("WESCA")
(Pennsylvania Subclass Members)

315. Plaintiff Hoza repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

316. The WESCA prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) 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 (3) 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.

317. 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 WESCA is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/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).

318. Defendant utilized the third-party tracking Pixels to intercept and collect Plaintiff Hoza and Pennsylvania Subclass Members' electronic communications with Defendant's GoodRx Platform, including Plaintiff Hoza and Pennsylvania Subclass Members' private information, PII and/or PHI.

319. To facilitate this wiretap, Defendant installed third party tracking Pixels on its GoodRx Platform.

320. Upon information and belief, Defendant knew and intended for the third-party pixels to intercept and collect Plaintiff Hoza and Pennsylvania Subclass Members' private information, procured through the wiretap, which Defendant then shared with third parties, without disclosure to or consent from Plaintiff Hoza and Pennsylvania Subclass Members.

321. Upon information and belief, Defendant intentionally used Plaintiff Hoza and Pennsylvania Subclass Members' private information, collected through a wiretap on its GoodRx Platform, for marketing and advertising purposes via Facebook.

322. Defendant intentionally intercepted Plaintiff Hoza and Pennsylvania Subclass Members' electronic communications containing their private information from its GoodRx Platform in real-time.

323. Plaintiff Hoza and Pennsylvania Subclass Members engaged in communications with Defendant through use of Defendant's GoodRx Platform.

324. Plaintiff Hoza and Pennsylvania Subclass Members had a justified expectation under the circumstances that their electronic communications would not be intercepted, shared with third parties, and used for marketing and advertising purposes.

325. Defendant employed tracking technology to intercept Plaintiff Hoza and Pennsylvania Subclass Members' electronic communications with Defendant.

326. Because the Pixel is invisible and buried in source code, Plaintiff Hoza and Pennsylvania Subclass Members were not aware that their electronic communications were being intercepted by Defendant.

327. Plaintiff Hoza and Pennsylvania Subclass Members did not consent to having their communications intercepted by Defendant.

COUNT XIII
Violation of the Florida Security of Communications Act ("FSCA")
Fla. Stat. §§ 934.01, *et seq*.
(Florida Subclass Members)

328. Plaintiff Cannell repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

329. It is a violation of the FSCA to intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any electronic communication. Fla. Stat. Ann. § 934.03(1)(a).

330. Further, it is a violation to intentionally use, or endeavor to use, "the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection[.]" Fla. Stat. Ann. § 934.03(1)(d).

331. The FSCA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a

wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce …" Fla. Stat. Ann. § 934.02(12).

332. Defendant violated § 934.03(1)(a) of the FSCA by intercepting Plaintiff Cannell and Florida Subclass Members' electronic communications when they visited the GoodRx Platform.

333. Defendant intercepted Plaintiff Cannell and Florida Subclass Members' electronic communications without disclosure or their prior consent via the third-party tracking pixels embedded in its GoodRx Platform.

334. Defendant violated § 934.03(1)(d) of the FSCA by using the unlawfully intercepted electronic communications when it shared Plaintiff Cannell and Florida Subclass Members' private information collected from its GoodRx Platform with third parties for marketing and advertising purposes.

335. Plaintiff Cannell and Florida Subclass Members had an expectation of privacy during their visits to Defendant's GoodRx Platform, which Defendant violated by intercepting their electronic communications through third party tracking pixels embedded in the GoodRx Platform.

336. As a result of Defendant's conduct, and pursuant to § 934.10 of the FSCA, Plaintiff Cannell and Florida Subclass Members were harmed and are each entitled to "liquidated damages computed at the rate of $100 for each day of violation or $1,000, whichever is higher[.]" Fla. Stat. Ann. § 934.10(d).

337. Plaintiff Cannell and Florida Subclass Members are also entitled to "reasonable attorney's fees and other litigation costs reasonably incurred." Fla. Stat. Ann. § 934.10(d).

COUNT XIV
Invasion of Privacy Under New Jersey's Constitution
(New Jersey Subclass Members)

338. Plaintiff Britton repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

339. The New Jersey Constitution, Art. 1, ¶ 1, provides that "All persons are by nature free and independent, and have certain natural and unalienable rights, among which are those of enjoying and defending life and liberty, of acquiring, possessing, and protecting property…" The New Jersey Supreme Court has "recognized a constitution-based privacy right in many contexts…" including "disclosure of confidential personal information." *Hennessey v. Coastal Eagle Point Oil Co*., 129 N.J. 81, 609 A.2d 11 (1992) (citing *Application of Martin*, 90 N.J. 295, 447 A.2d 1290 (1982).

340. In the world of the Internet, the nature of the technology requires individuals to obtain an IP address to access the Web. **Users make disclosures to ISPs for the limited goal of using that technology and not to promote the release of personal information to others**. **Under our precedents**, **users are entitled to expect confidentiality under these circumstances**." *State v. Reid,* 194 N.J. 386, 945 A.2d 26 (2008)(emphasis added). "We find that Article I, Paragraph 7, of the New Jersey Constitution protects an individual's privacy interest in the subscriber information…" *Id*.

341. Plaintiff Britton and New Jersey Subclass Members have a legally protected privacy interest, as recognized by the New Jersey Constitution, common law and the 4th Amendment to the United States Constitution.

342. Plaintiff Britton and New Jersey Subclass Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant

would violate state and federal privacy laws. Plaintiff Britton and New Jersey Subclass Members were not aware and could not have reasonably expected that Defendant would surreptitiously install software on the GoodRx Platform to automatically track and transmit to third parties each New Jersey Subclass Member's private information.

343. Plaintiff Britton and New Jersey Subclass Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information and financial information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff Britton and New Jersey Subclass Members' knowledge or consent.

344. At all relevant times, by using software to capture and communicate Plaintiff Britton and New Jersey Subclass Members' private information, including unique identifiers and FIDs, Defendant intentionally invaded Plaintiff Britton and New Jersey Subclass Members' privacy rights under the New Jersey Constitution.

345. Plaintiff Britton and New Jersey Subclass Members did not authorize Defendant to capture and transmit to third parties their private information, including PII and/or PHI.

346. This invasion of privacy is serious in nature, scope, and impact because it relates to Plaintiff Britton and New Jersey Class Members' private communications, personally identifiable information, and/or health information. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right.

347. As a result of Defendant's actions, Plaintiff Britton and New Jersey Subclass Members have suffered harm and injury, including, but not limited to, an invasion of their privacy rights.

348. Plaintiff Britton and New Jersey Subclass 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.

349. Plaintiff Britton and New Jersey Subclass Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests as a result of its intrusions upon Plaintiff Britton and New Jersey Subclass Members' privacy.

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

351. Plaintiff Britton and New Jersey Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT XV
Violations of N.Y. Civ. Rights Laws §§ 50, 51
(New York Subclass Members)

352. Plaintiff Davis repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

353. Plaintiff Davis and New York Subclass Members have a statutory privacy interest in their names, portraits, pictures, and voices under New York law.

354. Defendant knowingly used Plaintiff Davis and New York Subclass Members' names and other Private Information in the State of New York for advertising and trade purposes without first obtaining their written consent.

355. Specifically, Defendant transmitted Plaintiff Davis and New York Subclass Members' names and/or FID to third parties for targeted online advertising and other commercial purposes, as described herein.

356. Defendant's use of Plaintiff Davis and New York Subclass Members' names and Private Information did not serve any public interest.

357. The unlawful tracking of Plaintiff Davis and New York Subclass Members and disclosure of their names in connection with their Private Information has caused Plaintiff Davis and New York Subclass Members to suffer damages. This includes damage to the value of their information, which Defendant appropriated for its own enrichment. Plaintiff Davis and New York Subclass Members have also suffered nominal damages.

358. Defendant failed to protect Plaintiff Davis and New York Subclass Members' Private Information and acted knowingly when it installed third party tracking technology onto its Platform because the purpose of the pixels is to track and disseminate individual's communications with the Platform for the purpose of marketing and advertising.

359. Because Defendant intentionally and willfully incorporated the tracking pixels onto its platform and encouraged patients to use that Platform for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff Davis and New York Subclass Members.

360. Plaintiff Davis and New York Subclass Members seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs. Alternatively, Plaintiff Davis and New York Subclass Members are entitled to nominal damages.

361. Plaintiff Davis and New York Subclass Members are entitled to exemplary and/or punitive damages as a result of Defendant's knowing violations of their statutory rights to privacy.

362. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff Davis and New York Subclass Members since their Private Information is still maintained by Defendant and still in the possession of third parties and the wrongful disclosure of the information cannot be undone.

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

364. Plaintiff Davis and New York Subclass Members also seek injunctive relief to enjoin Defendant from further intruding into Plaintiff Davis and New York Subclass Members' statutory privacy interests.

COUNT XVI
Violation of the Security Breach and Notification Act
§ 12:18. The New York SHIELD Act
(New York Subclass Members)

365. Plaintiff Davis repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

366. The SHIELD Act applies to any business that owns or licenses computerized data that includes the "private information" of New York residents (including employees), regardless of whether the business otherwise operates in New York state. N.Y. Gen. Bus. Law § 899-aa (McKinney).

367. "**In determining whether information has been accessed**, or is reasonably believed to have been accessed, **by an unauthorized person or a person without valid**

authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person:

> (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
> (2) indications that the information has been downloaded or copied; or
> (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
> (d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.

Id.(emphasis added).

368. "**Any person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security** of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, **or is reasonably believed to have been, accessed or acquired by a person without valid authorization**." *Id*. (emphasis added).

369. Plaintiff Davis and New York Subclass Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal data security and privacy laws. Plaintiff Davis and New York Subclass Members were not aware and could not have reasonably expected that Defendant would

surreptitiously install software on its GoodRx Platform to automatically track and transmit to third parties Plaintiff Davis and New York Subclass Members' private information.

370. Plaintiff Davis and New York Subclass Members were under the impression that they were providing sensitive information to GoodRx and only GoodRx. Any other entities in possession of their information would be unauthorized and be considered a breach of their privacy. Plaintiff Davis and New York Subclass Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information and financial information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff Davis and New York Subclass Members' knowledge or consent.

371. At all relevant times, by using software to capture and communicate Plaintiff Davis and New York Subclass Members' private information, including unique identifiers and FIDs, Defendant intentionally invaded Plaintiff Davis and New York Subclass Members' privacy rights.

372. Plaintiff Davis and New York Subclass Members did not authorize Defendant to capture and transmit to third parties their private information, including PII and/or PHI.

373. Therefore, the acquiring of that information by third parties resulted in an unauthorized user viewing and receiving Plaintiff Davis and New York Subclass Members' personal data.

374. Under the SHIELD Act, Defendant should have notified Plaintiff Davis and New York Subclass Members immediately "in the most expedient time possible and without unreasonable delay…" N.Y. Gen. Bus. Law § 899-aa (McKinney).

375. Instead, Plaintiff Davis and New York Subclass Members remained wholly unaware that their personal data was being viewed by an unauthorized third party.

376. Plaintiff Davis and New York Subclass Members have been damaged as a direct and proximate result of third-party companies' unauthorized acquisition of their personal data and the lack of disclosure of this fact by Defendant and are entitled to just compensation, including monetary damages.

377. Plaintiff Davis and New York Subclass Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm to their security interests as a result of its intrusions upon Plaintiff Davis and New York Subclass Members' privacy.

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

379. Plaintiff Davis and New York Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT XVII
Violation of New York General Business Law § 349
(New York Subclass Members)

380. Plaintiff Davis repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

381. Defendant is considered "businesses" under New York General Business Law 349 ("GBL § 349").

382. Defendant's business acts and practices constitute unfair and deceptive practices under GBL § 349.

383. New York is a state with a public policy that protects consumers' privacy interests. These interests include protecting consumers' personal data.

384. Defendant violated GBL § 349 by intercepting Plaintiff Davis and New York Subclass Members' sensitive data PII and PHI and disclosing it to third parties without Plaintiff Davis and New York Subclass Members' consent.

385. Due to the unlawful disclosure of the PII and PHI, Defendant took money and property from Plaintiff Davis and New York Subclass Members.

386. Therefore, Plaintiff Davis and New York Subclass Members seek all available damages under state consumer protection laws, including statutory damages under GBL§ 349.

387. Plaintiff Davis and New York Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT XVIII
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. Comp. Stat. Ann. §§ 505/1, *et seq.*
(Illinois Subclass Members)

388. Plaintiff Benedict repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

389. The Illinois Consumer Fraud and Deceptive Business Practices Act (commonly known as the "Consumer Fraud Act") was enacted to give consumers a remedy for wrongs committed against them in the marketplace.

390. The Act prohibits the use of any deception, fraud, false pretenses or promises, concealment, suppression, or omission of any fact that is material to a business dealing or transaction.

391. GoodRx's conduct in this case constitutes use, deception, false promises, misrepresentation and the concealment/oppression/omission of a very critical fact — that GoodRx was sharing Plaintiff Benedict and Illinois Subclass Members' PII and PHI with third parties.

392. Accordingly, pursuant to 815 Ill. Comp. Stat. Ann. §505/1, et seq., Plaintiff Benedict and Illinois Subclass Members are entitled to recover actual damages.

393. Plaintiff Benedict and Illinois Subclass Members also seek such other relief as this Court may deem just and proper.

COUNT XIX
Negligence Per Se
(Pled in the Alternative, All Class Members)

394. Plaintiffs repeat and incorporate by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

395. GoodRx's actions were intentional, but its actions were also negligent and violated FTC statutes.

396. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" as interpreted and enforced by the FTC. Various FTC publications and orders also form the basis of GoodRx's duty.

397. The Health Breach Notification Rule (the "Rule" or the "HBNR"), 16 C.F.R. § 318, requires that any "vendor of personal health records" notify individuals when the security of their individually identifiable health information has been breached. See 16 C.F.R. § 318(a)(1). The notice "shall be sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security." 16 C.F.R. § 318.4(a).

398. GoodRx had a duty to comply with Section 5 of the FTC Act.

399. GoodRx breached its duty to comply with the FTC Act when it engaged in unfair practices of handling Plaintiffs and Class Members' PII and PHI.

400. GoodRx also breached when it violated the HBNR by failing to provide timely notice to Plaintiffs and Class Members that it shared their personal information with third parties.

401. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act and the HBNR were intended to protect.

402. GoodRx's violation of Section 5 of the FTC Act and HBNR constitutes negligence per se.

403. The injury suffered by Plaintiffs and Class Members was a reasonably foreseeable result of GoodRx's breach of its duties. GoodRx knew or should have known that the breach of its duties would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the improper disclosure of their PII and PHI.

404. Accordingly, as a direct and proximate result of GoodRx's negligence, Plaintiffs and Class Members have suffered damages including compensatory, punitive, and nominal damages.

405. Plaintiffs and Class Members also seek such other relief as this Court may deem just and proper.

COUNT XX
Common Law Negligence
(Pled in the Alternative, All Class Members)

406. Plaintiffs repeat and incorporate by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

407. GoodRx owed a duty of care to Plaintiffs and Class Members to exercise reasonable care to protect their information consistent with the various statutory requirements, industry regulations, industry guidelines, and common law.

408. GoodRx had a special relationship with its users that involved Plaintiffs and Class Members providing GoodRx with highly sensitive PII and PHI.

409. Instead of exercising care and fulfilling its duty of safeguarding this information, GoodRx voluntarily shared this information with third parties without the consent of Plaintiffs and Class Members.

410. GoodRx breached its duty of care when it shared this confidential PII and PHI to third parties, and in doing so, it was foreseeable that Plaintiffs and Class Members could suffer an injury as a result of these disclosures.

411. As a direct and proximate result of GoodRx's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT XXI
Unjust Enrichment/Quasi-Contract
(California Subclass Members)

412. Plaintiff Hodges repeats and incorporates by reference the allegations contained in paragraphs 1 through 163 as if fully set forth herein.

413. California law permits a standalone claim for unjust enrichment, allowing the court to construe the cause of action as a quasi-contract claim. *E.g., Astiana v. Hain Celestial Group, Inc*., 783 F.3d 753, 756 (9th Cir. 2015).

414. California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss. *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 599 (9th Cir. 2020).

415. California law requires disgorgement of unjustly earned profits regardless of whether a Defendant's actions caused Plaintiff Hodges and California Subclass Members to directly expend his or her own financial resources or whether a Defendant's actions directly caused Plaintiff Hodges and California Subclass Members' property to become less valuable.

416. Under California law, a stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable.

417. Plaintiff Hodges and California Subclass Members retain a stake in the profits garnered from their private information because the circumstances are such that, as between Plaintiff Hodges and California Subclass Members, on the one hand, and Defendant, on the other hand, it is unjust for Defendant to retain these profits.

418. By intercepting (and facilitating interception), disclosing, and using for targeted advertising Plaintiff Hodges and California Subclass Members' private information and bundled with their other personal information, without their permission, Defendant generated revenues and was unjustly enriched at the expense of Plaintiff Hodges and California Subclass Members. It would be inequitable and unconscionable for Defendant to retain the profit, benefit, and other compensation it obtained from using Plaintiff Hodges and California Subclass Members' private information bundled with their Facebook ID for targeted advertising.

419. Plaintiff Hodges and California Subclass Members seek an order from the Court requiring Defendant to 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.

420. Plaintiff Hodges and California Subclass 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.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of all putative Class Members, respectfully request that the Court enter judgment in favor of Plaintiffs and the Class and against Defendant as follows:

A. Certifying the Class and appointing Plaintiffs as Class Representatives;

B. Appointing Plaintiffs' counsel as Class Counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiffs and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest;

H. Awarding Plaintiffs and Class Members reasonable attorneys' fees, costs, and litigation expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury of any and all issues in this action so triable of right.

Dated: October 27, 2023

Respectfully submitted,

WHITFIELD COLEMAN & MONTOYA
Attorney for Plaintiff
201 Sevilla Ave, Second Floor
Coral Gables, FL 33134
Ph: 786-206-7874
Fax: 786-206-0660

By: */s/* Patrick S. Montoya
Patrick Montoya
Florida Bar No. 524441
Markus M. Kamberger
Florida Bar No. 111566

Jonathan B. Cohen (FL Bar No. 27620)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
3833 Central Ave.
St. Petersburg, FL 33713
jcohen@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
221 W. Monroe Street, Suite 2100
Chicago, IL 60606
gklinger@milberg.com

Daniel K. Bryson*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
900 W. Morgan St.
Raleigh, NC 27603
dbryson@milberg.com

Jacob R. McManamon
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC

3833 Central Ave.
St. Petersburg, FL 33713
jmcmanamon@milberg.com

* *Pro hac vice* application forthcoming

Attorneys for Plaintiffs and Class Members