Previn Warren
Abigail Burman
401 9th Street NW Suite 630
Washington DC 20004
Tel: 202-386-9610
pwarren@motleyrice.com
aburman@motleyrice.com

Attorneys for Plaintiff
Additional counsel on signature page.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

E.H. and C.S., *on behalf of themselves and all others similarly situated,*

Plaintiffs,

vs.

META PLATFORMS, INC.,

Defendants.

Civil Action No. 3:23-cv-4784

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs E.H. and C.S. ("Plaintiffs"), individually and on behalf of all others similarly situated, assert the following against Defendant Meta Platforms, Inc. ("Meta") based upon personal knowledge, information and belief, and/or the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. For years, Meta has surreptitiously received consumers' sensitive health information through an invisible tracker called the Meta Pixel. Third-party businesses, including health care providers and other covered entities,[1] can place the Pixel on their websites and configure it to transmit

[1] All third-party companies discussed in this Complaint are Health Insurance Portability and Accountability Act (HIPAA) covered entities and/or California Medical Information Act (CMIA) covered entities. For simplicity, the Complaint refers to each as a "Covered Entity" and collectively as "Covered Entities." *See infra* § I.B.

a vast array of identifying details about consumers to Meta. The data Meta collects includes information such as specific prescriptions, diagnoses, and symptoms that even close friends and family might not have known about—but Meta did. Furthermore, these transmissions occur even if, like Plaintiffs, consumers do not have a Facebook account. Plaintiffs bring this suit to address Meta's gross violation of their privacy and commodification of their health information.

2. Although Meta claims to be a social network, its true business is advertising, which drives the vast majority of Meta's revenue. Meta's specialty is targeted ads, for which advertisers pay a premium. Targeted ads are shown by Meta to specific audiences identified by advertisers in conjunction with Meta.

3. Meta is able to finetune audiences for advertisers by relying on enormous caches of data it constantly mines from people's Internet activity. This data concerns every aspect of people's lives—from their browsing history to their address books. The tentacles of Meta's data collection efforts are not limited to Facebook users; Meta collects extensive information about individuals who have never had, or no longer have, Facebook accounts.

4. Indeed, Meta has publicly acknowledged that it uses data from people without Facebook accounts (hereinafter "non-users") for a variety of business purposes, including product development, customer analytics reports, and security. These uses alone make it clear that non-user data is essential to oil the gears that keep Facebook profitable. But Meta's lack of internal data controls also makes it impossible for Meta to constrain non-user data to just these acknowledged uses. Instead, the non-users' data Meta collects spreads far and wide throughout Meta's systems.

5. Meta collects non-users' data through a variety of tracking mechanisms. One such mechanism is the Pixel. The Pixel is an invisible piece of code that businesses can seamlessly and secretly integrate into their websites, free of charge. Once integrated into a website, the Pixel tracks the activity of the website's users and feeds that information back to Meta.

6. Specifically, the Pixel transmits "event data," information about consumers' use of a website that not only includes their browsing behavior but, for certain kinds of websites, can also include detailed and identifiable health care information. Depending on the way a Pixel is configured, it can receive far more just someone's email, full name, and address—it can receive information as

sensitive as specific mental health symptoms. These transmissions occur even though, when coming from the website of a Covered Entity, this information is extensively protected by federal and state health care privacy laws.

7. Plaintiffs, who do not have Facebook accounts, had a broad array of identifiable health information, including their name, contact information, account creation information, and mental health questionnaire answers, transmitted while using the services of a telehealth company. Plaintiffs were not aware that their information was being sent to Meta, and they did not at any point consent to its transmission.

8. Plaintiffs and other non-users made the conscious decision to withhold their information from Meta by refusing to create Facebook accounts or by deleting their existing accounts. Nonetheless, Meta has followed these individuals into the digital equivalent of doctors' offices, support group meetings, and pharmacies.

9. Meta's illicit interception of non-users' sensitive health data violates Electronic Communications Privacy Act, the California Invasion of Privacy Act, the common law and California Constitution rights to privacy, the Unfair Competition Law, and the Consumers Legal Remedies Act, as well as unjustly enriching Meta and tortiously converting non-users' data to Meta's own use.

10. Plaintiffs seek to represent a class of people without a Facebook account whose health information was obtained without their consent by Meta from a Covered Entity. Plaintiffs seek statutory, actual, compensatory, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained and other relief the Court deems just and proper.

PARTIES

11. Plaintiff E.H. is a resident of Oklahoma.

12. Plaintiff C.S. is a resident of Massachusetts.

13. Each Plaintiff visited the website and used the services of a Covered Entity that provided online treatment to patients. Each Plaintiff created an account with that Covered Entity using their full name, address, email, and phone number. Each Plaintiff completed an intake questionnaire on the website of the Covered Entity that asked detailed questions about their health. Each Plaintiff

paid the Covered Entity, which used Plaintiffs' payments to fund its purchase of targeted advertising from Meta.

14. Plaintiffs do not currently have Facebook accounts, and they also did not have accounts at the time they used the Covered Entity's telehealth services.

15. Through the Pixel, Meta intercepted a broad array of information from Plaintiffs when they signed up for and visited the Covered Entity's website, including their full name, email address, phone number, and zip code; the fact that they had created an account; and health intake questionnaire answers.

16. Plaintiffs were unaware that this information was being intercepted and transmitted to Meta. Had Plaintiffs known of the interceptions they would not have used the Covered Entity's website. Indeed, prior to using the Covered Entity's services, Plaintiff E.H. had deleted the Facebook account they previously had, in part because of their desire to protect their personal information from Meta.

17. Plaintiffs also received less value from the Covered Entity than they paid for, because the Covered Entity was sharing their economically valuable health care data but did not provide Plaintiffs with any concomitant discount.

18. Defendant Meta Platforms, Inc. is a Delaware corporation and multinational technology conglomerate. Its headquarters and principal place of business are in Menlo Park, California.

19. In 2022, Meta's total revenue was $116.6 billion. While Meta is best known for its Instagram and Facebook social media products, the vast majority of its revenue actually comes from its advertising business, which sells ads that are placed on both its products and on other companies' products.

JURISDICTION AND VENUE

20. Jurisdiction is proper pursuant to 28 U.S.C. § 1332(d) because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 members of the putative class defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of the Defendant.

21. This Court has general personal jurisdiction over Defendant Meta because Defendant's principal place of business is in California.

22. Additionally, a substantial part of the events and conduct giving rise to Plaintiffs' and the Class and Subclass' claims occurred in California.

23. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), (c), and (d) because Defendant Meta transacts business in this District and a substantial portion of the events giving rise to Plaintiffs' and the Class and Subclass' claims occurred in this District.

FACTUAL BACKGROUND

I. Meta illicitly intercepted Plaintiffs' and Class Members' sensitive health information.

a. Meta uses the Pixel to intercept non-users' health information.

24. A pixel is a snippet of code, invisible to the naked eye, which can easily be added to any website.

25. A pixel is distinct from a cookie, though both are used by companies to collect personal data. A cookie is a small piece of text that is downloaded to a users' browser as they browse the Internet, carrying information about a users' interaction with the website that set the cookie.

26. The Meta Pixel is offered by the company as an ostensibly "free" analytics and advertising tool—not accounting for its enormous costs to consumer privacy.

27. The Meta Pixel has become ubiquitous across the Internet. It appears on over two million websites, including approximately 44% of the sites visited by non-users.

28. Once activated, the Pixel functions as an all-seeing eye, transmitting consumers' data to Meta in real time, regardless of whether or not those consumers have Facebook accounts.

29. The unit for the Pixel's data transmissions is called an "event." Events can be triggered when a person navigates to a page or takes any other action on a site, including clicking on page elements, adding something to their cart, scrolling to a certain point on the page, or filling out survey questions.

30. By default, an event transmission includes data about the page that was being viewed when the event was triggered and the IP address of the person browsing. But Meta offers businesses who use the Pixel the ability to collect far more than this basic event data. For instance, it offers a feature called "automatic advanced matching." This feature automatically identifies and sends to Meta information from form fields and other website features. Such data can include consumers' full names, emails, phone numbers, birthdays, addresses, and other unique identifiers generated by the business such as loyalty numbers. This information makes other data transmitted through an event identifiable to a particular consumer (who, again, may be a non-user).

31. While such data is nominally "hashed" or encrypted, the hashing can easily be undone with free, widely available tools. As such, none of the data collected by the Pixel is actually de-identified; all of it can be linked to specific individuals either alone or in combination with other information.

32. In an even greater privacy violation, Meta allows businesses to transmit "custom" event data. These data parameters are set by businesses and, in the case of health-related businesses, can include intimate details about treatment that are protected by law and that a user believes to be private. For example, the Pixel can transmit consumers' answers to questions asking if they have taken specific medications or experienced specific symptoms.

33. In the context of Covered Entities, this means that the data shared by the Pixel often goes beyond simply showing that a consumer browsed a Covered Entity's website. By sharing that a consumer filled out a form, created an account, answered a questionnaire, and/or engaged in other affirmative acts, event data conveys to Meta that the consumer was actually seeking to use the Covered Entities' service—thereby revealing their medical history and treatment decisions.

34. It is nearly impossible for an ordinary consumer to know whether a Pixel is being used on a website. Pixels, including Meta's, are intentionally designed to be invisible to the naked eye, and

their data transmissions are not apparent from a website's URL or other commonly visible data. The only way to know that a Pixel is tracking your use of a website is to install specialty software or use browser tools that are intended for developers to monitor and log site transmissions. Even if a user was able to determine that a Pixel is being used, it is also extremely difficult for them to understand the breadth of the data the Pixel is collecting. The transmissions are not in plain English; they consist of specialized abbreviations, coding terms, and "hashed" values that seem nonsensical to the layperson. So, to fully track Meta's data interceptions, a consumer would have to access the source code for the website they were using, monitor the site's activity, and decipher terms of art specific to the Pixel.

b. Meta intercepted Plaintiffs' and Class Members' health information.

35. Cerebral is a telehealth company that provides behavioral and medication treatment to patients. From October 2019 to January 2023, Cerebral surreptitiously placed the Pixel on its site. By doing so, Cerebral allowed Meta to intercept consumers' sensitive medical information in real time, despite its obligations to treat such information with the highest degree of care.

36. Like a bug hidden in the ceiling of a therapist's office, Meta used the Pixel to intercept and eavesdrop on Plaintiffs' highly sensitive and identifiable health disclosures.

37. The information the Pixel intercepted was exhaustive. It included the fact that Plaintiffs had created an account, first name, last name, phone number, email, and zip code. This type of account creation data is in and of itself identifiable health information, as accounts were only created by people seeking treatment from Cerebral (rather than casually browsing its site).

38. But the Pixel also intercepted answers to intake questionnaires that Cerebral patients had to complete as part of the sign-up process, such as how often in the previous two weeks they had felt "down, depressed, or hopeless." Like the account creation data, the questionnaire responses showed that Plaintiffs were actively using Cerebral's services, while also broadcasting Plaintiffs' specific symptoms directly to Meta.

39. Plaintiffs are not the only non-users whom Meta has ensnared in its vast commercial surveillance operation. The Pixel on Cerebral's website intercepted the information of more than 3 million patients.

40. Nor were the Pixel's interceptions limited to Cerebral patients. The Pixel consumed data across a wide swath of Covered Entities' websites. For example, the Pixel intercepted identifying information and a range of other protected data from more than 100,000 patients of Monument, an alcohol use disorder telehealth company. That data included the fact that people were signing up for a plan and their answers to a detailed intake questionnaire about their mental health and drinking habits.

41. Similarly, a review of the top 100 hospitals in America found that one third of their websites had the Pixel, which transmitted visitors' IP addresses whenever they clicked a button to schedule an appointment.

42. Class Members are other non-users like Plaintiffs, whose extremely sensitive health information was tracked and transmitted to Meta through the Pixel. Decisions about whether and how to seek medical treatment are deeply personal. But without their knowledge or consent, Plaintiffs and Class Members were making these decisions in full view of Meta.

43. Meta's violation of Plaintiffs' and Class Members' privacy is especially egregious because they either never signed up for Facebook accounts or chose to delete their accounts—refusing to give Meta a window into intimate details of their lives only to have Meta illicitly create one.

c. Plaintiffs and Class Members did not consent to Meta's interception of their health information.

44. Plaintiffs and Class Members are non-users, which again means they do not maintain Facebook accounts. As such, there is no argument that they somehow assented to the interception of their sensitive health data by agreeing to Facebook's terms of service.

45. Importantly, even if Plaintiffs or Class Members *had* agreed to Meta's terms of service, they would not have consented to these interceptions by virtue of that agreement. Meta's Privacy Policy statement generically states that Meta receives "information using cookies and similar technologies, such as the Meta pixel or Social plugins, when you visit other websites and apps that use Meta Products." No reasonable person would understand this to mean that Meta intercepts sensitive, identifiable health information from health care providers. That's especially so given Meta's Data Policy, which informs consumers that other companies must "have lawful rights to collect, use and share your data before providing us with any data" and must "adhere to strict confidentiality

obligations in a way that is consistent with this Data Policy and the agreements that we enter into with them."

46. Moreover, until the beginning of 2023, Meta's California-specific privacy notice stated that it would collect "Data with special protections," which would include Plaintiffs' and Class Members' health information, only "if you choose to provide it." Plaintiffs and Class Members did not choose to provide Meta with their extensively protected data. Indeed, they were never even given the opportunity to make such a choice.

47. Meta acknowledges that the use of Pixel tracking requires additional consent from users beyond merely using or benefitting from Meta's services. Meta's business terms of service state that, before using the Pixel, a business must obtain "all necessary consents from users," and they further require businesses to represent that they "have all of the necessary rights and permissions and a lawful basis" to collect the information that the Pixel intercepts. Again, no such consents, rights, or permissions were obtained from Plaintiffs or Class Members.

d. Plaintiffs and Class Members reasonably expected their health information to remain private.

48. The sensitive health data of Plaintiffs and Class Members is protected by overlapping federal and state regulations. Relevant here are the HIPAA privacy rule and the California Medical Information Act (CMIA). As defined herein, each Covered Entity is subject to at least one of these regulations, if not both. The privacy rule and CMIA all require specific authorizations before Covered Entities can release or obtain health information—authorizations that Plaintiffs and Class Members did not provide. These privacy protections, combined with the highly sensitive nature of the data obtained by Meta, created a reasonable expectation by Plaintiffs and Class Members that this data would remain private.

49. At the federal level, the HIPAA privacy rule sharply limits the disclosure of protected health information ("PHI") by HIPAA-covered entities and their business associates (collectively, "regulated entities") absent specific authorization carried out according to the HIPAA regulations. Because Meta provides analytics and marketing tools to HIPAA-Covered Entities through the Pixel,

Meta is a "business associate" for the purposes of HIPAA. However, Meta never entered into a business associate agreement with any Covered Entities, as required by HIPAA to permit PHI sharing.

50. Regulated entities can only disclose PHI as permitted by HIPAA, which requires patient authorization for most releases of PHI, and specifically requires patient authorization "for any use or disclosure of protected health information for marketing." 45 CFR §§ 164.502(a)(3), 164.508(a)(3), 164.508(c)(vi). Among other requirements, an authorization must be signed and dated by the patient.

51. Notably, it is *not* sufficient authorization for a regulated entity to "inform[] individuals in its privacy policy, notice, or terms and conditions of use" that it plans to share their information with ad brokers through tracking technology. Moreover, the Department of Health and Human Services has recently explained that regulated entities are "not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors," meaning such disclosures violate the HIPAA privacy rule.[2]

52. The information Meta intercepted from Plaintiffs and Class Members constituted PHI: (a) it related to the past, present, or future physical or mental health or condition of users; the provision of health care to users; and the past, present, or future payment for the provision of health care to users; and (b) it was connected with such identifying details as users' IP addresses and emails.

53. Furthermore, *all* identifying information "collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the [identifying information], such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's [identifying information] through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the

[2] Office of Civil Rights, Department of Health and Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

Covered Entity), and thus relates to the individual's past, present, or future health or health care or payment for care."[3]

54. California's medical information privacy law, CMIA, further protects consumers beyond the federal floor created by HIPAA. CMIA extends to "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor;"[4] "any business that "maintain[s] medical information . . . in order to make the information available to an individual or to a provider of health care" or offers consumer hardware or software that does the same; and"[a]ny business that offers a mental health digital service to a consumer." CCC §§ 56.06(a)-(b), 56.101(a)-(b), 56.101(d).

55. Entities that are covered by CMIA generally cannot release medical information without patients' written authorization. And, absent express authorization, they are explicitly forbidden from "intentionally . . . us[ing] for marketing, or otherwise us[ing] medical information for a purpose not necessary to provide health care services to the patient." CCC § 56.10(d).

56. The information Meta intercepted from Plaintiffs and Class Members constituted medical information because it came from a health care provider, as defined by CMIA; was related to patients' medical history, condition, and treatment; and contained individually identifying details such as patients' full names, contact information, and IP addresses.

57. Meta affirmatively avails itself of and thereby subjects itself to California law, maintaining its principal place of business in California.

58. By using the Pixel to intercept Plaintiffs' and Class Members' medical information, Meta knowingly participated with health care entities in violating CMIA.

59. At no point did Plaintiffs or other Class Members complete the authorizations that were necessary for their information to be lawfully intercepted. The web of statutory and regulatory protections set forth above thus should have ensured that their sensitive health data would not be shared with Meta.

---

[3] *Id.*

[4] "Contractor" is defined as a "medical group, independent practice association, pharmaceutical benefits manager, or a medical service organization and is not a health care service plan or provider of health care." CCC § 56.06(d).

e. Meta knowingly collects sensitive health information through the Meta Pixel.

60. Meta has long known that its tracking technologies intercept health information. And it has long known that the strategies it uses to combat the interception of health information are ineffective.

61. Consumer advocates have expressed concern about the secret transmission of sensitive health data from third-party services to Meta—and Meta's use of that data for marketing.

62. An investigation by the New York State Department of Financial Services conducted from 2019 to 2021 found that Meta routinely obtained health information from other companies' apps. The department found that Meta "does little to ensure that developers are actually aware of [the prohibition on transmitting sensitive health information] or to make particular note of it when the developers create the Custom Events that result in the transmission of sensitive data."

63. In response to that investigation and the negative publicity that followed, Meta touted its development of a "Health Terms Integrity System" to filter out sensitive health information and prevent it from being used in its ad-ranking and optimization systems. This system works by reviewing the discrete data of each Pixel transmission and comparing it to a block list of health-related-terms.

64. However, in practice, this system often does not work at all. As of 2021, the block list only encompassed terms in English. And in 2022, investigative journalists found that Meta failed to block the collection of data that was obviously health-related, such as information from sites with URLs that included "post-abortion," "i-think-im-pregnant," and "abortion-pill."[5]

65. Even when it does work as intended, Meta's system is underinclusive by design. By reviewing only discrete event data, the system does not take into account the broader context of data transmissions, which can be highly revealing. Consider when a user enters their email address into a health company's sign-up form. This is in and of itself identifiable health information, as it connects a user's identity to their search for treatment. But Meta's system would not flag this as a transmission of health care information if the event data is a user's email address and the URL of the form does not

[5] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, The Markup (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

contain any health-care related words. In this way, large amounts of sensitive health information are transmitted to Meta without even the possibility of restriction.

66. But Meta not only fails to stop the collection of sensitive health information, it also actively pushes the Pixel on health care businesses—the very companies that are most likely to be Covered Entities and transmit sensitive health information. Meta maintains a specialized landing page for advertisers in the health industry, has a policy specific to health ads, and maintains a page highlighting ad campaigns from health-related companies. These pages are reflective of Meta's concerted push to attract health care advertising clients in the last few years, with at least 30 employees dedicated to working with health and pharmaceutical companies. Between 2017 and 2019, health and pharmaceutical companies nearly tripled their ad spending on Facebook mobile ads alone, spending nearly $1 billion in 2019.

67. Meta does not cut off a business's access to the Pixel even when it knows the company is transmitting health information. For example, Meta once flagged that Monument, the online substance use provider that was transmitted its members' specific symptoms to Meta, was improperly sending sensitive health data via the Pixel. But the company was able to simply determine for itself that no sensitive health information was being transmitted and continue its Pixel transmissions, without Meta ever challenging this obviously absurd conclusion. In situations like these, Meta has acted in blatant disregard of the obviously deeply sensitive nature of the information transmitted to it.

68. Furthermore, Meta is unable to cordon off sensitive health information from the other data it holds. As a leaked internal memo explains, putting data into Meta's systems is like "pour[ing] . . . ink into a lake of water . . . . How do you put that ink back in the bottle?" Similarly, in a deposition, two highly experienced Facebook engineers stated that there is typically no documentation of what happens to *any* individuals' data once it enters Facebook's systems.[6]

69. Once collected, Plaintiffs' information became part of Meta's data horde, used as needed to power Meta's operations and serve its business customers.

[6] Sam Biddle, *Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data*, The Intercept (Sept. 7, 2022), https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/.

f. Meta has an extensive history of violating non-users' privacy.

70. Meta has a storied history of deceiving the public about its collection and use of non-users' data. This dates back to the company's earliest years, when it began to track people's off-site browsing activity.

71. In 2007, Meta (then Facebook) launched the beacon, a piece of code that would transmit browsing behavior on other sites back to Meta. In an interview with the New York Times, Meta explicitly denied the use of beacons to share any information with Facebook without people's consent. However, the same day the article was published, a computer scientist found that beacons in fact transmitted data about people who had no Facebook account at all. A few days later, Meta acknowledged its initial misrepresentation.

72. The next big scandal relating to Meta's tracking of non-users came in 2011, when a consumer complaint was made to Ireland's data protection authority. The complaint alleged that Meta was amassing "shadow profiles" on non-users—data about non-users gleaned from information that users and businesses provide to the site.

73. The complaint rapidly sparked public concern, motivated by the fact that, as members of Congress explained in a 2011 letter, "[w]ith more than 800 million active users and an untold number of non-users visiting Facebook or partnering websites every day, your company has the opportunity to collect vast amounts of data about an enormous number of people." In response, Meta flatly denied the existence of "shadow profiles."

74. But, in 2013, a bug exposed millions of people's contact information, including contact information that was "not connected to any Facebook users." This fact contradicted the company's representations that it did not retain information about non-users. Further underscoring Meta's flagrant disregard for the privacy of non-users, Meta only notified users about the breach.

75. Then, in 2015, a Belgian court ruled that Meta was illegally tracking non-users' browsing data through cookies and the Pixel. The Belgian ruling was quickly followed by rulings from the French and Spanish data protection authorities penalizing Meta for illicitly collecting browsing data from non-users.

76. However, it was not until 2018 that Meta finally publicly admitted that it collects off-site browsing information about non-users. As one journalist explained, this practice undermined all of Meta's "repeated cries that people who use the internet—not even just people who use Facebook—have control over their data . . . . To opt out of Facebook's data collection, first you'd have to even know a service you're not on is collecting your information, and then you'd have to sign up for that service to opt out of it."

77. Meta instituted transparency measures for account-holders' off-site data in 2019, allowing them access to high level-summaries of how their off-Facebook browsing history has been tracked in the last 180 days. But to this day, people without Facebook accounts, like Plaintiffs and Class Members, still have no way to track the data that Meta receives about them through the Pixel.

II. Health Data is a valuable commodity.

78. The information that Meta illicitly amassed from Plaintiffs and Class Members was tremendously valuable.

79. Personal data is now the most valuable commodity in the world, "the new oil" of the tech economy.

80. Health data, like that intercepted from Plaintiffs and other non-users, is particularly valuable. Medical data is a multi-billion-dollar market, with a single medical record having a value of approximately $1,000.

81. The value of medical data is even higher when individuals can set the price for their own data. More than half of Americans would demand more than $100,000 to give Meta access to their health data, while less than four percent of Americans would share health data with Facebook for free.

82. Plaintiffs placed significant, quantifiable value on the data intercepted by the Pixel.

83. Consumer data is also specifically valuable to Meta. Meta has directly participated in the market for consumer data, at one point paying people $20 a month for full access to their browsing and phone data, and purchasing bulk quantities of data from third-party data brokers.

84. More fundamentally, consumer data drives the value of Meta's ad-supported business model. Meta's ad targeting models utilize over 15,000 data points, each of which is fed by thousands

of inputs. Meta's machine learning algorithms use this data to surgically carve up the Internet, offering advertisers the ability to reach hyper-specific micro-demographics. Targeted ads purchased from Meta are particularly in demand and generate more than twice the revenue for Meta as compared to non-targeted ads, in part due to the precision of Meta's targeting.

85. The enormous reservoirs of data required to fuel targeted ads are thus Meta's most valuable asset. Meta values its ability to track user activity so highly that it took out a full-page newspaper ad to protest Apple's attempt to limit it. Apple's decision ultimately cost Meta over $10 billion in annual revenue.

86. Meta's supply of data must be constantly replenished in order for its ad targeting models to remain up to date. As Meta has explained, "[m]achine learning is a system that learns as it receives new data." Without new data, Meta's ad models would fail to target with precision, leading advertisers to turn elsewhere.

87. This fundamental (and fundamentally problematic) business model has led Meta to harvest the data of non-users like Plaintiffs and Class Members to power its broader ad targeting infrastructure and sharpen its inferences about which people are most likely to respond to which ads. Again, non-users are individuals who have attempted to avoid Facebook's all encompassing data collection—but whom Facebook simply refuses to leave alone. Meta's secret exploitation of Plaintiffs' and Class Members' deeply private medical information was intentional, not mere corporate carelessness.

III. Meta relies on Pixel data from non-users for a wide variety of business purposes.

88. Meta benefits in a variety of ways from the data it collects from non-users like Plaintiffs and Class Members.

89. First, Meta uses this data to power and improve the machine learning algorithms that allow it to sell ads targeted to its users. Specifically, Meta uses non-user data to identify Facebook users with similar data and better predict those users' interests. To give a simplified example, if Meta learns through a Pixel that a non-user who has signed up for a certain website is 25 years old, that information signals to Meta that users who are 25 might be interested in the site. Meta can charge

advertisers additional money because of the extra, non-user-derived layer of knowledge that was used to target the ad. It's all grist for the billion-dollar ad mill.

90. Machine learning inferences can also inform more insidious targeting. One writer described how, after seeking treatment for depression, she was flooded with Facebook ads suggesting she had other, increasingly serious mental health diagnoses—ads that in turn worsened her mental health.

91. Second, in an ironic twist, Meta's targeted ads are sometimes targeted to non-users themselves. Meta maintains a system called "Audience Network ads" that allows advertisers to place Meta-targeted ads on products that Meta does not own. In 2016, Meta announced that it would allow advertisers to target such ads to non-users, using data collected from the Pixel and other tracking technologies (including data from non-users). Meta has never formally ended this program.

92. Third, non-user data is used to generate analytics reports that Meta shows to businesses that use the Pixel. These analytic tools serve several core business purposes for Meta. Their availability incentivizes businesses to adopt the Pixel and other Meta tracking tools, allowing Meta to vacuum up valuable data. Moreover, because these tools can be used to inform targeting and purchasing decisions, they encourage businesses to buy ads from Meta.

93. In addition to the above, Meta uses non-user data for a host of other purposes, including security and other internal product development efforts.

94. None of these benefits accrued to Plaintiffs and Class Members, who do not even have Facebook accounts.

95. Meta's vast well of Pixel data has been instrumental in its dominance of the online advertising market. Because of the Pixel's ubiquity on the web, Meta can target its ads in far more sophisticated ways than its competitors, with an attendant increase in value. Meta's reach also makes it almost impossible for competitors to enter the market.

96. While Meta long proclaimed that Facebook is "free and always will be," its hidden, violative data collection practices have a very real cost for Plaintiffs, Class Members, and all users of the Internet.

STATUTE OF LIMITATIONS

97. The applicable statutes of limitations have been tolled pursuant to the discovery rule and by Meta's knowledge and concealment of its misconduct via the misrepresentations and omissions alleged herein.

98. Plaintiffs and Class Members were not aware that their sensitive health information had been intercepted by Meta. The interception occurred via technology that is specifically designed to be invisible to visitors of a website, and Plaintiffs and Class Members could not have identified this information through reasonable diligence.

99. This is particularly true because Plaintiffs and Class Members do not have Facebook accounts, and so could not view any records of the Pixel transmissions of their data.

100. Furthermore, Meta knowingly, actively, affirmatively, or negligently concealed its collection and use of Plaintiffs' and Class Members' sensitive health data.

101. Meta did not inform Plaintiffs and Class Members that their tracking technologies were intercepting sensitive, legally protected health data, and that it was not requiring third parties to comply with applicable state and federal regulations before sharing data with Meta.

CLASS ACTION ALLEGATIONS

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

Class: All residents of the United States who are not Facebook users, about whom Meta obtained the following from a Covered Entity: (a) personally identifying information and (b) the fact that an account with a Covered Entity was created; personal information entered during the process of creating an account with a Covered Entity; answers to questionnaires; shopping cart and checkout data; booking and appointment information; billing information; and/or other information that in combination with personally identifying information constitutes protected health information.

Subclass: All members of the Class who paid a Covered Entity for their goods and services.

103. Numerosity: The exact number of members of the Class and Subclass is unknown and unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable because the Class likely consists of hundreds of thousands of individuals. Members of the Class and Subclass can be ascertained through Meta's records.

104. Predominant Common Questions: The Class and Subclass's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class and Subclass include, but are not limited to, the following:

- Whether Meta acquired Class and Subclass Members' health data;
- Whether Class and Subclass Members' sensitive, identifiable health information has economic value;
- Whether Meta violated the Electronic Communications Privacy Act
- Whether Meta violated the California Invasion of Privacy Act;
- Whether Meta intruded upon Class Members' seclusion;
- Whether Meta invaded Class Members' privacy;
- Whether Meta was unjustly enriched by Class Members' health data;
- Whether Meta tortiously converted Class Members' health data;
- Whether Meta violated the Unfair Competition Law;
- Whether Meta violated the Consumer Legal Remedies Act;
- And Whether Meta has any argument that Class and Subclass Members somehow authorized the release of their sensitive, identifiable health information, despite not maintaining Facebook accounts.

105. Typicality: Plaintiffs' claims are typical of the claims of the other members of the Class and Subclass, arising from the same conduct by Defendants and based on the same legal theories. Plaintiffs and members of the Class and Subclass are people without a Facebook account whose data was obtained by Meta from a Covered Entity without their consent.

106. Adequate Representation: Plaintiffs have and will continue to represent and protect the interests of the Class and Subclass. Plaintiffs raise the claims that could be reasonably expected to be

raised by members of the Class and Subclass. Furthermore, Plaintiffs have no interests that are antagonistic or adverse to the interests of the Class and Subclass, and Defendant does not have any defenses that are unique to Plaintiffs. Plaintiffs' counsel is competent and experienced in complex litigation and class actions, including complex litigation related to technology companies. Plaintiffs' counsel also has no interests that are adverse to the interests of the Class or Subclass.

107. Substantial Benefit: Certification of this class action would substantially benefit the class 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 and Subclass is impracticable. Class Members' injuries are likely insufficient to warrant individual action, so denial of class certification would unfairly advantage Defendants' unlawful conduct. Hearing all Class Members' claims separately would also burden the Court, requiring it to expend judicial resources on duplicative management decisions and adjudications, rather than taking advantage of the economies of scale created by comprehensive supervision by a single court.

108. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on subsequent developments, and/or following additional investigation and discovery or other developments.

California Law Applies

109. California law applies to the claims of Plaintiffs and Class Members.

110. Meta has its principal place of business in California and conducts substantial business in the state. The decisions described and conduct underlying the allegations within this Complaint were substantially made, carried out by, and beneficial to Meta's business in California, and had a substantial effect on California's economic marketplace.

111. The products and websites described in this Complaint, including the omissions and misrepresentation contained therein, were substantially developed and maintained in California.

112. California thus has a greater material interest than any other state in having its law applied to the claims against Defendant.

CLAIMS FOR RELIEF

COUNT 1

Violation of Electronic Communications Privacy Act ("ECPA")

On Behalf of Plaintiffs and the Class

(18 U.S.C. §§ 2510, *et seq.*)

113. All preceding factual statements and allegations are incorporated herein by reference.

114. The ECPA prohibits the unauthorized interception of the contents of an electronic communication. 18 U.S.C. § 2511.

115. The data transmissions between Plaintiffs and Class Members on the one hand, and Covered Entities on the other, are communications for the purpose of the ECPA. 18 U.S.C. § 2510(12).

116. Through the Pixel, Meta contemporaneously acquired the contents of communications between Plaintiffs and Class Members and Covered Entities.

117. Meta's interceptions were intentional. The foundational purpose of the Pixel is to clandestinely intercept communications made on third-party websites and share their contents with Meta for use in Meta's own business operations.

118. The intercepted communications include but are not limited to the following content:

a. The content of Plaintiffs' and Class Members' communications regarding their registrations for Covered Entities' services and tools, including the fact that they were creating an account and the contact information they provided.

b. The contents of Plaintiffs' and Class Members' communications with Covered Entities about their specific symptoms and conditions.

c. Full-string URLs that contain information concerning the substance, purport, or meaning of Plaintiffs' and Class Members' communications with Covered Entities.

119. These communications constitute PHI and individually identifiable medical information.

120. The following devices, as defined by 18 U.S.C. § 2510(5), were used in the interceptions:

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices:

c. Meta's servers;

d. The servers of the Covered Entity webpages that have the Meta Pixel;

e. The Pixel source code used to acquire Plaintiffs' and Class Members' communications.

121. Meta is not a party to Plaintiffs' and Class Members' communications with the Covered Entities.

122. Neither Plaintiffs and Class Members nor Covered Entities consented to Meta's interceptions of these communications.

123. Plaintiffs and Class Members did not consent to Meta acquiring their communications with Covered Entities.

124. Meta did not obtain legal authorization from Plaintiffs and Class Members to obtain these communications, as required by HIPAA and CMIA. Nor did Meta require the Covered Entities to obtain legal authorization to share these communications.

125. The Covered Entities did not validly consent to Meta's interception of Plaintiffs' and Class Members' health care communications. Covered Entities' use of the Pixel alone is insufficient to show that they actually consented to Meta's interception of statutorily protected health care communications. Furthermore, under state and federal law, Covered Entities were prohibited from sharing Plaintiffs' and Class Members' communications without the Plaintiffs' and Class Members' authorization.

126. Meta's purpose in acquiring the contents of Plaintiffs' and Class Members' communications was tortious, criminal, and designed to violation state statutes. These unlawful purposes include:

a. The unauthorized acquisition of individually identifiable health information, which is tortious regardless of the means used;

b. The criminal acquisition and use of individually identifiable health information without authorization, in violation of HIPAA. 42 U.S.C. §§ 1320d-6(a)(2), (b)(3);

c. Intrusion upon Plaintiffs' and Class Members' seclusion;

d. Violation of the UCL;

e. Violation of the CLRA;

f. Violation of the California Constitution's right to privacy;

g. Aiding and abetting violation of CMIA;

h. Violation of Cal. Penal Code § 484 for statutory larceny.

127. For Meta's violations set forth above, Plaintiffs and Class Members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any profits made by [Meta] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

128. Unless enjoined, Meta will continue to commit the violations of law alleged here. Plaintiffs want to continue to communicate with Covered Entities through online platforms but have no practical way of knowing if their communications are being intercepted by Meta, and thus continue to be at risk of harm from Meta's conduct.

129. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members seek monetary damages for the greater of (i) the sum of the actual damages suffered by the Plaintiffs and Class Members and any profits made by Meta as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

COUNT 2

Violation of California Invasion of Privacy Act ("CIPA")

On Behalf of Plaintiffs and the Class

(Cal. Penal Code §§ 630, *et seq.*)

130. All preceding factual statements and allegations are incorporated herein by reference.

131. CIPA is "intended to protect the right of privacy of the people of this state" against "the development of new . . . techniques for the purpose of eavesdropping upon private communications and . . . the invasion of privacy resulting from the . . . increasing use of such . . . techniques." Cal. Penal Code § 630.

132. Meta's interception and use of users' data through the Pixel violated § 631 of CIPA, the wiretapping provision. In relevant part, this provision prohibits willfully attempting to learn the contents or meaning of a communication in transit without the consent of all parties, and using or attempting to use information obtained as a result of those willful attempts. Cal. Penal Code § 631(a).

133. Meta's Pixel intercepted, and transmitted to Meta, communications sent from Plaintiffs to Covered Entities. In fact, the explicit purpose of Meta's Pixel is to intercept communications as they are occurring and surreptitiously transmit them to Meta. Meta then willfully attempted to learn the contents of these communications and used that information for its own commercial gain.

134. The same is true for communications sent by Class Members to Covered Entities. Meta's Pixel intercepted and transmitted these communications, and Meta then used the information contained therein for its commercial gain. Upon information and belief, certain of these communications were received by Meta at its headquarters in California.

135. Meta cannot be considered a party to the communications that it intercepted. Rather than simply intercepting and storing the information it collected via Pixel on the Covered Entities' behalf, Meta processed the data, using it for a variety of internal purposes.

136. The data that Meta intercepted was "content" within the meaning of § 631(a) because it included the substance of Plaintiffs' and Class Members' communications with covered entities, such as the buttons they were clicking, the answers they were inputting, and the services they were using.

137. Meta's interception and use of users' data through the Pixel also violated CIPA's eavesdropping provision, § 632(a). The eavesdropping provision prohibits recording or eavesdropping on confidential communications without the consent of all parties. Cal. Penal Code. § 632(a).

138. Plaintiffs' and Class Members' communications with Covered Entities were confidential communications. Unlike online communications more generally, these communications

were made for the purpose of obtaining health care and were related to health status and treatment. The communications also revealed facts about Plaintiffs' and Class Members' medical history and treatment that were protected by state and federal privacy regulations. Plaintiffs and Class Members reasonably expected their transmissions of information to be confined to their health care providers and did not reasonably expect that they would be overheard or recorded.

139. Without the knowledge of Plaintiffs and Class Members, Meta received the sensitive, identifiable medical information that Plaintiffs and Class Members communicated to Covered Entities.

140. Plaintiffs and Class Members did not consent to Meta's interception and eavesdropping through the Meta terms of service and privacy policies.

141. Meta is headquartered in California, designed and carried out its scheme to intercept Plaintiffs' and Class Members' data from California, and has adopted California substantive law to govern its relationship with its users.

142. Plaintiffs and Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of $5,000 per violation or three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as other equitable relief as may be proper.

COUNT 3

Invasion of Common Law Right to Privacy – Intrusion Upon Seclusion

On Behalf of Plaintiffs and the Class

143. All preceding factual statements and allegations are incorporated herein by reference.

144. A claim for intrusion upon seclusion requires pleading that the defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs had a reasonable expectation of privacy; and that the intrusion was highly offensive to a reasonable person.

145. Meta's collection of Plaintiffs' and Class Members' user data—which included their identifying information; information about specific symptoms, diagnoses, and treatments; information demonstrating that they were actively seeking covered entities' services—was an intentional intrusion upon their seclusion. This data was highly sensitive and legally protected, and Plaintiffs and Class Members did not consent to its collection by Meta.

146. Plaintiffs and Class Members had a reasonable expectation of privacy in this data, particularly because it included identifiable health information. First, Plaintiffs and Class Members did not consent to Meta collecting their data. In fact, this information is so sensitive that Meta (falsely) publicly disclaims collecting it at all. While Meta claimed that it would not acquire or use data in any way not described in its privacy policy, and any partners using tools like the Pixel must have "lawful rights" to the data, this was—as Meta knew—untrue. Second, the specific type of data that Meta collected, identifiable medical information, carries with it a particularly strong expectation of privacy because of the strong legal prohibitions on its disclosure.

147. Meta's intrusion on Plaintiffs and Class Member's privacy would be highly offensive to a reasonable person. Medical treatment decisions are intensely private, and effective treatment depends on the trust that confidentiality builds between providers and patients. Meta stripped Plaintiffs and Class Members of this confidentiality, treating them like experiments to be constantly observed.

148. Plaintiffs and Class Members seek appropriate relief for the injury to their privacy interests, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests and disgorgement of profits made by Meta as a result of their intrusions upon Plaintiffs' and Class Members' privacy.

149. Plaintiffs and Class Members are also entitled to punitive damages. By intercepting identifiable health information—even after it was aware of the sensitive nature of the information—and turning that information into a profit center, Meta intentionally and maliciously violated Plaintiffs' and Class Members' privacy, and further violated the state and federal governments' strong public policy in favor of privacy. Punitive damages are needed to deter Meta and other online advertising companies from engaging in similar conduct in the future.

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

COUNT 4

Invasion of Constitutional Right to Privacy

On Behalf of Plaintiffs and the Class

(Cal. Const., Art. 1, § 1)

151. All preceding factual statements and allegations are incorporated herein by reference.

152. Article I, Section 1 of the California Constitution states 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."

153. To state a claim for invasion of privacy in violation of the California Constitution, a plaintiff must show that they possess a legally protected privacy interest, they maintain a reasonable expectation of privacy, and the breach of their privacy was highly offensive.

154. Meta's collection of Plaintiffs' and Class Members' user data—which included their identifying information; information about specific symptoms, diagnoses, and treatments; and other information demonstrating that they were actively seeking covered entities' services—was intentional intrusion upon their seclusion. This data was highly sensitive and legally protected, and Plaintiffs and Class Members did not consent to its collection by Meta.

155. Plaintiffs and Class Members had a reasonable expectation of privacy in this data, particularly because it included identifiable health information. By secretly tracking Plaintiffs' and Class Members' use of Covered Entities' websites, Meta acquired information about their health status, including specific information about their medical history and/or treatment decisions. This information is considered by the general public to be deeply private. Additionally, this information is specifically and heavily protected from disclosure under state and federal law, enhancing the general policy in favor of privacy expressed by the California Constitution.

156. Plaintiffs and Class Members did not consent to Meta collecting this data. Nor could they, as this type of information is so sensitive that Meta refuses to publicly acknowledge that it is collected.

157. Meta's invasion of Plaintiffs' and Class Members' privacy by collecting and using their identifiable health information would be highly offensive to a reasonable person. Plaintiffs' and Class Members' medical history and treatment decisions were and are highly private. Privacy is essential to the decision to seek medical treatment and beneficial to therapeutic and clinical relationships more broadly.

158. Plaintiffs and Class Members are also entitled to punitive damages. By intercepting identifiable health information—even after it was informed of the sensitive nature of the information—and turning that information into a profit-center, Meta intentionally and maliciously violated Plaintiffs' and Class Members' privacy, and further violated California's strong public policy in favor of privacy. Punitive damages are needed to deter Meta and other online advertising companies from engaging in similar conduct in the future.

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

COUNT 5

Unjust Enrichment

On Behalf of Plaintiffs and the Class

(Cal. Const., Art. 1, § 1)

160. All preceding factual statements and allegations are incorporated herein by reference.

161. Meta unjustly received and retained benefits from Plaintiffs and Class Members at their expense.

162. Plaintiffs and Class Members conferred a benefit upon Meta in the form of their extremely valuable identifiable medical information, which Meta illicitly and without consent intercepted and used for their own business purposes.

163. Meta was paid by ad buyers, including Cerebral and other Covered Entities, for ad targeting services that were built using Plaintiffs' and Class Members' data. Meta also refined its other revenue-generating products with this information and used this information in analytics reports to attract additional advertising customers.

164. Meta obtained this benefit at the expense of Plaintiffs and Class Members because it denied them the value of their identifiable health information, and Meta did not provide them with any commensurate compensation.

165. The benefit that Meta derived from Plaintiffs' and Class Members' data rightfully belongs to Plaintiffs and Class Members. Because Meta was only able to obtain this data from Plaintiffs and Class Members through the unfair, tortious, and illegal conduct described in this Complaint, it

would be unjust for Meta to retain any of the profits or other benefits that they derived from this conduct.

166. Plaintiffs and Class Members lack any remedy at law to address the harm caused by Meta's use and profit from, rather than Meta's interception of, their unlawfully obtained data. Additionally, the deep privacy injuries of Plaintiffs and Class Members cannot be wholly remedied by monetary relief.

167. For these reasons, Plaintiffs seeks the disgorgement of all unlawful or inequitable proceeds that Meta received, and such other relief as the Court may deem just and proper.

COUNT 6

Conversion

On Behalf of Plaintiffs and the Class

168. All preceding factual statements and allegations are incorporated herein by reference.

169. Plaintiffs and Class Members have a property interest in the identifiable health care data they provide to Covered Entities. They have exclusive possession of this data, as demonstrated by the legally protectable right and interest in the data conferred by the web of state and federal regulations that strictly governs the dissemination of this information and generally requires patients' explicit, specific authorization for it to be shared and used outside narrow, strictly defined circumstances. This data can only be acquired by covered entities with patients' assent, and they alone can, without restriction, permit this data to be shared with third parties and sanction its use outside of specific statutorily defined functions. Furthermore, without Plaintiffs' and Class Members' experiences and efforts to describe and seek treatment for their health conditions, this data would not exist in the first place (nor could it be aggregated into records for use by medical professionals).

170. Meta took possession of Plaintiffs' and Class Members' property—their identifiable health care data provided to Covered Entities—without their consent.

171. Plaintiffs and Class Members never authorized Meta to intercept the data Plaintiffs and Class Members shared with Covered Entities, nor did they consent in any other manner to Meta's interception, possession, and use of this data.

172. Meta's conversion of Plaintiffs' and Class Members' property was intentional. While Meta claimed that it would not acquire or use data in any way not described in its privacy policy and any partners using tools like the Pixel must have "lawful rights" to the data, this was – as Meta knew – untrue.

173. Meta expressly designed the Pixel to be able to automatically and secretly transmit individually identifiable information from third parties, including Covered Entities.

174. Meta knew that the Pixel was being used to obtain identifiable health information from Covered Entities. While Meta built an entire screening system nominally intended to prevent receipt of this information, it never worked effectively—a fact that Meta also knew. Meta was additionally aware of specific instances where companies were using the Pixel to transmit sensitive health information and allowed these companies to continue using the Pixel for that purpose.

175. Furthermore, Meta actively urged Covered Entities to use the Pixel and aggressively targeted health care companies as advertising clients—businesses whose placement of a Pixel on their sites would by definition involve the transmission of protected health care information.

176. Once Meta illicitly obtained Plaintiffs' and Class Members' property, it further exercised dominion over it by accepting it into Meta's data systems, using it extensively in Meta's own operations, and making no effort to return it to Plaintiffs or Class Members or obtain the authorizations necessary to lawfully hold and use it. Meta thereby deprived Plaintiffs of the ability to control the dissemination and use of the identifiable health information they provided to Covered Entities. Plaintiffs, who never consented to Meta taking this data in the first place, likewise did not consent to Meta's exercise of dominion over it.

177. The damages caused by conversion are presumed to be "[t]he value of the property at the time of the conversion, with the interest from that time." CCC § 3336. For Plaintiffs and Class Members this is the fair market value of their health data at the time of the conversion, which is readily ascertainable in light of the robust market for health care data described earlier in the complaint.

178. In accordance with CCC § 3336, Plaintiffs and Class Members seek the fair market value of their data at the time of the conversion.

179. Plaintiffs and Class Members are also entitled to punitive damages. By intercepting and using the identifiable health information Plaintiffs and Class Members provided to Covered Entities—even after it was aware of the protected nature of the information—Meta maliciously disregarded Plaintiffs' and Class Members' property rights.

COUNT 7

Violation of Unfair Competition Law ("UCL")

On Behalf of Plaintiffs and the Subclass

(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

180. All preceding factual statements and allegations are incorporated herein by reference.

181. Meta's conduct was unlawful, fraudulent, and unfair, in violation of the UCL. Cal. Bus. & Prof. Code § 17200.

182. The laws violated by Meta include but are not limited to:

a. ECPA 18 U.S.C. §§ 2510, *et seq.*;

b. CIPA, Cal. Penal Code §§ 631, 632(a);

c. The California Constitution's right to privacy, Cal. Const., Art. 1, § 1;

d. And HIPAA, 42 U.S.C. § 1320d-6.

183. Meta also fraudulently concealed the extent and sensitivity of the health data that it collected from Plaintiffs and Subclass Members. Meta did not disclose 1) that the Pixel was receiving sensitive health information that is protected by state and federal regulations or 2) that Meta did not in practice require Covered Entities to have any data authorizations before using the Pixel. The intent of these omissions was to deceive consumers like the Plaintiffs and Subclass Members about facts that Meta, as evidenced by its long history of non-user and health information privacy scandals, knew were likely to be material.

184. Meta had an obligation to disclose this information to Plaintiffs and Subclass Members. Meta had exclusive knowledge of the fact that it was receiving Plaintiffs' and Subclass Members' sensitive health information and did not require data authorizations for the use of the Pixel. This information was not reasonably accessible to Plaintiffs and Subclass Members and should have been disclosed prior to Meta intercepting their data.

185. Meta's concealments and omissions were material to Plaintiffs and Subclass Members, such that they actually relied on them. Plaintiffs and Subclass Members do not have Facebook accounts precisely because they are uncomfortable feeding any information into Meta's multibillion-dollar ad machine, let alone the detailed and intimate information the Pixel intercepted from Covered Entities. Had Plaintiffs and Subclass Members known that Meta was receiving their sensitive, identifiable health information even though they had not given their consent for it to be shared, they would not have used the Covered Entities' services.

186. For the same reasons, Meta's concealments and omissions were and are likely to be material to a reasonable consumer, given the sensitivity of the information involved and the strong legal protections for, and policy preferences in favor of, such information remaining confidential. The materiality of Meta's interception and use of non-user data—and the likelihood that a reasonable consumer would have been aware of the practices if Meta had publicly disclosed them—is further evidenced by the long list of non-user data scandals in which Meta has been embroiled.

187. Meta's conduct was also unfair. It violated California's strong public policy in favor of protecting consumers' privacy interests, which is reflected in the state's broad constitutional and statutory privacy protections, as well as the federal policy of ensuring that health information remains private. Additionally, Meta's interception of users' deeply private information, in violation of its own policies, was unethical, immoral, and unscrupulous. The harm caused by disclosing this information was significant, and there was no corresponding benefit to Plaintiffs and Subclass Members, who do not even have Facebook accounts. Furthermore, Meta's use of this information, which was illicitly and unlawfully procured, gave Meta a substantial advantage over other companies in the online advertising and analytics industry. Meta's interception of sensitive health information, without informing consumers, also impaired the market for health care services, preventing Plaintiffs and Subclass Members from making informed decisions about how to choose and interact with Covered Entities or assess the true cost of Covered Entities' services.

188. Meta's violation of the UCL economically injured Plaintiffs and Subclass Members in three respects.

189. First, Plaintiffs and Subclass Members paid for services from Covered Entities in large part because of their understanding that, consistent with state and federal law, the health-related information they shared with Covered Entities would be kept highly confidential. Had Plaintiffs and Subclass Members been made aware that Meta was intercepting their identifiable health information, they would not have been willing to use the Covered Entities' services.

190. Second, by intercepting the confidential medical information of Plaintiffs and Subclass Members, Meta denied them the privacy protections for which they paid and that were required by law, and thus denied Plaintiffs and Subclass Members the full value of the Covered Entity services they paid for.

191. Even though Meta received extensive advertising revenue from the Covered Entities, revenues that were made up in part from payments Plaintiffs and Subclass Members made to the Covered Entities, Plaintiffs and Subclass members were not compensated for Meta's use of their data.

192. For these reasons, Plaintiffs seek restitution on behalf of themselves and Subclass Members for the money that they paid to Covered Entities.

193. Plaintiffs also seek injunctive relief on behalf of themselves and Subclass Members. Absent injunctive relief barring Meta from intercepting Plaintiffs' and Subclass Members' sensitive health information, Meta's violation of the UCL and Plaintiffs' and Subclass Members' privacy will continue unchecked.

194. The deep privacy violation suffered by Plaintiffs and Subclass Members cannot be wholly remedied by monetary relief, and such remedies at law are inadequate.

COUNT 8

Violation of Consumers Legal Remedies Act ("CLRA")

On Behalf of Plaintiffs and the Subclass

(Cal. Bus. & Prof. Code §§ 1750, *et seq.*)

195. All preceding factual statements and allegations are incorporated herein by reference.

196. The CLRA prohibits unfair and deceptive acts and practices in any transaction that is intended to or results in the sale of goods and services. CCC § 1770(a).

197. The barred acts and practices include misrepresenting certification of goods or services, representing that goods or services have characteristics that they do not, and representing that a transaction confers or involves rights, remedies, or obligations that it does not have or involve, or that are prohibited by law. CCC § 1770(a)(2), (3), (14).

198. Meta concealed from Plaintiffs and the Subclass the fact that 1) it continued to invite the disclosure of sensitive health information in violation of numerous state and federal laws, and 2) it was actually receiving such information because 3) its system was configured to accept health information regardless of whether patients have given the statutorily required permissions, thereby violating § 1770(a)(2), (3), and (14) of the CLRA.

199. Meta had an obligation to disclose this information to Plaintiffs and Subclass Members. Meta had exclusive knowledge of the fact that it was receiving Plaintiffs' and Subclass Members' sensitive health information and did not require data authorizations for the use of the Pixel. This information was not reasonably accessible to Plaintiffs, Class, and Subclass Members and should have been disclosed prior to Meta intercepting their data.

200. Meta's concealments and omissions were material to Plaintiffs and Subclass Members, such that they actually relied on them. Plaintiffs and Subclass Members do not have Facebook accounts precisely because they are uncomfortable feeding any information into Meta's multibillion-dollar ad machine, let alone the detailed and intimate information the Pixel intercepted from Covered Entities. Had Plaintiffs and Subclass Members known that Meta was receiving their sensitive, identifiable health information even though they had not given their consent for it to be shared, they would not have used the Covered Entities' services.

201. For the same reasons, Meta's concealments and omissions were and are likely to be material to a reasonable consumer, given the sensitivity of the information involved and the strong legal protections for, and policy preferences in favor of, such information remaining confidential. The materiality of Meta's interception and use of non-user data—and the likelihood that a reasonable consumer would have been aware of the practices if Meta had publicly disclosed them—is further evidenced by the long list of non-user data scandals in which Meta has been embroiled.

202. At this time, Plaintiffs and Subclass Members seek only injunctive relief for this cause of action, but reserve the right to amend their complaint to seek monetary relief after providing statutory notice.

PRAYER FOR RELIEF

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

A. Certifying the Class and Subclass and appointing Plaintiffs as their representatives;

B. Appointing the law firm Motley Rice LLC as class counsel;

C. Finding that Defendants' conduct was unlawful, as alleged herein;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper;

E. Awarding Plaintiffs and the Class and Subclass Members statutory, actual, compensatory, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiffs and the Class and Subclass Members pre-judgment and post-judgment interest;

G. Awarding Plaintiffs and the Class and Subclass Members reasonable attorneys' fees, costs, and expenses; and

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

DATED: September 18, 2023

MOTLEY RICE LLC

Previn Warren*
Abigail Burman*†
401 9th Street NW Suite 630
Washington DC 20004
Tel: 202-386-9610
pwarren@motleyrice.com
aburman@motleyrice.com

Mathew Jasinski*
One Corporate Center
20 Church St., 17th Floor
Hartford, CT 06103
mjaskinski@motleyrice.com

**PRO HAC VICE APPLICATIONS TO BE FILED*

†Admitted only in Maryland, not admitted in the District of Columbia. Practicing under the supervision of the membership of Motley Rice, LLC.

WAGSTAFFE, VON LOEWENFELDT, BUSCH & RADWICK LLP

/s *Frank Busch*
James M. Wagstaffe (95535)
Frank Busch (258288)
100 Pine Street, Suite 2250
San Francisco, CA 94111
Tel: 415-357-8900
wagstaffe@wvbrlaw.com
busch@wvbrlaw.com