James M. Wagstaffe (95535)
Frank Busch (258288)
WAGSTAFFE, VON LOEWENFELDT, BUSCH & RADWICK LLP
100 Pine Street, Suite 2250
San Francisco, CA 94111
Tel: (415) 357-8900
Fax: (415) 357-8910
wagstaffe@wvbrlaw.com
busch@wvbrlaw.com

Carol C. Villegas (*pro hac vice* forthcoming)
Michael P. Canty (*pro have vice* forthcoming)
Melissa H. Nafash (*pro hac vice* forthcoming)
LABATON SUCHAROW LLP
140 Broadway
New York, NY 10005
Tel: (212) 907-0700
Fax: (212) 818-0477
cvillegas@labaton.com
mcanty@labaton.com
mnafash@labaton.com

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
Rachel Kesten (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JANE DOE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

META PLATFORMS, INC. F/K/A FACEBOOK, INC., UCSF MEDICAL CENTER, AND DIGNITY HEALTH MEDICAL FOUNDATION.

Defendants.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Jane Doe, on behalf of herself and all others similarly situated, asserts the following against Defendants Meta Platforms, Inc. (f/k/a/ "Facebook, Inc.") ("Meta"), UCSF Medical Center, and Dignity Health Medical Foundation, based upon personal knowledge, where applicable, information and belief, and the investigation of counsel, which included, among other things,

consultation with experts in the field of data privacy.

SUMMARY OF ALLEGATIONS

1. Founded in 2004 as a social networking website for college students, Meta has evolved into one of the largest advertising companies in the country.[1] To date, Meta generates nearly 98% of its revenue through advertising bringing in a grand total of $114.93 billion.

2. To power its advertising business, Meta collects data in a variety of ways, one of which is through its "Meta Pixel."

3. Meta Pixel is a snippet of code embedded on a third-party website that tracks a users' activity as the users navigate through a website. Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information they input into the website.[2]

4. For instance, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added something to their cart, as well as what they purchased.

5. Meta Pixel takes each of these pieces of information it harvests and sends it to Meta with personally identifiable information ("PII"), such as the users IP address, name, email, or phone number. Meta stores this data on its own server, and, in some instances, for years on end.[3]

6. Third-party websites that incorporate Meta Pixel benefit from the ability to analyze a user's experience and activity on its website to assess the website's functionality and traffic. The third-party website also gains information about its customers through the Meta Pixel that can be used to target/retarget them with advertisements, as well as to measure the results of advertisement efforts.

---

[1] John Gramlich, *10 facts about Americans and Facebook.* (June 1, 2021), https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

[2] Meta Business Help Center, *About Meta Pixel,* https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited July 13, 2022)

[3] The Markup, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients* (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

7. The benefit of third-party use of Meta Pixel to Meta, however, is far more sinister. When Meta Pixel is incorporated, unbeknownst to users and without their consent, Meta gains the ability to surreptitiously gather every user interaction with the website ranging from what a user clicks on to the personal information entered on a website. Meta aggregates this data against all websites.[4] Meta benefits from this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users.

8. Meta Pixel is wildly popular and embedded on millions of websites, including 30% of the top 80,000 most popular websites.

9. Alarmingly, Meta Pixel is incorporated on websites that are used to store and convey sensitive medical information intended to stay private. For example, Meta Pixel is embedded on the websites of 33 of the top 100 hospitals in America and on password-protected patient portals of seven health systems, such as those of UCSF Medical Center and Dignity Health Medical Foundation (hereinafter "Healthcare Defendants").

10. When a user enters its health information through Healthcare Defendants' websites and patient portals that incorporate Meta Pixel, such as to make an appointment, this information—including, in some instances, specifically what the user is treated for—is sent to Meta via Meta Pixel.

11. This data, which can include health conditions (e.g., Alzheimer's), diagnoses (e.g., COVID-19), procedures, test results, treatment status, the treating physician, medications, allergies, and PII (hereinafter "User Data"), is obtained and used by Meta, as well as other parties, in connection with targeted advertising.

12. Jane Doe (hereinafter "Plaintiff") had her User Data, including sensitive medical information, harvested by Meta through the Meta Pixel tool without her consent when she entered her information on the patient portals for UCSF Medical Center (My Chart) and Dignity Health's

[4] About Facebook Pixel | Meta Business Help Center, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited on July 21, 2022); and Unique Metrics | Meta Business Help Center (facebook.com), https://www.facebook.com/business/help/283579896000936 (last visited on July 21, 2022).

(My Portal) websites, and continued to have her privacy violated when her User Data was used for profit by Meta when it allowed pharmaceutical and other companies to send her targeted advertising related to her medical conditions.

13. As a result of Meta's illegal information gathering, Plaintiff received advertisements that were specifically tailored to her User Data, including sensitive medical information, that she entered on her patient portals.

14. These advertisements were tailored and directed to Plaintiff by Meta as part of Meta's advertising business in which Meta profits from providing third parties with access to persons most likely to be interested in their products or services, otherwise known as the target audience.[5]

15. Meta knows that the User Data collected through its Pixel on Healthcare Defendants' websites includes highly sensitive medical information but, in reckless disregard for patient privacy, continues to collect, use, and profit from this information.

16. Likewise, Healthcare Defendants knew by embedding Meta Pixel—a Meta advertising tool—they were sharing and permitting Meta to collect and use Plaintiff's and the Class members' User Data, including sensitive medical information.

17. Defendants' actions constitute an extreme invasion of Plaintiff and Class members' right to privacy and violate federal and state statutory and common law.

PARTIES

A. Plaintiff

18. Plaintiff Jane Doe ("Plaintiff Doe") is a resident of Sacramento County, California.

19. Plaintiff is a Facebook user and has had a Facebook account since at least 2012.

20. Plaintiff is a patient at UCSF Medical Center and Dignity Health. She has been using Dignity Health's My Portal since 2017 and UCSF Medical Center's My Chart since approximately February 2022.

---

[5] *Help your ads find the people who will love your business*. Facebook Advertising Targeting Options | Meta for Business, https://www.facebook.com/business/ads/ad-targeting?content_id=7ko93HYgrMsIy4k (last visited on July 14, 2022).

21. To make appointments, track and receive test results, receive medical treatment, and communicate with her doctors, Plaintiff was advised to utilize the online portals associated with UCSF Medical Center and Dignity Health.

22. Plaintiff's use of these patient portals entailed entering her User Data, including sensitive medical information, such as her heart and knee conditions into My Chart and My Portal.

23. Facebook surreptitiously collected this data and associated it with Plaintiff's Facebook account for use in targeting her with advertisements.

24. Indeed, after entering this information on the hospital websites, Plaintiff received targeted advertisements for related medications and treatments on her Facebook page, in her email, and in her text messages.

B. Defendants

25. Defendant Meta Platforms, Inc., f/k/a/ Facebook, Inc. is a Delaware corporation with its principal place of business located at 1601 Willow Road, Menlo Park, California 94025.

26. Defendant UCSF Medical Center is a public nonprofit educational institution with its principal place of business located at 490 Illinois Street, 4th Floor San Francisco, CA 94143-0000.

27. Defendant Dignity Health Medical Foundation is a not-for-profit organization with its principal place of business located at 185 Berry Street, Suite 200 San Francisco, CA 94107.

JURISDICTION AND VENUE

28. This Court has jurisdiction over the subject matter of this action 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 putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

29. This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 since this suit is brought under the laws of the United States, i.e., the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, and supplemental jurisdiction pursuant to 28

U.S.C. § 1367 over the remaining state common law and statutory claims as these state law claims are part of the same case or controversy as the federal statutory claim over which the Court has original jurisdiction.

30. This Court has general personal jurisdiction over Meta because it maintains its' principal place of business in California. Additionally, Meta is subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State.

31. This Court has general personal jurisdiction over UCSF Medical Center because it maintains its' principal place of business in California. Additionally, UCSF Medical Center is subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State.

32. This Court has general personal jurisdiction over Dignity Health Medical Foundation because it maintains its' principal place of business in California. Additionally, Dignity Health Medical Foundation is subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State.

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

34. Divisional Assignment: A substantial part of the events and omissions giving rise to the violations of law alleged herein occurred in the County of San Mateo, and as such, this action may properly be assigned to the San Francisco or Oakland divisions of this Court pursuant to Civil Local Rule 3-2(c).

FACTUAL BACKGROUND

A. Meta's Advertising Business

35. Founded in 2004 by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes, Meta began as a social networking website for college students.[6] The platform was a massive success, totaling more than one million users in 2004 and more than six million users the following year.[7]

36. In 2006, Meta expanded its membership from college students to anyone over the age of thirteen and by 2008 it had surpassed "Myspace" as the most popular and most visited social networking platform.[8]

37. Realizing the value of having direct access to millions of consumers, in 2007, Meta began monetizing its platform by launching "Facebook Ads," proclaiming it to be a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."[9]

---

[6] Jay Fuchs, *How Facebook Ads Have Evolved [+What This Means for Marketers]* (June. 11, 2021), https://blog.hubspot.com/marketing/history-facebook-adtips-slideshare

[7] The Associated Press, *Number of active users at Facebook over the years* (Oct. 23, 2012), https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANpSrN2n4sKRGr12jtBZzUHTDb2xEJOlCpRlshEwWGsyM4Iod1yAJWMKksxlai44WgP2LMk1642n4eWX7_6MtaBZWG1e5RvxW2ywyhrq7TnA3d4GQ2G3x9fTjnfjFnGrotu rfjOuXfN2uQpmCN580CwsKEQ9jsp8UB1NBQNQ2ly7

[8] Michael Arrington, Facebook No Longer The Second Largest Social Network | TechCrunch, https://techcrunch.com/2008/06/12/facebook-no-longer-the-second-largest-social-network/#:~:text=It%20was%20sort%20of%20inevitable,by%20Comscore%20and%20shown%20above. (last visited on July 18, 2022)

[9] *Meta, Facebook Unveils Facebook Ads* (Nov. 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/

38. Today, Meta provides advertising on its own platforms, such as Facebook and Instagram, as well as websites outside these apps through the Facebook Audience Network. Facebook alone has more than 2.9 billion active users.[10]

39. Meta offers several advertising options based on the type of audience the advertiser wants to target. A few of these options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and then an even more granular approach within the audiences called "Detailed Targeting." Each of Meta's advertising tools allow an advertiser to target users based on their personal data, including geographic location, demographics (e.g. age, gender, education, job title, and more), interests (e.g. preferred foods, movies), connections (e.g. to a particular event or Facebook page), and behaviors (e.g. purchases, device usage, and pages visited), among other things. This audience can be created by Meta, the advertiser, or a combination of both.

40. Ad Targeting has been extremely successful due, in large part, to Meta's ability to target people at a granular level. "Among many possible target audiences, [Meta] offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[11]

41. Given the highly granular data used to target specific users, it is no surprise that Meta's advertising segment quickly became Meta's most successful business unit with millions of companies and individuals utilizing Facebook's advertising services.

42. By 2009, Meta derived $761 million through its advertising business.[12] Just ten years later, Meta's revenue from advertising would increase by nearly 100 times.

---

[10] S. Dixon, *Number of monthly active Facebook users worldwide as of 1st quarter 2022*, Statista (July 15, 2022), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[11] Natasha Singer, *What You Don't Know About How Facebook Uses Your Data* (Apr. 11 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

[12] Rishi Iyengar, *Here's how big Facebook's ad business really is*, CNN Business (July 1, 2020), https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html

43. As the chart below illustrates, Meta "generate[s] substantially all of [its] revenue from selling advertising placements to marketers."[13] Indeed, Meta had a 36% increase in revenue in 2021 compared to 2020, which was "mostly driven by an increase in advertising revenue."[14]

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$117.93 billion	$114.93 billion	97.46%
2020	$85.97 billion	$84.17 billion	97.90%
2019	$70.70 billion	$69.66 billion	98.52%
2018	$55.84 billion	$55.01 billion	98.51%
2017	$40.65 billion	$39.94 billion	98.25%

44. Due to its ability to target people based on such granular data, Meta's ad-targeting capabilities have frequently come under scrutiny. For instance, in June 2022, Meta entered a settlement with the Department of Justice regarding its Lookalike Ad service, which permitted targeting by landlords based on race and other demographics in a discriminatory manner.

45. Acknowledging that micro-level targeting is highly problematic, in November of 2021, Meta announced that it was removing options that "relate to topics people may perceive as sensitive," such as "Health causes (e.g., 'Lung cancer awareness', 'World Diabetes Day', 'Chemotherapy'),Sexual orientation (e.g., 'same-sex marriage' and 'LGBT culture')", "Religious practices and groups (e.g., 'Catholic Church' and 'Jewish holidays')", as well as "Political beliefs, social issues, causes, organizations, and figures."[15]

B. How Meta Accesses and Uses Data Through Meta Pixel

46. Peter Eckersley, Chief Computer Scientist for the Electronic Frontier Foundation, explained that by utilizing Meta's tracking tools "'Facebook can learn almost anything about you

[13] Meta Platforms, Inc. Form 10-K for fiscal year ended December 31, 2021, https://www.sec.gov/Archives/edgar/data/1326801/000132680122000018/fb-20211231.htm (last visited on July 15, 2022).

[14] *Id.*

[15] Meta, *Removing Certain Ad Targeting Options and Expanding Our Ad Controls* (Nov. 9, 2021), https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls

by using artificial intelligence to analyze your behavior.'. . .'That knowledge turns out to be perfect . . . for advertising . . . ."[16]

47. Meta uses a variety of tracking tools to collect data about individuals, including through software development kits incorporated into third party applications, its "Like" and "Share" buttons (known as "social plug-ins"), and other methodologies, which it then uses to power its advertising segment. One of its most powerful tools is Meta Pixel, formerly known as Facebook Pixel, which launched in 2015.

48. Meta touted Meta Pixel as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website."[17] According to Meta, to use Meta Pixel an advertiser need only "place a single pixel across [its] entire website to report and optimize for conversions" so that the advertiser could "measure the effectiveness of [its] advertising by understanding the actions people take on [its] website."[18]

49. For a company or advertiser, once Meta Pixel is set up on a website, it tracks users as they navigate through the website and logs which pages are visited, buttons clicked, the specific (and personal) information entered in forms, as well as "optional values" set by the website.[19] Meta Pixel tracks this data regardless of whether the user is logged into Facebook.[20]

50. For Meta, the Pixel acts as a conduit of information, sending the information it collects to Meta through scripts running in the user's internet browser. The information is sent in data packets labeled with PII, including the user's IP address.

---

[16] Natasha Singer, *What You Don't Know About How Facebook Uses Your Data* (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

[17] Cecile Ho, *Announcing Facebook Pixel* (Oct. 14, 2015), https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/

[18] Oviond, *Understanding the Facebook Pixel*, (2022) https://www.oviond.com/understanding-the-facebook-pixel

[19] Meta Pixel (2022), https://developers.facebook.com/docs/meta-pixel/

[20] Pixel Hunt, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients* (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

51. If the user has a Facebook account, the User Data collected is linked to the individual users' Facebook account. For example, if the user is logged into their Facebook account when the user visits a website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Meta to link the data collected by Meta Pixel to the specific Facebook user.

52. Alternatively, Meta can link the data to a users' Facebook account through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users.[21]

53. Meta can also link User Data to Facebook accounts through identifying information collected through Meta Pixel through what Meta calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Meta to link users. Using Automatic Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.[22]

54. Meta then provides the websites using Meta Pixel with this data in the "Meta Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads.[23] For example, these websites can use this data to create "custom audiences" to target the specific Facebook user, as well as other Facebook users who match members' of the audiences criteria.[24] They can also search through the Meta Pixel data to find a specific type of users to target, for instance, men over a certain age.

---

[21] Clearcode, *Third- to First-Party*, https://clearcode.cc/blog/facebook-first-party-cookie-adtech/#facebook-cookie-pixel:-from-third--to-first-party

[22] While Meta purports to "hash" the PII provided by patients, Meta actually uses the hashed format ***specifically to link Meta Pixel data to Facebook profiles***. Todd Feathers, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites* (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[23] Meta Business Help Center https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[24] Meta For Developers, *Custom Audiences*, https://developers.facebook.com/docs/meta-pixel/implementation/custom-audiences

55. Meta benefits from the data derived from the pixel as well, using it to serve targeted advertisements and identify users to be included in targeted ads.

56. Recently, an investigation by The Markup[25] revealed that the Meta Pixel is embedded on the websites of 33 of the top 100 hospitals in the nation, collecting User Data, including sensitive medical information, and sending it to Meta when a user interacts with the website. For example, when a user on the hospital website clicks the "Schedule Online" button next to a doctor's name, Meta Pixel sends the text of the button, the doctor's name, and the search term used to find the doctor to Meta. If the hospital's website has a drop-down menu to select a medical condition in connection with scheduling an appointment, that condition is also transmitted to Meta through Meta Pixel.

57. Even more egregiously intrusive, Meta Pixel is installed inside password-protected patient portals of at least seven health systems. When a user navigates through their patient portal, Meta Pixel sends Meta data including the patients' medication information, prescriptions, descriptions of their issues, notes, test results, and details about upcoming doctor's appointments.

58. Although Meta purports to "hash" the PII provided by patients, Meta actually uses the hashed format ***specifically to link Meta Pixel data to Facebook profiles***.[26] Meta has designed the Pixel such that Meta receives the information about patient actions on the medical provider's properties contemporaneous with their making. As soon as a patient takes any action on a webpage which includes the Facebook Pixel—such as clicking a button to register, login, or logout of a patient portal or to create an appointment—Facebook code embedded in the page re-directs the content of the patient's communication to Facebook while the exchange of the communication between the patient and the medical provider is still occurring.

---

[25] The Markup is a nonprofit organization that was founded in 2018. It investigates how powerful institutions are collecting and using technology. The Markup, *Big Tech Is Watching You. We're Watching Big Tech*. (June 19, 2022), https://themarkup.org/

[26] Pixel Hunt, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites* (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

59. The 33 hospitals found to have the Meta Pixel collecting and sending patient appointment details to Meta collectively reported more than ***26 million patient admissions and outpatient visits in 2020 alone***. However, the number of impacted patients is likely higher as The Markup's investigation was limited to just over 100 hospitals.

60. David Holtzman, a health privacy consultant was "deeply troubled" by the results of The Markup's investigation and indicated "it is quite likely a HIPAA violation" by the hospitals, such as Healthcare Defendants.

61. Laura Lazaro Cabrera, a legal officer at Privacy International, indicated that Meta's access to use even only some of these data points—such as just the URL—is problematic. She explained, "'Think about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data.'"[27]

62. Recently, Meta employees admitted to the lax protections over sensitive data. Meta engineers on the ad and business product team wrote in a 2021 privacy overview "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[28]

63. Plaintiff Jane Doe fell victim to Meta's unlawful collection and sharing of her sensitive medical information. Plaintiff Doe is a patient of UCSF and Dignity Health Medical Foundation hospital.

64. Plaintiff's use of the patient portals of these hospitals and entered her User Data, including sensitive medical information, such as her heart and knee conditions.

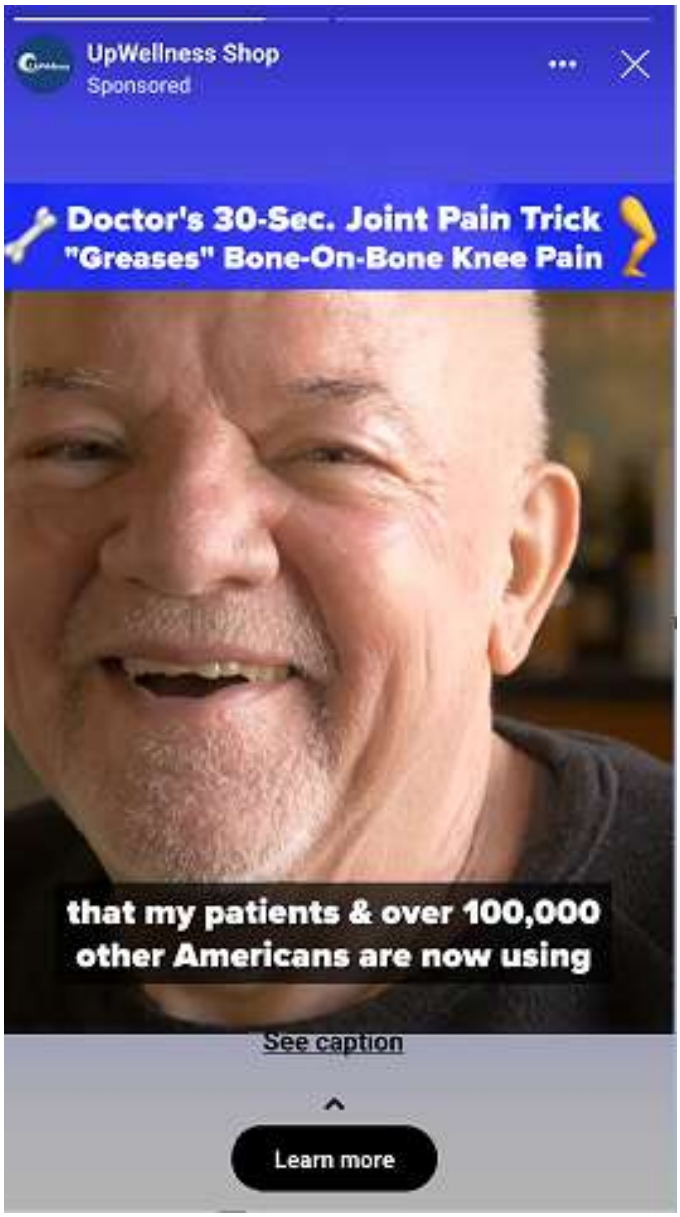
---

[27] Pixul Hunt, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients* (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

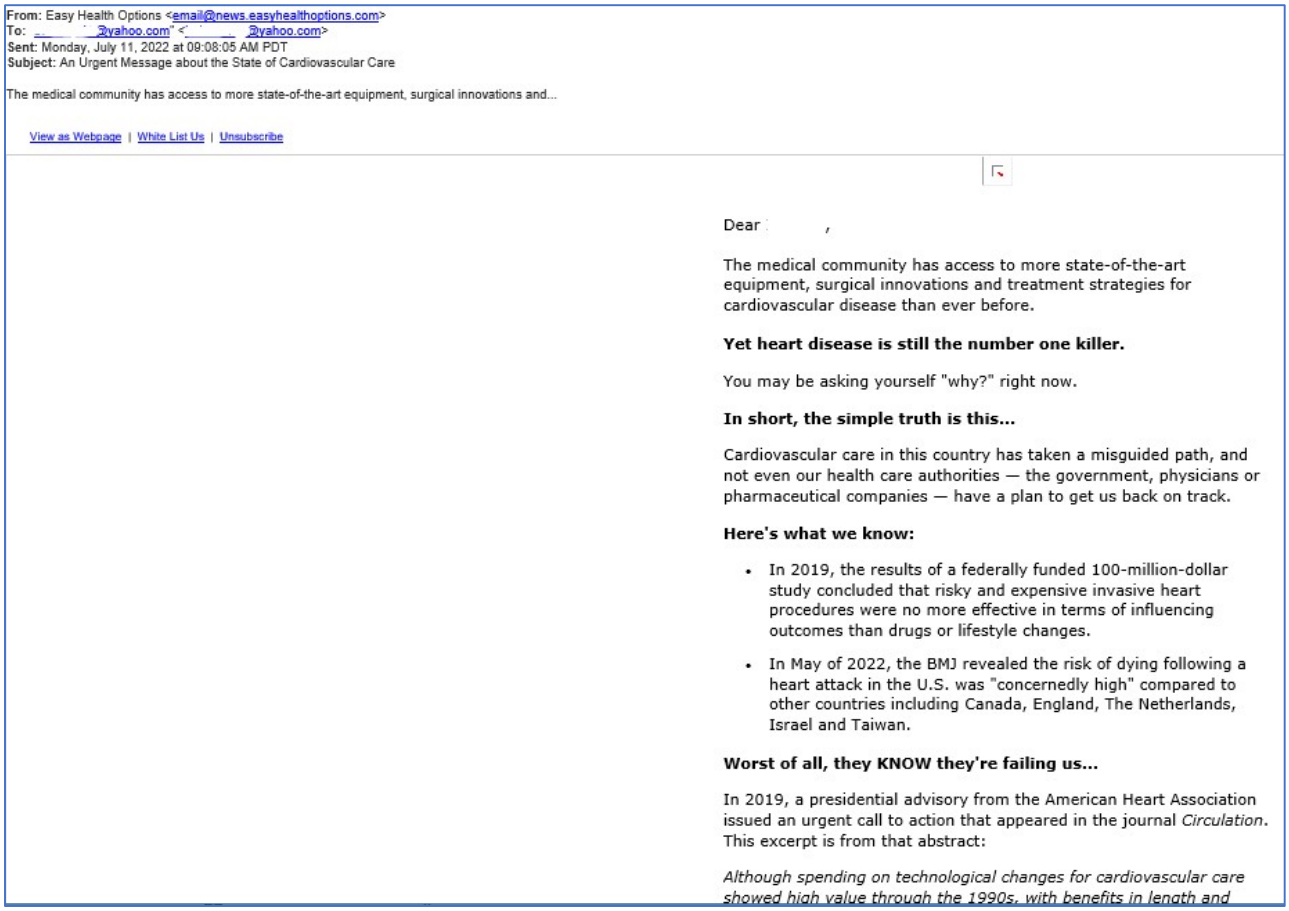
[28] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document* (Apr. 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

65. After entering this information on the hospitals' patient portals, and receiving her test results and heart condition diagnosis, Plaintiff Doe started receiving ads on her Facebook page related to this condition, as demonstrated below:

66. Likewise, after entering this information on the hospitals' patient portals, Plaintiff Doe started receiving ads on her Facebook page relating to her knee condition. For example:



67. Plaintiff Doe also began receiving targeted email advertising, as demonstrated below, to the email address associated with her Facebook account, related to the same conditions for which she provided User Data through the Healthcare Defendants website:



From: Easy Health Options <email@news.easyhealthoptions.com>
To: [redacted]@yahoo.com" <[redacted]@yahoo.com>
Sent: Monday, July 11, 2022 at 09:08:05 AM PDT
Subject: An Urgent Message about the State of Cardiovascular Care

The medical community has access to more state-of-the-art equipment, surgical innovations and...

View as Webpage | White List Us | Unsubscribe

Dear [redacted],

The medical community has access to more state-of-the-art equipment, surgical innovations and treatment strategies for cardiovascular disease than ever before.

Yet heart disease is still the number one killer.

You may be asking yourself "why?" right now.

In short, the simple truth is this...

Cardiovascular care in this country has taken a misguided path, and not even our health care authorities — the government, physicians or pharmaceutical companies — have a plan to get us back on track.

Here's what we know:

- In 2019, the results of a federally funded 100-million-dollar study concluded that risky and expensive invasive heart procedures were no more effective in terms of influencing outcomes than drugs or lifestyle changes.
- In May of 2022, the BMJ revealed the risk of dying following a heart attack in the U.S. was "concernedly high" compared to other countries including Canada, England, The Netherlands, Israel and Taiwan.

Worst of all, they KNOW they're failing us...

In 2019, a presidential advisory from the American Heart Association issued an urgent call to action that appeared in the journal *Circulation*. This excerpt is from that abstract:

Although spending on technological changes for cardiovascular care showed high value through the 1990s, with benefits in length and

C. Plaintiff and Class Members Do Not Consent to Defendants' Collection or Use of Their User Data

68. Plaintiff Doe and Class members have no idea that Defendants are collecting and utilizing their User Data, including sensitive medical information, when they engage with websites that incorporate Meta Pixel because the software is seamlessly incorporated in the background.

69. For instance, when Plaintiff Doe logged into Healthcare Defendants' patient portal, there was no indication that Meta Pixel was embedded or that it would collect her sensitive medical information.

70. Plaintiff Doe, and all Class members, could not consent to Defendants' conduct when they were unaware their sensitive medical information would be collected and used in the first place.

71. While Meta purports to maintain a "Data Policy" that vaguely states under a buried heading "Information from partners" that its "partners provide information about your activities"

including "websites you visit," Plaintiff and Class members would not visit or read Meta's website, let alone their Data Policy, when scheduling appointments or inputting medical information intended for Healthcare Defendants, i.e., their medical providers.

72. Even if Plaintiff did encounter Meta's Data Policy stating in vague terms that Meta may receive information from "websites you visit," this undescriptive provision would not be understood by any reasonable user to mean that Meta collects and uses User Data, including specific inputs by the user or sensitive medical information provided to Healthcare Defendants to receive medical services.

73. Indeed, the collection of Plaintiff's sensitive medical information is inconsistent with the remaining provisions contained in Meta's Data Privacy. Namely, Meta states that each of its purported "partners" are "require[d]" to have "lawful rights to collect, use and share [users'] data before providing any data to [Meta]." However, Healthcare Defendants do not have the legal right to use or share Plaintiffs' and Class members data, as this information is protected by the Health Insurance Portability and Accountability Act of 1996's ("HIPAA") Privacy Rule, which protects all electronically protected health information a covered entity like Healthcare Defendants "create[], receive[], maintain[], or transmit[]" in electronic form. *See* 45 C.F.R. § 160.103. The Privacy Rule does not permit the use and disclosure of protected health information to Meta for use in targeted advertising. *See* 45 C.F.R. § 164.502.

74. Thus, Defendants did not obtain consent to collect, use, and store Plaintiff's and Class members' sensitive medical information.

D. Defendants Knew Plaintiff's User Data Included Sensitive Medical Information, Including Medical Records

75. Defendants were aware that by incorporating Meta Pixel onto hospital websites, this would result in the disclosure and use of Plaintiff's and Class members' User Data, including sensitive medical information.

76. By virtue of how Meta Pixel works, i.e., sending all interactions on a website to Meta, Healthcare Defendants were aware that their patients' sensitive User Data would be sent to Meta when they made appointments and otherwise interacted with their websites.

77. Indeed, software companies like MyChart that provide online access to medical records utilized by Healthcare Defendants have "specifically recommended heightened caution around the use of custom analytics."[29] Despite this, Healthcare Defendants continued to use Meta Pixel on their websites.

78. Meta also was acutely aware that by placing its Meta Pixel on Healthcare Defendants' websites, it would enable the collection of Plaintiff's and Class members' sensitive User Data, it would receive this data, and this data would be incorporated and made available for use in its advertising network.

79. While a Meta spokesperson, Dale Hogan, claims that it is "against [Meta's] policies for websites and apps to send sensitive health data about people through [its] Business Tools," and that its system is purported "designed to filter out potentially sensitive data" these policies and procedures were not enforced or entirely ineffective.[30]

80. Indeed, a complaint by the Federal Trade Commission in 2021 revealed that Meta was receiving medical information through its Business Tools from a popular women's health app, including pregnancy data, for years (at least between June 2016 to February 2019). The FTC also found that Meta used this information for its own research and development.

81. The New York State Department of Financial Services ("NYSDFS") reached a similar conclusion in February of 2021, finding that Meta collected sensitive data, including medical information, in violation of its own policies. Regarding Meta's policies, NYSDFS explained "[m]erely stating a rule, however, has little meaning if the rule is not enforced, and the unfortunate

---

[29] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[30] https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story

fact is that Facebook does little to track whether . . . developers are violating this rule and takes no real action against developers that do." NYDFS concluded that "Facebook's efforts here [are] seriously lacking" and that "[u[ntil there are real ramifications for violating Facebook's policies, Facebook will not be able to effectively prohibit the sharing of sensitive user data with third-parties."[31]

82. The Markup also found during the course of its investigation that Meta's purported "filtering" failed to discard even the most obvious forms of sexual health information, including URLs that included the phrases "post-abortion" "i-think-im-pregnant" and "abortion-pill."

83. In fact, documents leaked to *Vice* in 2021 reveal that Meta's own employees acknowledge that Meta cannot adequately control how its own systems use data. One Meta engineer on Meta's Ad and Business Product team explained "We do not have adequate level of control and explainability over how our systems use data, and thus we can't confidentially make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"

84. Serge Egelman, research director of the Usable Security & Privacy Group at UC Berkeley's International Computer Science Institute explained Meta has no incentive to enforce its own policies because "[t]hat costs them money to do. As long as they're not legally obligated to do so, why would they expend any resources to fix [it]?"[32]

85. Despite that Meta knew it was receiving medical information through its Business Tools when enabled on apps and websites that provide health-related services—and that its purported "policies" were grossly deficient—Meta still enabled Meta Pixel on Defendant-Medical Providers websites and received sensitive medical information well through 2022.

---

[31] New York State Department of Financial Services, *Report on Investigation of Facebook Inc. Data Privacy Concerns,* (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

[32] *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients* - Reveal (revealnews.org), https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/ (last visited July 19, 2022).

E. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their User Data, Especially With Respect to Sensitive Medical Information

86. Plaintiff and Class members have a reasonable expectation of privacy in their User Data, including personal information and sensitive medical information.

87. Patient health information specifically is protected by federal law under HIPAA.

88. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

89. This federal legal framework applies to health care providers, such as the Healthcare Defendants.

90. Given the application of HIPAA to the Healthcare Defendants, Plaintiff and the members of the Class had a reasonable expectation of privacy over their protected health information.

91. Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information from millions of individuals, as Defendants have done here, violates expectations of privacy that have been established as general social norms.

92. Privacy polls and studies uniformly show that the overwhelming 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.

93. For example, 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.[33] 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.[34]

94. Users act consistent with these preferences. 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 share data when prompted.[35]

95. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[36] The article continues "Children today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[37]

96. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' sensitive medical information. For example, Dena Mendelsohn—the former

[33] *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/.

[34] *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-confused-and-feeling-lack-of-control-over-their-personal-information/.

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

[36] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, THE MIT PRESS READER, https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/.

[37] *Id.*

Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you're charged on loans, and leave you vulnerable to workplace discrimination.[38]

97. Defendants surreptitiously collected and used Plaintiff and Class members' User Data, including, highly sensitive medical information, through Meta Pixel in violation of Plaintiff's and Class members' privacy interests.

F. Plaintiff's User Data that Defendants' Disclosed, Collected, and Used is Plaintiff's Property, Has Economic Value, and its Illicit Disclosure Caused Economic Harm

98. Meta has built its business around the collection of personal data because the "world's most valuable resource is no longer oil, but ***data***."[39] As the *Economist* analogized, a user's personal data is "the oil of the digital era."[40]

99. It is common knowledge in the industry that there is an economic market for consumers' personal data—including the User Data that Defendants collected from Plaintiff and Class members.

100. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and

---

[38] Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPORTS (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.

[39] *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-longer-oil-but-data (emphasis added).

[40] *Id.*

location" information are sold for about "$0.50 per 1,000 people."[41] This estimate was based upon "industry pricing data viewed by the Financial Times," at the time.[42]

101. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30 per name."[43] That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge"[44] and that the value of a single user's data (within the corporate acquisition context) can vary from $15 to more than $40 per user.[45]

102. In an August 2021 Washington Post article, legal scholar Dina Srinivasan said that consumers "should think of Facebook's cost as [their] data, and scrutinize the power it has to set its own price." And this price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from $19 per year to $164 per year between 2013 and 2020.[46]

103. The Organization for Economic Cooperation and Development ("OECD") published in 2013 a paper titled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[47] In this paper, the OECD measured prices demanded by companies concerning User Data derived from "various online data warehouses."[48] OECD indicated that "[a]t

---

[41] Emily Steel, et al., *How much is your personal data worth?,* FIN. TIMES (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz3myQiwm6u.

[42] *Id.*

[43] Pauline Glickman and Nicolas Glady, *What's the Value of Your Data?,* TECHCRUNCH (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

[44] *Id.*

[45] *Id.*

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

[47] *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.oecd-ilibrary.org/docserver/5k486qtxldmq-en.pdf.

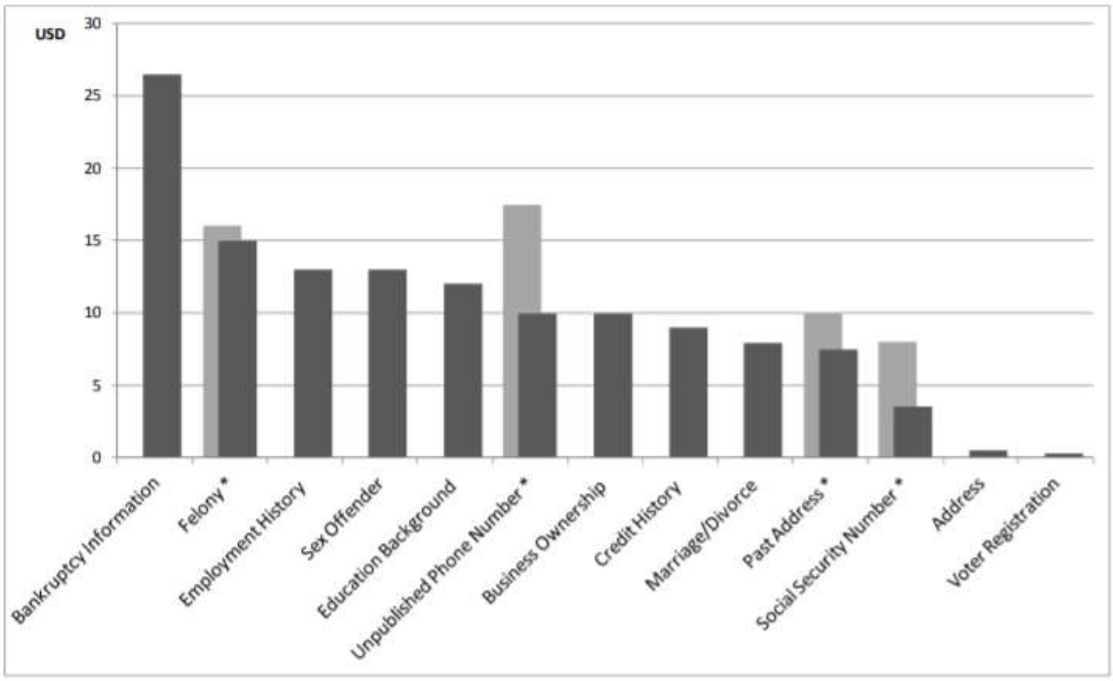
[48] *Id.* at 25.

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 is estimated to cost USD 55."[49]

104. The OECD published in this same paper a chart demonstrating the various "Market prices for personal data by type"[50]:

Figure 7. Market prices for personal data by type

(per record)



* two different prices provided by different providers.

Sources: Locate Plus (address Unpublished Phone Number Felony) Pallorium (address, past address Unpublished Phone Number Social Security Number) KnowX via Swipe Toolkit (Past address, Marriage/Divorce Bankruptcy Information Business Ownership) LexisNexis via Swipe Toolkit (Education Background Employment History Social Security Number Felony sex offender) Experian (Credit History) Voters online.com (voter registration)

105. Notably a 2021 report from *Invisibly* found that personal medical information is one of the ***most valuable pieces of data*** within this data-market. "It's worth acknowledging that because health care records often feature a more complete collection of the patient's identity, background,

[49] *Id.*

[50] *Id.* at 26.

and personal identifying information (PII), health care records have proven to be of particular value for data thieves. While a single social security number might go for $0.53, a complete health care record sells for $250 on average. For criminals, the more complete a dataset, the more potential value they can get out of it. As a result, health care breaches increased by 55% in 2020."[51] The article noted the following breakdown in average price for record type:

Record Type	Average Price
Health Care Record	$250.15
Payment Card Details	$5.40
Banking Records	$4.12
Access Credentials	$0.95
Social Security Number	$0.53
Credit Record	$0.31
Basic PII	$0.03

106. Furthermore, individuals can sell or monetize their own data if they so choose. Indeed, ***Defendants*** themselves have valued individuals' personal data in real-world dollars.

107. Meta has offered to pay individuals for their voice recordings,[52] and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Meta to collect data on how individuals use their smartphones.[53]

---

[51] *Id.*

[52] Jay Peters, *Facebook will now pay you for your voice recordings*, THE VERGE (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnciations-app.

[53] Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data,* CNBC (Jan. 29. 2019), https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html.

108. A myriad of other companies and apps such as Nielsen Data, Killi, DataCoup, and AppOptix offer consumers money in exchange for their personal data.[54]

109. Given the monetary values that data companies—***like Meta***—have ***already*** paid for personal information in the past, Defendants have deprived Plaintiffs of the economic value of their sensitive medical information by acquiring such data without providing proper consideration for Plaintiffs' property.

G. Meta's History of Egregious Privacy Violations

110. Since 2007, Meta's core business model has been monetizing user information – at the expense of its users. As the Federal Trade Commission ("FTC") noted in a 2019 complaint against Meta, "substantially all of Facebook's $55.8 billion in 2018 revenues came from advertising."[55]

111. In 2007, when Meta launched "Facebook Beacon," users were unaware that their online activity was tracked, and that the privacy settings originally did not allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut down.

112. Just two short years later, Meta made controversial modifications to its Terms of Service, which allowed Meta to use anything a user uploaded to its site for any purpose, at any time, even after the user ceased to use Facebook. The Terms of Service also failed to provide any way for users to completely delete their accounts. Under immense public pressure, Meta eventually returned to its previous Terms of Service.

113. In November 2011, Meta, settled charges with the Federal Trade Commission ("FTC") relating to its sharing of Facebook user information with advertisers as well as its false claim that third-party apps were able to access only the data they needed to operate when, in-fact, the apps could access nearly all of a Facebook user's personal data. Jon Leibowitz, Chairman of the FTC, warned "Facebook is obligated to keep the promises about privacy that it makes to its

---

[54] *28 Apps That Pay You For Data Collection: Earn a Passive Income*, DOLLAR BREAK (July. 7, 2022), https://www.dollarbreak.com/apps-that-pay-you-for-data-collection/.

[55] Complaint For Civil Penalties, Injunction, And Other Relief, *United States v. Facebook, Inc.*, Case No. 19-cv-2184-TJK (D.C. July 24, 2019), ECF No. 1.

hundreds of millions of users . . . Facebook's innovation does not have to come at the expense of consumer privacy."[56]

114. The resulting Consent Order prohibited Meta from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Meta makes user information accessible to third parties.[57]

115. Meta faced yet another privacy scandal in April 2015 when it was revealed they could not keep track of how many developers were using previously downloaded Facebook User Data.

116. Also in 2015, it was revealed Meta once more violated users' privacy rights when it was revealed that Meta's "Tag Suggestion" feature harvested and stored users' facial data from photos without asking for consent or providing notice, in violation of Illinois' Biometric Information Privacy Act. Meta ultimately settled claims related to this unlawful conduct for $650 million.

117. In 2018, Meta was again in the spotlight for failing to protect users' privacy. Meta testified before Congress that a company called Cambridge Analytica may have harvested the data of up to 87 million users in connection with the 2016 election. This led to yet another FTC investigation in 2019 into Meta's data collection and privacy practices, resulting in a record-breaking five-billion-dollar settlement.

118. That same year, a report revealed that Meta had violated users' consent on privacy by granting access to users' information to over 150 companies.[58] Some companies were even able to read users' private messages. This deal, in turn, helped Meta bring in more users.

119. In June 2020, after promising users app developers would not have access to data if users were not active in the previous 90 days, Meta revealed that it still enabled third-party

---

[56] *Id.*

[57] Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012)

[58] Elizabeth Schulze, *Facebook let tons of companies get info about you, including Amazon, Netflix, and Microsoft*, (Dec. 19, 2018), https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html.

developers to access this data.[59] This failure to protect users' data enabled thousands of developers to see data on inactive users if those users were Facebook friends with someone who was an active user.

120. On February 18, 2021, New York State Department of Financial ("NYSDFS") Services released a report detailing the significant privacy concerns associated with Meta's data collection practices, including the collection of health data. The report noted that while Meta maintained a policy that instructed developers not to transmit sensitive medical information, Meta received, stored, and analyzed this data anyway. The report further concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective at enforcing Facebook's policy or preventing the receipt of sensitive data." Meta was unwilling to review the data it previously collected and analyzed and so the NYSDFS called on federal regulators to compel Meta to undergo such a process.

121. In June 2022, Meta entered a settlement with the U.S. Department of Justice relating to claims that the company allowed landlords to market housing ads in a discriminatory manner by utilizing Meta's ad targeting tool called "Lookalike Audiences." This tool purportedly allowed advertisers to target users by race, gender, religion, and other sensitive characteristics. As part of the settlement, Meta agreed to decommission this egregious targeting tool.

122. Despite Meta's multitude of egregious privacy violations, it continues to show a blatant disregard for the privacy rights of users, including by collecting and utilizing Plaintiff's and Class members' highly sensitive medical information without consent.

TOLLING, CONCEALMENT, AND ESTOPPEL

123. The applicable statutes of limitation have been tolled as a result of Defendants' knowing and active concealment and denial of the facts alleged herein.

124. Defendants seamlessly incorporated Meta Pixel into websites, providing no indication to users that they were interacting with a website with Meta Pixel enabled.

---

[59] Kurt Wagner And Bloomberg, *Facebook admits another blunder with user data* (July 1, 2020), https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/

125. Defendants had exclusive knowledge that Healthcare Defendants' websites incorporated Meta Pixel yet failed to disclose that by interacting with the Meta Pixel-enabled websites that Plaintiffs and Class members sensitive medical information would be collected, used, and stored by Meta.

126. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct, including because there were no disclosures or other indication that they were interacting with Meta-Pixel enabled websites.

127. The earliest Plaintiff and Class members, acting with due diligence, could have reasonably discovered this conduct would have been on June 15, 2022, following the release of The Markup's investigation.

128. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Under the circumstances, Defendants were under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendants are therefore estopped from relying on any statute of limitations.

CLASS ACTION ALLEGATIONS

129. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

> **Nationwide Class:** All natural persons in the United States whose User Data was collected through Meta Pixel.[60]
>
> **California Subclass:** All natural persons residing in California whose User Data was collected through Meta Pixel.
>
> **Facebook Subclass:** All Facebook (or other subsidiaries of Meta) users in the United States whose User Data was collected through Meta Pixel.

130. Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents

[60] Plaintiff has defined the Classes based on currently available information and hereby reserves the right to amend the definition of the Classes, including, without limitation, the Class Period.

have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendants' counsel.

131. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Classes likely consists of millions of individuals, and the members can be identified through Meta's records.

132. **Predominant Common Questions:** The Classes' 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 Classes include, but are not limited to, the following:

a. Whether Meta violated Plaintiff's and Class members' privacy rights;

b. Whether Meta's acts and practices violated California's Constitution, Art. 1, § 1.;

c. Whether Meta was unjustly enriched;

d. Whether Meta violated the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*;

e. Whether Meta's acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;

f. Whether Meta's acts and practices violated California's Business and Professions Code §§ 17200, *et seq.*;

g. Whether Meta's acts and practices violated California's Business and Professions Code §§ 17200, *et seq.*;

h. Whether Meta aided and abetted the affected hospitals in violation of the California's Business and Professions Code §§ 17200, *et seq.*;

i. Whether Meta aided and abetted tortious acts;

j. Whether Meta's acts and practices violated the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*;

k. Whether Meta's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

l. Whether Meta's acts and practices violated the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502;

m. Whether Plaintiff and the Class members are entitled to equitable relief, including but not limited to, injunctive relief, restitution, and disgorgement; and,

n. Whether Plaintiff and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

133. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. The claims of Plaintiff and the members of the Class arise from the same conduct by Defendants and are based on the same legal theories.

134. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendants have no defenses unique to any Plaintiff. Plaintiff and her 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 Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

135. **Substantial Benefits:** 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.

136. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

137. California substantive laws apply to every member of the Class. California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Classes under the

Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiff and Class members, thereby creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

138. Meta's Terms of Service includes a choice of law provision wherein Meta and its users agree to apply the laws of the State of California to govern any claim.[61] Moreover, Meta's principal place of business is located at 1601 Willow Road, Menlo Park, CA 94025 and it conducts substantial business in California, such that California has an interest in regulating Meta's conduct under its laws. Meta's choice of law provision in its Terms of Service, plus its decision to reside in California and avail itself of California's laws, renders the application of California law to the claims herein constitutionally permissible.

139. UCSF Medical Center's principal place of business is located at 490 Illinois Street, 4th Floor San Francisco, CA 94143-0000 and it conducts substantial business in California, such that California has an interest in regulating UCSF Medical Center's conduct under its laws. UCSF Medical Center's decision to reside in California and avail itself of California's laws, renders the application of California law to the claims herein constitutionally permissible.

140. Defendant Dignity Health Medical Foundation's principal place of business is located at 185 Berry Street, Suite 200 San Francisco, CA 94107, and it conducts substantial business in California, such that California has an interest in regulating Dignity Health Medical Foundation's conduct under its laws. Dignity Health Medical Foundation's decision to reside in California and avail itself of California's laws, renders the application of California law to the claims herein constitutionally permissible.

141. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Classes, and California has a greater interest in applying its laws here than any other interested state.

[61] Facebook Terms of Service, https://www.facebook.com/legal/terms (last visited July 21, 2022).

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class and Subclasses)
Against Meta

142. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

143. Plaintiff asserts claims for intrusion upon seclusion and so must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which Plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

144. Meta's collection and use of Plaintiff and Class members' sensitive User Data, including the user's name, email address, phone number, information entered into forms, the doctor's name, the search term used to find the doctor (i.e., "heart disease"), the condition selected from any dropdown menus (i.e., "Alzheimer's"), the users' medications, information regarding their allergies, and details about their upcoming doctor's appointments, constitutes an intentional intrusion upon Plaintiff and Class members' solitude or seclusion in that Meta collected these sensitive details that were intended to stay private from third parties without users' consent.

145. Plaintiff and Class members had a reasonable expectation of privacy in their User Data, including sensitive medical information. Plaintiff and Class members did not consent to, authorize, or know about Meta's intrusion at the time it occurred. Plaintiff and Class members never agreed that Meta could collect or disclose their User Data, including sensitive medical information.

146. Plaintiff and Class members did not consent to, authorize, or know about Meta's intrusion at the time it occurred. Plaintiff and Class members never agreed that their sensitive medical information would be collected or used by Meta.

147. Meta's intentional intrusion on Plaintiff's and Class members' solitude or seclusion without consent would be highly offensive to a reasonable person. Plaintiff and Class members reasonably expected that their sensitive User Data would not be collected or used.

148. The surreptitious taking and disclosure of sensitive User Data from thousands if not millions of individuals was highly offensive because it violated expectations of privacy that have been established by social norms. Privacy polls and studies show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is collected or shared.

149. Given the nature of the User Data Meta collected and disclosed, such as the user's name, email address, phone number, information entered into forms, the doctor's name, the search term used to find the doctor (i.e., "heart disease"), the condition selected from any dropdown menus (i.e., "Alzheimer's"), the users' medications, information regarding their allergies, and details about their upcoming doctor's appointments, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

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

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

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

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

154. Plaintiff also seeks such other relief as the Court may deem just and proper.

SECOND CLAIM FOR RELIEF
Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(On Behalf of Plaintiff and the Class and Subclasses)
Against Meta

155. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

156. 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." California Constitution, Article I, Section 1.

157. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (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.

158. The right to privacy in California's constitution creates a right of action against private and government entities.

159. Plaintiff and Class members have and continue to have a reasonable expectation of privacy in their personal information, identities, and User Data pursuant to Article I, Section I of the California Constitution.

160. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances, including that: (i) the User Data collected by Defendant Meta included personal, sensitive medical information, decisions, and medical diagnoses; and (ii) Plaintiff and Class members did not consent or otherwise authorize Meta to collect and use this private information for their own monetary gain.

161. The confidential and sensitive User Data, which Meta intruded upon, intercepted, collected, and disclosed without Plaintiff's and Class members' authorization or consent, included sensitive medical information, such as the user's name, email address, phone number, information entered into forms, the doctor's name, the search term used to find the doctor (i.e., "heart disease"), the condition selected from any dropdown menus (i.e., "Alzheimer's"), the users' medications, information regarding their allergies, and details about their upcoming doctor's appointments.

162. Meta's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the data collected was highly sensitive and personal, as protected by the California Constitution; (ii) Defendants did not have authorization or consent to collect this information; and (iii) the invasion deprived Plaintiff and Class members the ability to control the circulation of said information, which is considered a fundamental right to privacy.

163. Meta's invasion violated the privacy rights of hundreds of thousands of Class members, including Plaintiff, without authorization or consent. Their conduct constitutes a severe and egregious breach of social norms.

164. As a result of Meta's actions, Plaintiff and Class members have sustained damages and will continue to suffer damages as a direct and proximate result of Meta's invasion of privacy.

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

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

167. Plaintiff also seeks such other relief as the Court may deem just and proper.

THIRD CLAIM FOR RELIEF
Violation Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class and Subclasses)

Against Healthcare Defendants

168. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

169. 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 have a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

170. Healthcare Defendants' disclosure of Plaintiff' and Class members' sensitive User Data, including the user's name, email address, phone number, information entered into forms, the doctor's name, the search term used to find the doctor (i.e., "heart disease"), the condition selected from any dropdown menus (i.e., "Alzheimer's"), the users' medications, information regarding their allergies, and details about their upcoming doctor's appointments, constitutes an intentional intrusion upon Plaintiff and Class members' solitude or seclusion in that Healthcare Defendants disclosed these sensitive details that were intended to stay private from third parties without users' consent.

171. Plaintiff and Class members had a reasonable expectation of privacy in their User Data, including sensitive medical information. Plaintiff and Class members did not consent to, authorize, or know about Healthcare Defendants' intrusion at the time it occurred. Plaintiff and Class members never agreed that Healthcare Defendants could disclose their User Data, including sensitive medical information.

172. Healthcare Defendant's intentional intrusion on Plaintiff's and Class members' solitude or seclusion without consent would be highly offensive to a reasonable person. Plaintiff and Class members reasonably expected that their sensitive User Data would not be disclosed.

173. The surreptitious taking and disclosure of sensitive User Data from thousands if not millions of individuals was highly offensive because it violated expectations of privacy that have been established by social norms. Privacy polls and studies show that the overwhelming majority of

Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is collected or shared.

174. Given the highly sensitive nature of the User Data Healthcare Defendants disclosed, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

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

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

177. Plaintiff and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class members for the harm to their privacy interests as well as a disgorgement of profits made by Healthcare Defendants as a result of its intrusions upon Plaintiff's and Class members' privacy.

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

179. Plaintiff also seeks such other relief as the Court may deem just and proper.

FOURTH CLAIM FOR RELIEF
Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(On Behalf of Plaintiff and the and Subclasses)
Against Healthcare Defendants

180. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

181. 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." California Constitution, Article I., Section 1.

182. To state a claim for invasion of privacy under the California Constitution, a plaintiff must allege (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.

183. The right to privacy in California's constitution creates a right of action against private and government entities.

184. Plaintiff and Class members have and continue to have a reasonable expectation of privacy in their personal information, identities, and User Data pursuant to Article One, Section One of the California Constitution.

185. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances, including that: (i) the User Data disclosed by Healthcare Defendants included personal, sensitive medical information, decisions, and medical diagnoses; and (ii) Plaintiff and Class members did not consent or otherwise authorize Healthcare Defendants to share and disclose this private information for their own monetary gain.

186. The confidential and sensitive User Data, which Healthcare Defendants intruded upon and disclosed without Plaintiff's and Class members' authorization or consent, included the user's name, email address, phone number, information entered into forms, the doctor's name, the search term used to find the doctor (i.e., "heart disease"), the condition selected from any dropdown menus (i.e., "Alzheimer's"), the users' medications, information regarding their allergies, and details about their upcoming doctor's appointments.

187. Healthcare Defendants' actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the data disclosed was highly sensitive and personal, as protected by the California Constitution; (ii) Defendants did not have authorization or consent to disclose this information; and (iii) the invasion deprived Plaintiff and Class members the ability to control the circulation of said information, which is considered a fundamental right to privacy.

188. Healthcare Defendants' invasion violated the privacy rights of hundreds of thousands of Class members, including Plaintiff, without authorization or consent. Their conduct constitutes a severe and egregious breach of social norms.

189. Plaintiff and Class members have sustained damages and will continue to suffer damages as a direct and proximate result of Healthcare Defendants' conduct, including an invasion of privacy.

190. Plaintiff and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class members for the harm to their privacy interests as well as a disgorgement of profits made by Healthcare Defendants as a result of its intrusions upon Plaintiff's and Class members' privacy.

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

192. Plaintiff also seeks such other relief as the Court may deem just and proper.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff and the Class and Subclasses)
Against Meta

193. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

194. Meta received benefits from Plaintiff and Class members and unjustly retained those benefits at their expense.

195. Plaintiff and Class members conferred a benefit upon Meta in the form of valuable sensitive medical information that Meta collected from Plaintiff and Class members, without authorization and proper compensation. Meta has collected and used this information for its own gain, providing Meta with economic, intangible, and other benefits, including substantial monetary compensation from third parties who utilize Meta's advertising services.

196. Meta unjustly retained those benefits at the expense of Plaintiff and Class members because Defendant's conduct damaged Plaintiff and Class members, all without providing any commensurate compensation to Plaintiff and Class members.

197. The benefits that Meta derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles in California and every other state for Meta to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

198. Meta should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Meta received, and such other relief as the Court may deem just and proper.

SIXTH CLAIM FOR RELIEF
Violation of California Confidentiality of Medical Information Act
Civil Code Section 56.06
("CMIA")
(On Behalf of Plaintiff and the Class and Subclasses)
Against Healthcare Defendants

199. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

200. Healthcare Defendants are deemed providers of health care under Cal. Civ. Code. Section 56.06, subdivision (a) and (b), because they maintain medical information and offer software to consumers that is designed to maintain medical information for the purposes of allowing its users to manage their information or for the diagnosis, treatment, or management of a medical condition.

201. Healthcare Defendants are therefore subject to the requirements of the CMIA and obligated under subdivision (b) to maintain the same standards of confidentiality required of a provider of health care with respect to medical information that it maintains on behalf of users.

202. Healthcare Defendants violated Civil Code section 56.06 because they did not maintain the confidentiality of users' medical information. Instead, Healthcare Defendants disclosed

to third parties Plaintiff's and Class members' medical information without consent, including information concerning physical and emotional health, family planning, as well as their interests in making personal decisions or conducting personal activities.

203. This information was shared with third parties, including Meta, whose business is to sell advertisements based on that data it collects about individuals, including the data Plaintiff and the Class shared with Healthcare Defendants.

204. Healthcare Defendants knowingly and willfully disclosed medical information without consent to Meta for financial gain. Namely, to market and advertise its services, or to allow others to market and advertise their services, in violation of Civil Code section 56.06 subdivisions (b) and (c). Healthcare Defendants conduct was knowing and willful as they were aware that Meta Pixel would collect all User Data inputted while using their website, yet intentionally embedded Meta Pixel anyway.

205. At the very least, HealthCare Defendants negligently disclosed medical information to Meta in violation of Civil Code section 56.06 subdivisions (b) and (c).

206. Accordingly, Plaintiff and Class 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 56.36(c); and reasonable attorneys' fees and other litigation costs reasonably incurred.

SEVENTH CLAIM FOR RELIEF
Violation of CMIA
Civil Code Section 56.101
(On Behalf of Plaintiff and the Class and Subclasses)
Against Healthcare Defendants

207. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

208. Civil Code section 56.101, subdivision (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."

209. Any health care provider who "negligently creates, maintains, preservers, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36."

210. Healthcare Defendants failed to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein because it disclosed to Meta, Plaintiff's and Class members' sensitive medical information without consent, including information concerning their health status, medical diagnoses, treatment, and appointment information, as well as PII.

211. Healthcare Defendants' failure to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information was, at the least, negligent and violates Civil Code section 56.06 subdivisions (b) and (c).

212. Accordingly, Plaintiff and Class 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 56.36(c); and reasonable attorneys' fees and other litigation costs reasonably incurred.

EIGHTH CLAIM FOR RELIEF
Violation of CMIA
Civil Code Section 56.10
(On Behalf of Plaintiff and the Class and Subclasses)
Against Healthcare Defendants

213. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

214. Civil Code section 56.10, subdivision (a), prohibits a health care provider from disclosing medical information without first obtaining an authorization, unless a statutory exception applies.

215. Healthcare Defendants disclosed medical information without first obtaining authorization when it disclosed to third parties Plaintiff's and Class members' sensitive medical information without consent, including information concerning their health status, medical

diagnoses, treatment, and appointment information, as well as PII. No statutory exception applies. As a result, Healthcare Defendants violated Civil Code section 56.10, subdivision (a).

216. Healthcare Defendants knowingly and willfully disclosed medical information without consent to Meta for financial gain. Namely, to market and advertise its services, or to allow others to market and advertise their services, in violation of Civil Code section 56.06 subdivisions (b) and (c).

217. At the very least, Healthcare Defendants negligently disclosed medical information in violation of Civil Code section 56.06 subdivisions (b) and (c) through the unauthorized disclosure of Plaintiff's and Class members' sensitive medical information.

218. Accordingly, Plaintiff and Class 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 56.36(c); (4) punitive damages pursuant to 56.35; and (5) reasonable attorneys' fees and other litigation costs reasonably incurred.

NINTH CLAIM FOR RELIEF
Aiding and Abetting Violation of California CMIA
Civil Code Section 56.06, 56.101, 56.10
(On Behalf of Plaintiff and the Class and Subclasses)
Against Meta

219. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

220. As set forth herein, Healthcare Defendants' disclosure of Plaintiff's and Class members sensitive medical information violates the CMIA.

221. By contracting with Healthcare Defendants to receive and use Plaintiff's and Class members' sensitive medical information, as well as providing the means to accomplish this objective, Meta acted intentionally or, alternatively, with knowledge that Healthcare Defendants' misappropriation of Plaintiff's and Class members' sensitive medical information was a violation of the CMIA.

222. Meta provided substantial assistance and encouragement to Healthcare Defendant's violation of the CMIA, including by provided the means, i.e., Meta Pixel, to share and disclose this data. Meta knew that Meta Pixel could be seamlessly integrated without altering users that their sensitive medical information would be shared with Meta.

223. Meta's agreements with Healthcare Defendants and receipt of Meta's sensitive medical information is a substantial factor in causing the violations of the CMIA alleged herein.

224. For example, in the absence of Meta Pixel, provided by Meta, Healthcare Defendants would likely not have shared Plaintiff's and Class members sensitive medical information.

225. Given the lucrative value of Plaintiff's and Class members' sensitive medical information, Meta was willing to receive, and encouraged, Healthcare Defendants to share this data.

226. As a result, Meta aided and abetted Healthcare Defendants' CMIA violations and are therefore jointly liable with Healthcare Defendants for the relief sought by Plaintiffs and the Class.

TENTH CLAIM FOR RELIEF
Violations of Cal. Bus. & Prof. Code §§ 17200 *et. seq.*
(On Behalf of the Facebook Subclasses)
Against Meta

227. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

228. Meta's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq*. ("UCL"), because, as alleged above, Meta violated the California common law, California Constitution, and the other statutes and causes of action described herein.

229. Meta's business acts and practices are "unfair" under the UCL. California has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data. Meta violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise misusing Plaintiff's and Class members' sensitive medical information without Plaintiff's and Class members' consent. Meta's conduct violates the policies of the statutes referenced herein.

230. Meta's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Meta secretly collecting, disclosing, and otherwise misusing Plaintiff's and Class members' sensitive medical information is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and Class members were completely unaware of Meta's conduct, they could not have possibly avoided the harm.

231. Meta's business acts and practices are also "fraudulent" within the meaning of the UCL. Meta has amassed a large collection of sensitive medical information without disclosing this practice and therefore acted without consumers' knowledge or consent.

232. In fact, Meta expressly told Facebook users that it would receive data ***only*** from its "partners" who are "require[d]" to have "lawful rights to collect, use and share [users'] data before providing any data to [Meta]." This would not include User Data collected from Healthcare Defendants, as this information is protected by the Health Insurance Portability and Accountability Act of 1996's ("HIPAA") Privacy Rule, which prohibits the disclosure of this information without authorization from the user. *See* 45 C.F.R. § 160.103. Meta's conduct was fraudulent because it represented to users that their User Data would not be collected, but did so anyway.

233. Meta's business acts and practices were likely to, and did, deceive members of the public including Plaintiff and Class members into believing this data was private.

234. Meta's violations were, and are, willful, deceptive, unfair, and unconscionable.

235. Had Plaintiff and Class members known that their sensitive medical information would be collected, associated with their Facebook, Instagram, or other social media accounts provided by Meta, and used by Meta for its own benefit, they would not have used these services.

236. Plaintiff and Class members have a property interest in their sensitive medical information. By surreptitiously collecting and otherwise misusing Plaintiff's and Class members' information, Defendants have taken property from Plaintiff and Class members without providing just or any compensation.

237. Plaintiff and Class members have lost money and property as a result of Meta's conduct in violation of the UCL. Health data, as well as PII, collected and used by Meta objectively has value. Companies are willing to pay for health data, like the data unlawfully collected and used by Meta. For instance, Pfizer annually pays approximately $12 million to purchase health data from various sources.[62]

238. Consumers also value their health data. According to the annual Financial Trust Index Survey, conducted by the University of Chicago's Booth School of Business and Northwestern University's Kellogg School of Management, which interviewed more than 1,000 Americans, 93 percent would not share their health data with a digital platform for free. Half of the survey respondents would only share their data for $100,000 or more, and 22 percent would only share their data if they received between $1,000 and $100,000.[63]

239. By deceptively collected and using this data, Meta has taken money or property from Plaintiff and Class members.

240. For these reasons, Plaintiff seek restitution and compensatory damages on behalf of herself and Class members.

ELEVENTH CLAIM FOR RELIEF
Violation of the Federal Wiretap Act
18 U.S.C §§ 2510, *et seq.*
(On Behalf of Plaintiff and the Class and Subclasses)
Against Meta

241. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

---

[62] Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, SCI. AM. (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

[63] Andrea Park, *How much should health data cost? $100K or more, according to patients*, BECKER'S HOSP. REV. (Feb. 12, 2020), https://www.beckershospitalreview.com/healthcare-information-technology/how-much-should-health-data-cost-100k-or-more-according-to-patients.html.

242. The Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

243. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

244. "Contents" is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

245. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

246. "Electronic communication" is defined 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 interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

247. Meta is a person for purposes of the Wiretap Act because it is a corporation.

248. The Meta Pixel is a "device or apparatus" that is "used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(4).

249. Plaintiff's and Class members' sensitive medical information which was intercepted by Defendants through the Meta Pixel are "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

250. Plaintiff and Class members reasonably expected that Meta was not intercepting, recording, or disclosing their electronic communications.

251. Plaintiff's and Class members' electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing

their private information, including by using their private information to develop marketing and advertisement strategies.

252. Interception of Plaintiff's and Class members' private and confidential electronic communications without their consent occurs whenever users engage with the hospital or patient portals to schedule an appointment. Meta is not party to these communications.

253. Meta's actions were at all relevant times knowing, willful, and intentional, particularly because Meta is a sophisticated party who know the type of data they intercept through their own products, i.e., SDKs.

254. Neither Plaintiff nor the Class consented to Defendant's interception, disclosure, and/or use of their sensitive User Data in their electronic communications with the hospital or patient portals. Nor could they—Meta, nor Healthcare Defendants never sought to, or did, obtain Plaintiff's or the Class members' consent.

255. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class and any profits made by Advertiser Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

TWELFTH CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 630, *et seq*. ("CIPA")
(On Behalf of Plaintiff and the Class and Subclasses)
Against Meta

256. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

257. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA") finding 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." *Id.* § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

258. Cal. Penal Code § 632 prohibits eavesdropping upon or recording of any confidential communication, including those occurring among the parties in the presence of one another or by means of a telephone, telegraph, or other device, through the use of an electronic amplifying or recording device without the consent of all parties to the communication.

259. By contemporaneously intercepting and accessing Plaintiff's and Class members' sensitive medical information communicated to the hospital or patient portals, Meta, without consent and authorization of all parties, eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 631(a) of the CIPA.

260. Meta utilized Plaintiff's and Class members' personal health information for their own purposes, including for advertising.

261. Plaintiff and the Class members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

262. Plaintiff and Class members have also suffered irreparable injury from these unauthorized acts of disclosure, their personal, private, and sensitive medical information have been collected, viewed, accessed, stored, and used by Meta, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, Plaintiff and Class members are entitled to injunctive relief.

THIRTEENTH CLAIM FOR RELIEF
Violation of the Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502
("CDAFA")

(On Behalf of Plaintiff and the Class and Subclasses)

263. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

264. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA") to "expand the degree of protection afforded . . . from tampering, interference, damage, and unauthorized access to [including the extraction of data from] lawfully created computer data and computer systems," finding and declaring that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals . . ." Cal. Penal Code § 502(a).

265. Plaintiff's and the Classes' devices on which they accessed the hospital or patient portals, including their computers, smart phones, and tablets, constitute "computers, computer systems, and/or computer networks" within the meaning of the CDAFA. *Id.* § 502(b)(5).

266. Meta violated § 502(c)(1)(B) of the CDAFA by knowingly accessing without permission Plaintiff's and Class members' devices in order to wrongfully obtain and use their personal data, including their sensitive medical information, in violation of Plaintiff and Class members' reasonable expectations of privacy in their devices and data.

267. Meta violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking, copying, and using Plaintiff's and the Class members' personally identifiable information, including their sensitive medical information.

268. The computers and mobile devices that Plaintiff and Class members used when accessing hospital or patient portals all have and operate "computer services" within the meaning of the CDAFA. Defendants violated §§ 502(c)(3) and (7) of the CDAFA by knowingly and without permission accessing and using those devices and computer services, and/or causing them to be accessed and used, *inter alia*, in connection with Meta's wrongful collection of such data.

269. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information." Defendant violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via Meta Pixel embedded into the hospital or patient portals which intercepted Plaintiff's and the Class members' private and sensitive medical information.

270. Plaintiff and Class members suffered damage and loss as a result of Defendant's conduct. Defendant's practices have deprived Plaintiff and the Class members of control over their valuable property (namely, their sensitive medical information), the ability to receive compensation for that data, and the ability to withhold their data for sale.

271. Plaintiff and the Class members seek compensatory damages in accordance with California Penal Code § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

272. Plaintiff and Class members have also suffered irreparable and incalculable harm and injuries from Defendant's violations. The harm will continue unless Defendants are enjoined from further violations of this section. Plaintiff and Class members have no adequate remedy at law.

273. Plaintiff and Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendants' violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiff and the Class members are also entitled to recover their reasonable attorneys' fees under § 502(e)(2).

FOURTEENTH CLAIM FOR RELIEF
Breach of Contract
(On Behalf of Plaintiff and the Class and Subclasses)
Against Healthcare Defendants

274. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

275. Healthcare Defendants expressly promised to safeguard Plaintiff's and Class members' User Data, including sensitive medical information.

276. For instance, Defendant UCSF Medical Center represents on its website that it is "committed to protecting [patients'] medical information."[64] Its "Notice of Privacy Practices" packet explicitly state that UCSF will only disclose patients' medical information for explicit reasons, none of which state that UCSF Medical Center will disclose PII and sensitive medical information to Meta for Meta's own use. Similarly, its "Privacy Statement" under the heading "Sharing of data" explicitly states that "Personal information is not disclosed ***without your consent*** other than as required by laws." UCSF's MyChart page simply states: "Your privacy is important to us. The information you provide on this web site is protected by federal laws. To learn more about how your rights to privacy are being protected, please contact the Customer Service Department."[65]

277. Likewise, Defendant Dignity Health Medical Foundation states in its Notice of Privacy Practices that it "understand[s] that [patients'] protected health information is privacy and personal" and that it is "committed to protecting it." In accordance with this representation, Defendant Dignity Health Medical Foundation promises not to disclose User Data, including sensitive health information, without "written permission" when it seeks to use this information in connection with marketing.

278. Plaintiff and Class members accepted Healthcare Defendants' promises not to disclose their User Data without explicit consent and/or authorization when they entered into contracts with Healthcare Defendants in which they paid money for medical services and/or treatment.

279. Plaintiff and Class members fully performed their obligations under their contracts with Healthcare Defendants, including by providing their User Data and paying for medical services and/or treatment.

---

[64] https://www.ucsfhealth.org/medical-records

[65] UCSF MyChart - Login Page (ucsfmedicalcenter.org) (last viewed on July 21, 2022).

280. Healthcare Defendants did not hold up their end of the bargain. Healthcare Defendants secretly disclosed Plaintiff and Class member's User Data, including sensitive medical information, to Meta without consent in violation of their agreement with Plaintiff and Class members.

281. Plaintiff and Class members would not have entrusted Healthcare Defendants with their User Data in the absence of a contract between them and Healthcare Defendants obligating them not to disclose this information.

282. As a direct and proximate result of Healthcare Defendants' breaches of their contracts, Plaintiffs and Class members sustained damages as alleged herein. Plaintiffs and Class members would not have used Healthcare Defendants' services, or would have paid substantially less for these services, had they known their User Data would be disclosed.

283. Plaintiff and Class members are entitled to compensatory and consequential damages as a result of Healthcare Defendants' breach of contract.

FIFTEENTH CLAIM FOR RELIEF
Breach of Implied Contract
Civil Code Section 56.06, 56.101, 56.10
(On Behalf of Plaintiff and the Class and Subclasses)
(In the alternative)
Against Healthcare Defendants

284. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

285. When Plaintiff and Class members paid money and provided their User Data to Healthcare Defendants in exchange for services, they entered implied contracts pursuant to which Healthcare Defendants agreed to safeguard and not disclose their User Data without consent.

286. Plaintiff and Class members accepted Healthcare Defendants' offers and provided their User Data to Defendants.

287. Plaintiff and Class members would not have entrusted Healthcare Defendants with their User Data in the absence of an implied contract between them and Healthcare Defendants obligating them not to disclose this information without consent.

288. Healthcare Defendants breached these implied contracts by disclosing Plaintiff and Class members' User Data to a third party, i.e., Meta.

289. As a direct and proximate result of Healthcare Defendants' breaches of these implied contracts, Plaintiffs and Class members sustained damages as alleged herein. Plaintiffs and Class members would not have used Healthcare Defendants' services, or would have paid substantially less for these services, had they known their User Data would be disclosed.

290. Plaintiff and Class members are entitled to compensatory and consequential damages as a result of Healthcare Defendants' breach of implied contract.

SIXTEENTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff and the Class and Subclasses)
Against Healthcare Defendants
(In the Alternative)

291. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

292. Plaintiff and Class members conferred a benefit upon Healthcare Defendants in the form of valuable sensitive medical information that Healthcare Defendants collected from Plaintiff and Class members under the guise of keeping this information private. Healthcare Defendants collected and used this information for its own gain, including for advertisement purposes or sale. Additionally, Plaintiff and Class members conferred a benefit upon Healthcare Defendants in the form of monetary compensation.

293. Plaintiff and Class members would not have used Healthcare Defendants services, or would have paid less for these services, if they had known Healthcare Defendants would use and disclose this information.

294. Healthcare Defendants unjustly retained those benefits at the expense of Plaintiff and Class members because Defendant's conduct damaged Plaintiff and Class members, all without providing any commensurate compensation to Plaintiff and Class members.

295. The benefits that Healthcare Defendants derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable under unjust enrichment

principles in California and every other state for Healthcare Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

296. Healthcare Defendants should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class respectfully requests that the Court enter an order:

A. Certifying the Classes and appointing Plaintiff as the Classes' representative;

B. Appoint the law firms Lowey Dannenberg, P.C., and Labaton Sucharow LLP as proposed interim class counsel;

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

D. Awarding declaratory relief against Defendant;

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

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

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

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

Dated: July 25, 2022

/s/*Frank Busch*
Frank Busch (258288)
James M. Wagstaffe (95535)
WAGSTAFFE, VON LOEWENFELDT, BUSCH & RADWICK LLP

100 Pine Street, Suite 2250
San Francisco, CA 94111
Tel: (415) 357-8900
Fax: (415) 357-8910
wagstaffe@wvbrlaw.com
busch@wvbrlaw.com

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
Rachel Kesten (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com

Carol C. Villegas (*pro hac vice forthcoming*)
Michael P. Canty (*pro hac vice forthcoming)*
Melissa H. Nafash (*pro hac vice forthcoming*)
LABATON SUCHAROW LLP
140 Broadway, Floor 34
New York, NY 10005
Tel: (212) 907-0700
Fax: (212) 818-0477
cvillegas@labaton.com
mcanty@labaton.com
mnafash@labaton.com