

Alexander A. Baehr, WSBA #25320
SUMMIT LAW GROUP, PLLC
315 Fifth Avenue S, Suite 1000
Seattle, WA 98104
Telephone: (206) 676-7000

Ekwan E. Rhow (pro hac vice forthcoming)
Marc E. Masters (pro hac vice forthcoming)
Barr Benyamin (pro hac vice forthcoming)
BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067
Telephone: (310) 201-2100

Jonathan M. Rotter (pro hac vice forthcoming)
Kara M. Wolke (pro hac vice forthcoming)
Pavithra Rajesh (pro hac vice forthcoming)
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

JANE DOE, Individually and on Behalf of All
Others Similarly Situated,

Plaintiff,

v.

MICROSOFT CORPORATION, a
Washington Corporation; QUALTRICS
INTERNATIONAL INC., a Delaware
Corporation; and QUALTRICS LLC, a
Delaware Limited Liability Company,

Defendants.

Case No. 2:23-cv-718

COMPLAINT – CLASS ACTION

DEMAND FOR JURY TRIAL

1 Plaintiff Jane Doe (“Plaintiff”), individually and on behalf of all others similarly situated,
2 for her complaint against Microsoft Corporation, Qualtrics International, Inc., and Qualtrics LLC
3 (together, “Defendants”) alleges the following upon information and belief, except as to those
4 allegations concerning Plaintiff, which are alleged upon personal knowledge.

5 **I. NATURE AND OVERVIEW OF THE ACTION**

6 1. Patients rightfully expect that their healthcare will be private. And the law protects
7 the privacy of healthcare information. This case is about a serious violation of that core privacy
8 interest.

9 2. Plaintiff, like millions of other class members, obtains healthcare from Kaiser
10 Permanente (“Kaiser”). As is true for any medical provider, the law protects the privacy of the
11 healthcare information held by Kaiser and exchanged between Plaintiff and Class Members, on the
12 one hand, and Kaiser, on the other.

13 3. One place that legal protection is important is the Kaiser Website, which Kaiser
14 Members use to access their medical records, including prescriptions and immunizations, research
15 their medical conditions, find and communicate with doctors, and undertake other interactions
16 related to the provision of healthcare services.

17 4. Unfortunately and unlawfully, Defendants repeatedly and systematically have
18 violated that legally-protected privacy interest by extracting private healthcare and other
19 information from Kaiser Members’ communications with the Kaiser Website.

20 5. Through Defendants’ code implemented on the Kaiser Website, Defendants have
21 vacuumed up information about Kaiser Members’ medical conditions, immunizations,
22 prescriptions, physician information, and other private data, including healthcare search terms,
23 videos watched, and links accessed. And all of that information is linked to particular patients
24 because Defendants each take that data together with unique identifiers that allow Defendants to
25 identify the Kaiser Member.

26

1 6. Plaintiff and class members did not consent to Defendants’ taking this highly
2 sensitive and legally-protected medical and other information. Defendants’ conduct is unlawful, and
3 it must be stopped.

4 **II. PARTIES**

5 7. Plaintiff Jane Doe is a resident of California. She is suing as a Jane Doe because the
6 confidentiality of her patient status is protected by law, as explained below. She has been a Kaiser
7 Member for at least 10 years and has used the Kaiser Website throughout her membership. She has
8 an account on the Kaiser Website. While logged into that account, she used the search function;
9 accessed immunization and medical records; made appointments; reviewed physician information;
10 reviewed medical conditions; and watched videos. As more fully explained below, Defendants
11 unlawfully intercepted and collected such data along with her personal identifiers.

12 8. Defendant Microsoft Corporation (“Microsoft”) is a publicly traded company
13 incorporated under the laws of Washington with its principal executive offices located in Redmond,
14 Washington. Microsoft offers computer hardware and software products for business and personal
15 users, including data analytics and cloud-computing applications. Among Microsoft’s various
16 business segments is its Search and News Advertising Business, which “is designed to deliver
17 relevant search, native, and display advertising to a global audience.”¹

18 9. Defendant Qualtrics International, Inc. is a Delaware corporation, and Defendant
19 Qualtrics LLC is a Delaware limited liability company (“Qualtrics”). Qualtrics’ principal places of
20 business are located in Seattle, Washington and in Provo, Utah. Qualtrics offers a cloud-based
21 subscription software platform for “experience management” for other organizations.

22 **III. JURISDICTION AND VENUE**

23 10. The Court has personal jurisdiction over Defendants because they each have
24 sufficient minimum contacts with this District in that each Defendant operates and markets its

25 ¹ Microsoft, Form 10-K for the period ended June 30, 2022 at 15 (July 28, 2022),
26 https://www.sec.gov/ix?doc=/Archives/edgar/data/0000789019/000156459022026876/msft-10k_20220630.htm

1 services throughout this State. Additionally, Defendants Microsoft and Qualtrics are headquartered
2 in this District.

3 11. This Court has subject matter jurisdiction pursuant to the Computer Fraud and Abuse
4 Act, 18 U.S.C. § 1030, *et seq.* The Court has supplemental jurisdiction over the remaining state law
5 claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or
6 controversy.

7 12. The Court also has subject matter jurisdiction pursuant to the Class Action Fairness
8 Act of 2005, 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds \$5 million,
9 exclusive of interest and costs, and Plaintiff is diverse from each Defendant.

10 13. Venue is proper in this District because a substantial part of the events or omissions
11 giving rise to the claim occurred in this District. Specifically, Defendants’ principal executive
12 offices are located in this District.

13 **IV. SUBSTANTIVE ALLEGATIONS**

14 **A. The Health Insurance Portability and Accountability Act (“HIPAA”)**

15 14. Patient health care information in the United States is protected by federal law under
16 the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing
17 regulations promulgated by the United States Department of Health and Human Services (“HHS”).

18 15. The HIPAA Privacy Rule establishes national standards to protect individuals’
19 medical records and other individually identifiable health information (collectively defined as
20 “protected health information” or “PHI”) and applies to health plans, health care clearinghouses,
21 and those health care providers that conduct certain health care transactions electronically. The Rule
22 requires appropriate safeguards to protect the privacy of protected health information and sets limits
23 and conditions on the uses and disclosures that may be made of such information without an
24 individual’s authorization. The Rule also gives individuals rights over their protected health
25 information, including rights to examine and obtain a copy of their health records, to direct a covered
26 entity to transmit to a third party an electronic copy of their protected health information in an

1 electronic health record, and to request corrections. The Privacy Rule is located at 45 CFR Part 160
2 and Subparts A and E of Part 164. <https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html>.

3 16. Under 45 C.F.R. § 164.502, a health care provider or business associate of a health
4 care provider “may not use or disclose ‘protected health information’ except as permitted or required
5 by” the HIPAA Privacy Rule.

6 17. Under 45 C.F.R. 160.103, the Privacy Rule defines “protected health information”
7 or PHI as “individually identifiable health information” that is “transmitted by electronic media;
8 maintained in electronic media; or transmitted or maintained in any other form or medium.”

9 18. Under 45 C.F.R. § 160.103, the Privacy Rule defines “individually identifiable health
10 information” as “a subset of health information, including demographic information collected from
11 an individual” that is (1) “created or received by a health care provider;” (2) “[r]elates to the past,
12 present, or future physical or mental health or condition of an individual; the provision of health
13 care to an individual; or the past, present, or future payment for the provision of health care to an
14 individual;” and (3) either (a) identifies the individual; or (b) with respect to which there is a
15 reasonable basis to believe the information can be used to identify the individual.”

16 19. Under 45 C.F.R. § 164.514, the HIPAA de-identification rule states that “health
17 information is not individually identifiable only if” (1) an expert “determines that the risk is very
18 small that the information could be used, alone or in combination with other reasonably available
19 information, by an anticipated recipient to identify an individual who is a subject of the information”
20 and “documents the methods and results of the analysis that justify such determination” or (2) “the
21 following identifiers of the individual or of relatives, employers, or household members of the
22 individual are removed: Names ... Medical record numbers; ... Account numbers ... Device
23 identifiers and serial numbers; ... Web Universal Resource Locators (URLs); Internet Protocol (IP)
24 address numbers; ... and any other unique identifying number, characteristic, or code.” In addition,
25 the covered entity must not “have actual knowledge that the information could be used alone or in
26 combination with other information to identify an individual who is a subject of the information.”

1 20. Under 42 U.S.C. § 1320d-6, any “person [individual ... or a corporation] who
2 knowingly and in violation of this part—(1) uses or causes to be used a unique health identifiers;
3 [or] (2) obtains individually identifiable health information relating to an individual ... shall be
4 punished” by fine or, in certain circumstances, imprisonment, with increased penalties for “intent to
5 sell, transfer, or use individually identifiable health information for commercial advantage[.]” The
6 statute further provides that a “person ... shall be considered to have obtained or disclosed
7 individually identifiable health information ... if the information is maintained by a covered entity
8 ... and the individual obtained or disclosed such information without authorization.”

9 21. Patient status (i.e., information connecting an individual with a healthcare provider)
10 alone is protected by HIPAA. See *In re Meta Pixel Healthcare Lit.*, 2022 U.S. Dist. LEXIS 230754,
11 *27-28 (N.D. Cal. Dec. 22, 2022) (holding that patient status is protected information under
12 HIPAA); *Arvidson v. Buchar*, No. ST-16-cv-410, 2018 WL 10613032, at *10 (V.I. Super. Ct. June
13 6, 2018) (ruling that patient names and a patient list were PHI which were therefore subject to special
14 disclosure requirements under HIPAA); *Use of Online Tracking Technologies by HIPAA Covered*
15 *Entities and Business Associates*, U.S. Health & Human Services (HHS guidance instructing that
16 information which connect an individual with a healthcare provider “is indicative that the individual
17 has received or will receive health care services,” and thus “relates to the individual’s past, present,
18 or future health or health care or payment for care”) (content current as of [*28] Dec. 1, 2022),
19 <https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-onlinetracking/index.html>.

20 22. Guidance from HHS instructs health care providers that patient status is protected by
21 HIPAA. In *Guidance Regarding Methods for De-identification of Protected Health Information in*
22 *Accordance with the Health Insurance Portability and Accountability Act Privacy Rule*, HHS sets
23 out:

24 Identifying information alone, such as personal names, residential
25 addresses, or phone numbers, would not necessarily be designated as
26 PHI. For instance, if such information was reported as part of a
 publicly accessible data source, such as a phone book, then this
 information would not be PHI because it is not related to health data.

1 ... *If such information was listed with health condition, health care*
2 *provision or payment data, such as an indication that the individual*
3 *was treated at a certain clinic, then this information would be PHI.*²

4 23. In its guidance for Marketing, HHS further instructs:

5 The HIPAA Privacy Rule gives individuals important controls over
6 whether and how their protected health information is used and
7 disclosed for marketing purposes. With limited exceptions, the
8 Rule requires an individual’s written authorization before a use
9 or disclosure of his or her protected health information can be made
10 for marketing. ... Simply put, a covered entity may not sell
11 protected health information to a business associate or any other
12 third party for that party’s own purposes. Moreover, *covered entities*
13 *may not sell lists of patients to third parties without obtaining*
14 *authorization from each person on the list.*³

15 24. HHS has previously instructed that HIPAA covers patient-status alone:

- 16 (a) “The sale of a patient list to a marketing firm” is not permitted under HIPAA.
17 65 Fed. Reg. 82717 (Dec. 28, 2000);
- 18 (b) “A covered entity must have the individual’s prior written authorization to use
19 or disclose protected health information for marketing communications,”
20 which would include disclosure of mere patient status through a patient list. 67
21 Fed. Reg. 53186 (Aug. 14, 2002);
- 22 (c) It would be a HIPAA violation “if a covered entity impermissibly disclosed a
23 list of patient names, addresses, and hospital identification numbers.” 78 Fed.
24 Reg. 5642 (Jan. 25, 2013); and
- 25 (d) The only exception permitting a hospital to identify patient status without
26 express written authorization is to “maintain a directory of individuals in its
 facility” that includes name, location, general condition, and religious

²https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/Deidentification/hhs_deid_guidance.pdf at 5 (emphasis added).

³ <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/marketing.pdf> at 1-2 (emphasis added).

1 affiliation when used or disclosed to “members of the clergy” or “other persons
2 who ask for the individual by name.” 45 C.F.R. § 164.510(1). Even then,
3 patients must be provided an opportunity to object to the disclosure of the fact
4 that they are a patient. 45 C.F.R. § 164.510(2).

5 25. There is no HIPAA-exception for the Internet or online patient portals.

6 26. Plaintiff, Class Members, and Subclass Members have not given consent to
7 Defendants’ possession or use of Plaintiff, Class Members, and Subclass Members’ PHI.

8 27. More broadly, even outside the HIPAA context, there is no consent to a third party
9 intercepting and collecting one’s private information data unless the individual understands that she
10 is authorizing the third party to collect such private medical information. And the third party must
11 expressly and specifically disclose that it may acquire the individual’s *medical information* and not
12 just the individual’s information in a general sense. *See In re Meta Pixel Healthcare Lit.*, --- F. Supp.
13 3d. ---, 2022 U.S. Dist. LEXIS 230754, *30-31 (N.D. Cal. Dec. 22, 2022) (holding that plaintiffs
14 did not consent to Meta’s collection of their medical information where Meta’s policies did not
15 “specifically indicate that Meta may acquire *health data* obtained from Facebook users’ interactions
16 with their *medical providers’* websites,” since “[Meta’s] generalized notice is not sufficient to
17 establish consent”).

18 **B. Background on Kaiser and its Website**

19 28. Third-party Kaiser Permanente (“Kaiser”) is an integrated managed care consortium
20 of for-profit and non-profit entities that is headquartered in Oakland, California. It operates 39
21 hospitals across eight states (California, Washington, Oregon, Colorado, Hawaii, Georgia,
22 Maryland, and Virginia).⁴ Kaiser serves a total of 12.6 million members, and approximately 9.4
23 million of them (or roughly 75%) reside in California.

24
25
26 ⁴ <https://about.kaiserpermanente.org/who-we-are/fast-facts>

1 29. Kaiser operates a website at <https://healthy.kaiserpermanente.org/> (the “Kaiser
2 Website”) through which it communicates with its members (“Kaiser Members”) and non-members
3 who use the Kaiser Website. By logging into their individual patient portal (“Kaiser Account”),
4 Kaiser Members can make appointments, search for doctors, review and manage their prescriptions,
5 and review their medical records and medical history more broadly.

6 30. Unbeknownst to Kaiser Members, code on the Kaiser Website includes software
7 development kits (“SDKs”) offered by Defendants Microsoft and Qualtrics that intercept and collect
8 Kaiser Members’ activity and their private medical data. These SDKs intercept and collect search
9 terms, videos watched, and the URLs of links that are accessed, all of which are associated with
10 unique user identifiers that are collected and enable each Defendant to identify the Kaiser Member
11 associated with the data. The Defendants’ SDKs covertly employ their tracking code such that
12 Kaiser Members have no indication that their web activity is transmitted to Defendants.

13 31. None of the Defendants’ SDKs are necessary for medically services.

14 **C. Each of the Defendants’ SDKs Collects Personal Data, PII, and PHI from Kaiser**
15 **Members**

16 32. Each of the Defendants’ SDKs collects a vast array of user data and content based
17 on a user’s browsing activity on the Kaiser Website, including a user’s personally identifiable
18 information (“PII”), a user’s PHI, a user’s search terms entered in the Kaiser Website, the URLs of
19 each page on the Kaiser Website that a user navigates to and/or from, the videos on the Kaiser
20 Website a user views, and/or the unique user identifiers a particular SDK associates with a user
21 (collectively, “Private Data”).

22 **1. Microsoft**

23 33. The Kaiser Website code includes Microsoft’s SDK (the “Microsoft SDK”). The
24 Microsoft SDK is tracking software that collects a user’s internet data through several unique user
25 identifiers and cookies. The unique user identifiers and cookies that the Microsoft SDK utilizes to
26

1 collect a user's data include the user's: (i) Microsoft Machine Unique Identifier ("MUID"); (ii)
2 Windows Live ID ("WLID"); and (iii) and the user's WLS identifier ("WLS").

3 34. The MUID cookie is a unique user identifier used for advertising, site analytics, and
4 other operational purposes, which links the user data it collects to a specific user and consists of an
5 alphanumeric string.

6 35. The WLID is a unique user identifier assigned to a specific user that consists of an
7 alphanumeric string and the user's name.

8 36. The WLS is a unique user identifier assigned to a specific user that consists of an
9 alphanumeric string. The WLS also includes a user's real name.

10 37. The Microsoft SDK also collects and sends to Microsoft identifying information
11 about a user's web browser, which it collectively terms "User-Agent" ("User Agent Data").

12 38. As integrated into the Kaiser Website, the Microsoft SDK intercepts and collects a
13 plethora of Private Data, including PII and PHI, from Kaiser Members when they use the Kaiser
14 Website without their knowledge or consent. The Private Data intercepted and collected includes,
15 as further described herein, search queries, visited webpages, videos, prescriptions, medical
16 conditions, immunization records, and allergies.

17 39. **Search Queries:** The Kaiser Website contains an integrated search bar that allows
18 visitors to the Kaiser Website to search for information on Kaiser's Website using search terms,
19 similar to using an Internet search engine like Google or Yahoo. Whenever a user on Kaiser's
20 Website utilizes the search bar on Kaiser's Website to search for information, the Microsoft SDK
21 intercepts and collects the search terms entered by the user, along with unique user identifiers
22 associated with the user, including MUID, WLID, and WLS. The unique user identifiers allow
23 Microsoft to link the search terms to a specific Kaiser Website user and identify the Kaiser Website
24 user. Microsoft's ability to identify the Kaiser Website user is enhanced by the SDK's collection of
25 User Agent Data.

1 40. The Microsoft SDK intercepts and collects all search queries, without discerning
2 their sensitivity, including, for example, those related to specific medical conditions a Kaiser
3 Website user is afflicted with, symptoms a Kaiser Website user is experiencing, or medications a
4 Kaiser Website user is prescribed.

5 41. Kaiser Website users, including Plaintiff and the Class Members, are unaware that
6 Microsoft is intercepting and collecting the above-described data through its SDK, and have not
7 provided their consent, whether implied or express, for Microsoft to obtain this data.

8 42. **Visited Webpages:** The Microsoft SDK intercepts and collects the URL (*i.e.*, web
9 address) and/or title of each page on the Kaiser Website that a Kaiser Website user navigates to, the
10 URL of the webpage from which the Kaiser Website user navigated to the newly-visited page, and
11 the unique user identifiers associated with the Kaiser Website user, including MUID, WLID, and
12 WLS. The unique user identifiers allow Microsoft to link the visited webpage to a specific Kaiser
13 Website user and identify that Kaiser Website user. Microsoft's ability to identify the Kaiser
14 Website user is enhanced by the SDK's collection of User Agent Data. The collection of a Kaiser
15 Website user's visited URLs and/or their titles occurs regardless of whether the Kaiser Website user
16 is logged into her Kaiser Account.

17 43. Furthermore, as explained below, when a Kaiser Member is logged into her Kaiser
18 Account through the Kaiser Website, the collected URLs and webpage titles divulge to Microsoft
19 some or all of the Kaiser Member's medical history and PHI, including the medications the Kaiser
20 Member is prescribed, the medical conditions the Kaiser Member suffers from, the Kaiser Member's
21 immunization record, and the Kaiser Member's allergies. Such URLs and page titles, when linked
22 with unique user identifiers such as MUID, WLID, and WLS, allow Microsoft to link medical
23 information, including PHI, to individual Kaiser Members.

24 44. Kaiser Website users, including Kaiser Members accessing their Kaiser Accounts
25 through the Kaiser Website, such as Plaintiff and the Class Members, are unaware that Microsoft is
26

1 collecting the above-described data through its SDK, and have not provided their consent, whether
2 implied or express, for Microsoft to obtain this data.

3 45. **Videos:** The Kaiser Website contains various videos that are available for Kaiser
4 Website users to watch. When a Kaiser Website user accesses a video on the Kaiser Website, the
5 Microsoft SDK intercepts and collects the URL of the webpage on which the video appears and the
6 title of the video, along with unique user identifiers associated with the Kaiser Website user,
7 including MUID, WLID, and WLS. The unique user identifiers allow Microsoft to link the accessed
8 video to a specific Kaiser Website user and identify the Kaiser Website user. Microsoft's ability to
9 identify the Kaiser Website user is enhanced by the SDK's collection of User Agent Data. The
10 collection and transfer of data relating to videos on the Kaiser Website occurs regardless of whether
11 the Kaiser Website user is logged in to her Kaiser Account.

12 46. Kaiser Website users, including Plaintiff and the Class Members, are unaware that
13 Microsoft is collecting the above-described data through its SDK, and have not provided their
14 consent, whether implied or express, for Microsoft to obtain this data.

15 47. **Prescriptions:** When logged in to her Kaiser Account on the Kaiser Website, a
16 Kaiser Member is able to view each of her prescribed medications by navigating to her personalized
17 "Prescription Details" page. When viewing her list of medications, a Kaiser Member is able to click
18 on a medication to navigate to a webpage within Kaiser's "Drug encyclopedia" with additional
19 information about that medication in order to learn more about it. Unbeknownst to Kaiser Members,
20 when a Kaiser Member clicks on a medication and navigates to that medication's "Drug
21 encyclopedia" webpage, the Microsoft SDK intercepts and collects: (i) the URL of that page, which
22 includes the medication's reference number in Kaiser's "Drug encyclopedia" and sometimes the
23 medication's name; (ii) the title of that page, which includes the medication's name; (iii) the URL
24 of the page from which the Kaiser Member is navigating (*i.e.*, the Kaiser Member's personalized
25 "Prescription Details" page accessed from her Kaiser Account); and (iv) the Kaiser Member's
26 MUID, WLID and/or WLS. The unique user identifiers allow Microsoft to link the prescribed

1 medication to a specific Kaiser Member and identify the Kaiser Member. Microsoft’s ability to
2 identify the Kaiser Member is enhanced by the SDK’s collection of User Agent Data. Additionally,
3 since the Microsoft SDK also intercepts and collects the URL from which the Kaiser Member is
4 navigating—the Kaiser Member’s personalized “Prescription Details” page, which is only
5 accessible when the Kaiser Member logs in to her Kaiser Account—Microsoft is able to determine
6 that the individual is, in fact, a Kaiser Member, and that the medication is prescribed to the Kaiser
7 Member.

8 48. The above-described data is PHI, since it is individually identifiable health
9 information that is transmitted by electronic media, maintained in electronic media, or transmitted
10 or maintained in any other form or medium.

11 49. Kaiser Members, including Plaintiff and the Class Members, are unaware that
12 Microsoft is collecting the above-described data through its SDK, and have not provided their
13 consent, whether implied or express, for Microsoft to obtain this data.

14 50. **Medical Conditions:** When logged in to her Kaiser Account through the Kaiser
15 Website, a Kaiser Member is able to view each of her medical conditions by navigating to her
16 personalized “Medical Record” page and then further navigating to her personalized “Health
17 summary” page. When viewing her list of medical conditions, each listed condition contains a
18 hyperlink reading “Learn more” that, when clicked, automatically runs a search on the Kaiser
19 Website for that medical condition using the name of the condition as a search query and navigates
20 the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst
21 to Kaiser Members, when a Kaiser Member clicks on the “Learn more” hyperlink for a given
22 medical condition, the Microsoft SDK intercepts and collects: (i) the URL of the page containing
23 the search results, which contains the name of the medical condition used for the search query and
24 reveals that the user navigated from her personalized “Health Summary” subpage within her
25 “Medical Record” page accessed from her Kaiser Account; (ii) the title of the page containing the
26 search results, which identifies that the Kaiser Member navigated from her personalized “Medical

1 Record” page; and (iii) the Kaiser Member’s MUID, WLID and/or WLS. The unique user
2 identifiers allow Microsoft to link the medical condition to a specific Kaiser Member and identify
3 the Kaiser Member. Microsoft’s ability to identify the Kaiser Member is enhanced by the SDK’s
4 collection of User Agent Data. Additionally, since the Microsoft SDK also intercepts and collects
5 data revealing the page from which the Kaiser Member is navigating—the Kaiser Member’s
6 personalized “Health summary” page, which is only accessible when the Kaiser Member logs in to
7 her Kaiser Account—as well as data showing that the Kaiser Member accessed the page containing
8 the search results from her personal “Medical Record” page more generally, Microsoft is aware that
9 the individual is a Kaiser Member and that the Kaiser Member suffers from the medical condition.

10 51. The above-described data is PHI, since it is individually identifiable health
11 information that is transmitted by electronic media, maintained in electronic media, or transmitted
12 or maintained in any other form or medium.

13 52. Kaiser Members, including Plaintiff and the Class Members, are unaware that
14 Microsoft is collecting the above-described data through the SDK, and have not provided their
15 consent, whether implied or express, for Microsoft to obtain this data.

16 53. **Immunization Record:** When logged in to her Kaiser Account through the Kaiser
17 Website, a Kaiser Member is able to view each of her immunizations by navigating to her
18 personalized “Medical Record” page, from there navigating to her personalized “Health summary”
19 page, and then selecting the “Immunizations” tab. When viewing her list of immunizations, each
20 listed immunization contains a hyperlink reading “Learn more” that, when clicked, automatically
21 runs a search on the Kaiser Website for the immunization using the name of the immunization as a
22 search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the
23 search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the “Learn
24 more” hyperlink for a given immunization, the Microsoft SDK intercepts and collects: (i) the URL
25 of the page containing the search results, which contains the name of the immunization used for the
26 search query and reveals that the user navigated from her personalized “Medical Record” page

1 accessed from her Kaiser Account; (ii) the title of the page containing the search results, which
2 identifies that the Kaiser Member navigated from her personalized “Medical Record” page; (iii) the
3 URL of the specific subpage within her “Medical Record” page from which the Kaiser Member is
4 navigating (*i.e.*, the Kaiser Member’s personalized “Immunizations” page); and (iv) the Kaiser
5 Member’s MUID, WLID and/or WLS. The unique user identifiers allow Microsoft to link the
6 immunization to a specific Kaiser Member and identify the Kaiser Member. Microsoft’s ability to
7 identify the Kaiser Member is enhanced by the SDK’s collection of User Agent Data. Additionally,
8 since the Microsoft SDK intercepts and collects the specific URL from which the Kaiser Member
9 is navigating—the Kaiser Member’s personalized “Immunizations” page, which is only accessible
10 when the Kaiser Member logs in to her Kaiser Account—as well as data showing that the Kaiser
11 Member accessed the page containing the search results from her personal “Medical Record” page
12 more generally, Microsoft is able to determine that the individual is a Kaiser Member and that the
13 Kaiser Member has received the immunization.

14 54. The above-described data is PHI, since it is individually identifiable health
15 information that is transmitted by electronic media, maintained in electronic media, or transmitted
16 or maintained in any other form or medium.

17 55. Kaiser Members, including Plaintiff and the Class Members, are unaware that
18 Microsoft is collecting the above-described data through the SDK, and have not provided their
19 consent, whether implied or express, for Microsoft to obtain this data.

20 56. **Allergies:** When logged in to her Kaiser Account on the Kaiser Website, a Kaiser
21 Member is able to view each of her allergies by navigating to her personalized “Medical Record”
22 page, from there navigating to her personalized “Health summary” page, and then selecting the
23 “Allergies” tab. When viewing her list of allergies, each listed allergy contains a hyperlink reading
24 “Learn more” that, when clicked, automatically runs a search on the Kaiser Website for the allergy
25 using the name of the allergy as a search query and navigates the Kaiser Member to a webpage on
26 the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser

1 Member clicks on the “Learn more” hyperlink for a given allergy, the Microsoft SDK intercepts and
2 collects: (i) the URL of the page containing the search results, which contains the name of the allergy
3 used for the search query and reveals that the user navigated from her personalized “Medical
4 Record” page accessed from her Kaiser Account; (ii) the title of the page containing the search
5 results, which identifies that the Kaiser Member navigated from her personalized “Medical Record”
6 page; and (iii) the Kaiser Member’s MUID, WLID and/or WLS. The unique user identifiers allow
7 Microsoft to link the allergy to a specific Kaiser Member and identify the Kaiser Member.
8 Microsoft’s ability to identify the Kaiser Member is enhanced by the SDK’s collection of User
9 Agent Data. Additionally, since the Microsoft SDK also intercepts and collects data showing that
10 the Kaiser Member accessed the page containing the search results from her personal “Medical
11 Record” page, Microsoft is able to determine that the individual is a Kaiser Member and that the
12 Kaiser Member suffers from the allergy.

13 57. The above-described data is PHI, since it is individually identifiable health
14 information that is transmitted by electronic media, maintained in electronic media, or transmitted
15 or maintained in any other form or medium.

16 58. Kaiser Members, including Plaintiff and the Class Members, are unaware that
17 Microsoft is collecting the above-described data through the SDK, and have not provided their
18 consent, whether implied or express, for Microsoft to obtain this data.

19 59. Microsoft is knowingly and intentionally intercepting and collecting, through the
20 SDK, the above-identified data from users of the Kaiser Website, including PHI from Kaiser
21 Members who access their Kaiser Account.

22 2. Qualtrics

23 60. Kaiser incorporates into the Kaiser Website Qualtrics’ Experience Management Site
24 Intercept software (“Site Intercept”). Site Intercept is a tracking software that collects a user’s
25 internet data through several unique user identifiers and cookies. The unique user identifiers and
26

1 cookies that Site Intercept utilizes to collect a user’s data include the user’s: (i) Anonymous Survey
2 ID (“ASID”); (ii) Contact ID; and (iii) Survey Instance ID (“SIID”).

3 61. The ASID is a unique user identifier assigned to a specific user that consists of a
4 numeric string.

5 62. The CID is a unique user identifier assigned to a specific user that consists of an
6 alphanumeric string. The CID is stored in a first-party cookie on a user’s computer, and it allows
7 Qualtrics to track the respondent across web pages. The CID is associated with the user’s account
8 in Qualtrics, which allows Qualtrics to store the user’s data.

9 63. The SIID is a unique user identifier assigned to a specific user that consists of an
10 alphanumeric string. The SID is stored in a first-party cookie on a user’s computer, and it allows
11 Qualtrics to track the user and to associate the responses with their CID.

12 64. In addition to the above-identified unique user identifiers and/or cookies, Site
13 Intercept also utilizes the following additional unique user identifiers and/or cookies associated with
14 users of the Kaiser Website: (i) ZoneID and/or ZID; (ii) InterceptID; (iii) ActionSetID; and (iv)
15 CreativeID (collectively the “Additional Qualtrics Identifiers”). A Kaiser Website user’s ZoneID
16 and/or ZID identifier or cookie is an alphanumeric string. A Kaiser Website user’s InterceptID
17 identifier and/or cookie is an alphanumeric string that has the same value as the user’s SIID. A
18 Kaiser Website user’s ActionSetID identifier or cookie is an alphanumeric string that has the same
19 value as the user’s ASID. A Kaiser Website user’s CreativeID is an alphanumeric string with the
20 same value as the user’s CID.

21 65. Site Intercept also collects and sends to Qualtrics identifying information about a
22 user’s web browser, which it collectively terms “User-Agent” (“User Agent Data”).

23 66. As integrated into Kaiser Website, Site Intercept collects and sends to Qualtrics user
24 data and identifying information, including PII and PHI, in three steps (“Qualtrics’ Data Collection
25 Process”). First, Site Intercept sends to Qualtrics’ servers a user’s ASID, CID, and SIID. Next, Site
26 Intercept sends to Qualtrics’ servers the additional user data described below, including a user’s

1 medical information, where it is combined with the user's ASID, CID, and SIID, along with the
2 Additional Qualtrics Identifiers. Through this step, Qualtrics is able to link users to their medical
3 information. Finally, Qualtrics' servers send a packet of digital data containing the user's unique
4 user identifiers and medical data back to the user's internet browser. Through these steps of data
5 transference, Qualtrics is able to match specific users to their medical information.

6 67. As integrated into the Kaiser Website, Site Intercept collects a plethora of Private
7 Data, including PII and PHI, from Kaiser Members when they use the Kaiser Website without their
8 knowledge or consent. The Private Data collected includes, as further described herein, search
9 queries, visited webpages, videos, prescriptions, medical conditions, immunization records, and
10 allergies.

11 68. **Search Queries:** The Kaiser website contains an integrated search bar that allows
12 visitors to the Kaiser Website to search for information on Kaiser's Website using search terms,
13 similar to using an Internet search engine like Google or Yahoo. Whenever a user on Kaiser's
14 Website utilizes the search bar on Kaiser's Website to search for information, Site Intercept
15 intercepts and collects the search terms entered by the user, along with unique user identifiers
16 associated with the user, including ASID, CID, and SSID, through Qualtrics' Data Collection
17 Process. The unique user identifiers allow Qualtrics to link the search terms to a specific user and
18 identify the user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of
19 User Agent Data.

20 69. Site Intercept collects all search queries, without discerning their sensitivity,
21 including, for example, those related to specific medical conditions a user is afflicted with,
22 symptoms a user is experiencing, or medications a user is prescribed.

23 70. Kaiser Members, including Plaintiff and the Class Members, are unaware that
24 Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have
25 not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser
26 to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

1 71. **Visited Webpages:** Site Intercept also intercepts and collects the URL (*i.e.*, web
2 address) and/or title of each page on the Kaiser Website that a user navigates to and the unique user
3 identifiers associated with the user, including ASID, CID, and SSID, through Qualtrics' Data
4 Collection Process. The unique user identifiers allow Qualtrics to link the visited webpage to a
5 specific user and identify the user. Qualtrics' ability to identify the user is enhanced by Site
6 Intercept's collection of User Agent Data. The collection of a user's visited URLs and/or their titles
7 occurs regardless of whether the user is logged into her Kaiser Account.

8 72. Furthermore, as explained below, when a Kaiser Member is logged into her Kaiser
9 account, the collected URLs and webpage titles may divulge to Qualtrics a large swath of the user's
10 medical history and PHI, including the medications a user is prescribed, the medical conditions a
11 user suffers from, the user's immunization record, the user's allergies, and the results of a user's
12 medical tests. Such URLs and page titles, when linked with unique user identifiers such as ASID,
13 CID, and SSID, allow Qualtrics to link medical information, including PHI, to individual users.

14 73. Kaiser Website users, including Kaiser Members accessing their Kaiser Accounts
15 through the Kaiser Website, such as Plaintiff and the Class Members, are unaware that Qualtrics is
16 intercepting and collecting the above-described data through Site Intercept, and have not provided
17 their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser to allow
18 Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

19 74. **Videos:** The Kaiser Website contains various videos that are available for users to
20 watch. When a user accesses a video on the Kaiser Website, Site Intercept intercepts and collects
21 the URL of the webpage on which the video appears, along with unique user identifiers associated
22 with the user, including ASID, CID, and SSID, through Qualtrics' Data Collection Process. The
23 unique user identifiers allow Qualtrics to link the accessed video to a specific user and identify the
24 user. Qualtrics' ability to identify the user is enhanced by Site Intercept's collection of User Agent
25 Data. The interception and collection of data relating to videos on the Kaiser Website occurs
26 regardless of whether the user is logged in to her Kaiser Account.

1 75. Kaiser Members, including Plaintiff and the Class Members, are unaware that
2 Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have
3 not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser
4 to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

5 76. **Prescriptions:** When logged in to her Kaiser Account on the Kaiser Website, a
6 Kaiser Member is able to view each of her prescribed medications by navigating to her personalized
7 “Prescription Details” page. When viewing her list of medications, a Kaiser Member is able to click
8 on a medication to navigate to a webpage within Kaiser’s “Drug encyclopedia” with additional
9 information about that medication in order to learn more about it. Unbeknownst to Kaiser Members,
10 when a Kaiser Members clicks on a medication and navigates to that medication’s “Drug
11 encyclopedia” webpage, Site Intercept intercepts and collects: (i) the URL for that page, which
12 includes the medication’s reference number in Kaiser’s “Drug encyclopedia” and sometimes the
13 medication’s name; and (ii) the user’s ASID, CID, and SSID, through Qualtrics’ Data Collection
14 Process. The unique user identifiers allow Qualtrics to link the prescribed medication to a specific
15 user, identify the user. Qualtrics’ ability to identify the user is enhanced by Site Intercept’s
16 collection of User Agent Data.

17 77. The above-described data is PHI, since it is individually identifiable health
18 information that is transmitted by electronic media, maintained in electronic media, or transmitted
19 or maintained in any other form or medium.

20 78. Kaiser Members, including Plaintiff and the Class Members, are unaware that
21 Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have
22 not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser
23 to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

24 79. **Medical Conditions:** When logged in to her Kaiser Account on the Kaiser Website,
25 a Kaiser Member is able to view each of her medical conditions by navigating to her personalized
26 “Medical Record” page and then further navigating to her personalized “Health summary” page.

1 When viewing her list of medical conditions, each listed condition contains a hyperlink reading
2 “Learn more” that, when clicked, automatically runs a search on the Kaiser Website for that medical
3 condition using the name of the condition as a search query and navigates the Kaiser Member to a
4 webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members,
5 when a Kaiser Member clicks on the “Learn more” hyperlink for a given medical condition, Site
6 Intercept intercepts and collects: the URL of the page containing the search results, which contains
7 the name of the medical condition used for the search query and reveals that the user navigated from
8 her personalized “Health Summary” subpage within her “Medical Record” page accessed from her
9 Kaiser Account; and (ii) the user’s ASID, CID, and SSID, through Qualtrics’ Data Collection
10 Process. The unique user identifiers allow Qualtrics to link the medical condition to a specific user
11 and identify the user. Qualtrics’ ability to identify the user is enhanced by Site Intercept’s collection
12 of User Agent Data. Additionally, since Site Intercept also intercepts and collects data showing that
13 the user accessed the page containing the search results from her personalized “Health Summary”
14 page, and from her personalized “Medical Record” page more generally, which are only accessible
15 when the user logs in to her Kaiser Account, Qualtrics is aware that the user is a Kaiser Member,
16 and that the user suffers from the medical condition.

17 80. The above-described data is PHI, since it is individually identifiable health
18 information that is transmitted by electronic media, maintained in electronic media, or transmitted
19 or maintained in any other form or medium.

20 81. Kaiser Members, including Plaintiff and the Class Members, are unaware that
21 Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have
22 not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser
23 to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

24 82. **Immunization Record:** When logged in to her Kaiser Account on the Kaiser
25 Website, a Kaiser Member is able to view each of her immunizations by navigating to her
26 personalized “Medical Record” page, from there navigating to her personalized “Health summary”

1 page, and then selecting the “Immunizations” tab. When viewing her list of immunizations, each
2 listed immunization contains a hyperlink reading “Learn more” that, when clicked, automatically
3 runs a search on the Kaiser Website for the immunization using the name of the immunization as a
4 search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the
5 search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the “Learn
6 more” hyperlink for a given immunization, Site Intercept intercepts and collects: (i) the URL of the
7 page containing the search results, which contains the name of the immunization used for the search
8 query and reveals that the user navigated from her personalized “Medical Record” page accessed
9 from her Kaiser Account; and (ii) the user’s ASID, CID, and SSID, through Qualtrics’ Data
10 Collection Process. The unique user identifiers allow Qualtrics to link the immunization to a
11 specific user and identify the user. Qualtrics’ ability to identify the user is enhanced by Site
12 Intercept’s collection of User Agent Data. Additionally, since Site Intercept also intercepts and
13 collects data showing that the user accessed the page containing the search results from her
14 personalized “Medical Record” page, which is only accessible when the user logs in to her Kaiser
15 Account, Qualtrics is aware that the user is a Kaiser Member, and that the user has received the
16 immunization.

17 83. The above-described data is PHI, since it is individually identifiable health
18 information that is transmitted by electronic media, maintained in electronic media, or transmitted
19 or maintained in any other form or medium.

20 84. Kaiser Members, including Plaintiff and the Class Members, are unaware that
21 Qualtrics is intercepting and collecting the above-described data through Site Intercept, and have
22 not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser
23 to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

24 85. **Allergies:** When logged in to her Kaiser Account on the Kaiser Website, a Kaiser
25 Member is able to view each of her allergies by navigating to her personalized “Medical Record”
26 page, from there navigating to her personalized “Health summary” page, and then selecting the

1 “Allergies” tab. When viewing her list of immunizations, each listed immunization contains a
2 hyperlink reading “Learn more” that, when clicked, automatically runs a search on the Kaiser
3 Website for the allergy using the name of the allergy as a search query and navigates the Kaiser
4 Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser
5 Members, when a Kaiser Member clicks on the “Learn more” hyperlink for a given allergy, Site
6 Intercept intercepts and collects: (i) the URL of the page containing the search results, which
7 contains the name of the allergy used for the search query and reveals that the user navigated from
8 her personalized “Medical Record” page accessed from her Kaiser Account; and (ii) the user’s
9 ASID, CID, and SSID, through Qualtrics’ Data Collection Process. The unique user identifiers
10 allow Qualtrics to link the allergy to a specific user and identify the user. Qualtrics’ ability to
11 identify the user is enhanced by Site Intercept’s collection of User Agent Data. Additionally, since
12 Site Intercept also intercepts and collects showing that the user accessed the page containing the
13 search results from her personalized “Medical Record” page, which is only accessible when the user
14 logs in to her Kaiser Account, Qualtrics is aware that the user is a Kaiser Member, and that the user
15 suffers from the allergy.

16 86. The above-described data is PHI, since it is individually identifiable health
17 information that is transmitted by electronic media, maintained in electronic media, or transmitted
18 or maintained in any other form or medium.

19 87. Kaiser Members, including Plaintiff and the Class Members, are unaware that
20 Qualtrics is intercepting and collecting the above-described data through Site Intercepts, and have
21 not provided their consent, whether implied or express, for Qualtrics to obtain this data, for Kaiser
22 to allow Qualtrics to obtain this data, or for Kaiser to share this data with Qualtrics.

23 **D. Plaintiff and the Class’s PII Has Value**

24 88. The value of personal data is well understood and generally accepted as a form of
25 currency.

1 89. It is by now incontrovertible that a robust market for this data undergirds the tech
2 economy.

3 90. The robust market for user data has been analogized to the “oil” of the tech industry.⁵
4 A 2015 article from TechCrunch accurately noted that “Data has become a strategic asset that allows
5 companies to acquire or maintain a competitive edge.”⁶ That article noted that the value of a single
6 Internet user—or really, a single user’s data—varied from about \$15 to more than \$40.

7 91. The Organization for Economic Cooperation and Development (“OECD”) itself has
8 published numerous volumes discussing how to value data such as that which is the subject matter
9 of this Complaint, including as early as 2013, with its publication “Exploring the Economic of
10 Personal Data: A Survey of Methodologies for Measuring Monetary Value”.⁷ The OECD
11 recognizes that data is a key competitive input not only in the digital economy but in all markets:
12 “Big data now represents a core economic asset that can create significant competitive advantage
13 for firms and drive innovation and growth.”⁸

14 92. In *The Age of Surveillance Capitalism*, Harvard Business School Professor
15 Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed
16 their business models from fee-for-services-provided to monetizing their users’ data—including
17 user data that is not necessary for product or service use, which she refers to as “behavioral surplus.”⁹
18 In essence, Professor Zuboff explains that revenue from user data pervades every economic

19 ⁵ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017),
20 <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data>.

21 ⁶ Pauline Glickman and Nicolas Glady, *What’s the Value of Your Data?* TechCrunch (Oct. 13, 2015),
22 <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

23 ⁷ *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value*,
OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013), <http://dx.doi.org/10.1787/5k486qtxldmq-en>.

24 ⁸ *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13, 2013),
25 https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledgecapital-growth-and-innovation_9789264193307-en.

26 ⁹ Shoshanna Zuboff, *The Age of Surveillance Capitalism* 166 (2019).

1 transaction in the modern economy. It is a fundamental assumption of these revenues that there is
2 a *market* for this data; data generated by Kaiser Members has economic value.

3 93. Professor Paul M. Schwartz writing in the Harvard Law Review, notes:

4 Personal information is an important currency in the new millennium.
5 The monetary value of personal data is large and still growing, and
6 corporate America is moving quickly to profit from the trend.
7 Companies view this information as a corporate asset and have
8 invested heavily in software that facilitates the collection of consumer
9 information.¹⁰

10 94. This economic value has been leveraged largely by corporations who pioneered the
11 methods of its extraction, analysis, and use. However, the data also has economic value to users.
12 Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize
13 their own data. For example, Nielsen Data and Mobile Computer will pay users for their data.¹¹
14 Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.¹²

15 95. There are countless examples of this kind of market, which is growing more robust
16 as information asymmetries are diminished through revelations to users as to how their data is being
17 collected and used.

18 96. As Professors Acquisti, Taylor and Wagman relayed in their 2016 article “The
19 Economics of Privacy,” published in the Journal of Economic Literature:

20 Such vast amounts of collected data have obvious and substantial
21 economic value. Individuals’ traits and attributes (such as a person’s
22 age, address, gender, income, preferences, and reservation prices, but
23 also her clickthroughs, comments posted online, photos uploaded to
24 social media, and so forth) are increasingly regarded as business

25 ¹⁰ Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055, 2056-57 (2004).

26 ¹¹ Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10, 2020),
<https://wallethacks.com/apps-for-selling-your-data/>.

¹² Jacob Kastrenakes, *A New TikTok Clone hit the top of the App Store by Paying users to watch videos*, The
Verge (May 29, 2020), <https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival>.

1 assets that can be used to target services or offers, provide relevant
2 advertising, or be traded with other parties.¹³

3 97. There is also a private market for users' personal information. One study by content
4 marketing agency Fractl has found that an individual's online identity, including hacked financial
5 accounts, can be sold for \$1,200 on the dark web.¹⁴ These rates are assumed to be discounted
6 because they do not operate in competitive markets, but rather, in an illegal marketplace. If a
7 criminal can sell other users' content, surely users can sell their own.

8 98. As to health data specifically, as detailed in an article in Canada's National Post:

9 As part of the multibillion-dollar worldwide data brokerage industry,
10 health data is one of the most sought-after commodities. De-identified
11 data can be re identified and brazen decisions to release records with
12 identifiable information are becoming commonplace).¹⁵

13 99. Further demonstrating the financial value of Class Members' medical data, CNBC
14 has reported that hospital executives have received a growing number of bids for user data:

15 Hospitals, many of which are increasingly in dire financial straits, are
16 weighing a lucrative new opportunity: selling patient health
17 information to tech companies.

18 Aaron Miri is chief information officer at Dell Medical School and
19 University of Texas Health in Austin, so he gets plenty of tech start-
20 ups approaching him to pitch deals and partnerships. Five years ago,
21 he'd get about one pitch per quarter. But these days, with huge data-
22 driven players like Amazon and Google making incursions into the
23 health space, and venture money flooding into Silicon Valley start-
24 ups aiming to bring machine learning to health care, the cadence is far
25 more frequent.

26 "It's all the time," he said via phone. "Often, once a day or more."

22 ¹³ Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature
23 2, at 444 (June 2016), <https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf>.

24 ¹⁴ Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MarketWatch
25 (June 6, 2018), [https://www.marketwatch.com/story/spooked-by-the-Googleprivacy-violations-this-is-how-much-
26 your-personal-data-is-worth-on-the-dark-web-2018-03-20](https://www.marketwatch.com/story/spooked-by-the-Googleprivacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20).

¹⁵ National Post, IRIS KULBATSKI: THE DANGERS OF ELECTRONIC HEALTH RECORDS, February 26,
2020, <https://nationalpost.com/opinion/iris-kulbatski-the-dangers-of-electronichealth-records> (last visited Dec. 29,
2022) (internal citations omitted).

* * *

1 [H]ealth systems administrators say [the data] could also be used in
2 unintended or harmful ways, like being cross-referenced with other
3 data to identify individuals at higher risk of diseases and then raise
4 their health premiums, or to target advertising to individuals.¹⁶

5 100. The CNBC article also explained:

6 De-identified patient data has become its own small economy:
7 There's a whole market of brokers who compile the data from
8 providers and other health-care organizations and sell it to buyers.
9 Just one company alone, IQVIA, said on its website that it has access
10 to more than 600 million patient records globally that are
11 nonidentified, much of which it accesses through provider
12 organizations. The buyers, which include pharma marketers, will
13 often use it for things like clinical trial recruiting

14 But hospital execs worry that this data may be used in unintended
15 ways, and not always in the patient's best interest.

16 * * *

17 Tech companies are also under particular scrutiny because they
18 already have access to a massive trove of information about people,
19 which they use to serve their own needs. For instance, the health data
20 Google collects could eventually help it micro-target advertisements
21 to people with particular health conditions. Policymakers are
22 proactively calling for a revision and potential upgrade of the health
23 privacy rules known as HIPAA, out of concern for what might happen
24 as tech companies continue to march into the medical sector.¹⁷

25 101. Time Magazine similarly, in an article titled, HOW YOUR MEDICAL DATA
26 FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, referenced the "growth of the big
health data bazaar," in which patients' health information is sold. It reported that:

[T]he secondary market in information unrelated to a patient's direct
treatment poses growing risks, privacy experts say. That's because
clues in anonymized patient dossiers make it possible for outsiders to

¹⁶ CNBC, HOSPITAL EXECs SAY THEY ARE GETTING FLOODED WITH REQUESTS FOR YOUR HEALTH DATA, <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-withrequests-for-your-health-data.html> (last visited Dec. 29, 2022).

¹⁷ *Id.*

1 determine your identity, especially as computing power advances in
2 the future.¹⁸

3 102. In short, there is economic value to users' data. The exact number will be a matter
4 for experts to determine.

5 103. Defendants have intercepted and collected Plaintiff's and Class Members' Private
6 Data, including PHI and PII, without providing anything of value to Plaintiff and Class Members in
7 exchange for that Private Data.

8 104. Defendants accessed Plaintiff's and the Class Members' Private Data, including PHI
9 and PII, without permission. The unauthorized access to Plaintiff's and Class Members' Private
10 Data, including PII and PHI, has diminished the value of that Private Data. Defendants have also
11 failed to provide any consideration for that Private Data. These actions and omissions have resulted
12 in harm to Plaintiff and Class Members.

13 **E. Defendants Intercepted and Collected Plaintiff's Private Data, Including PII
14 and PHI, Causing Plaintiff Harm**

15 105. Plaintiff has been a Kaiser Member for at least 10 years and has used the Kaiser
16 Website throughout her membership. She has an account on the Kaiser Website. While logged into
17 that account, she used the search function; accessed immunization and medical records; made
18 appointments; reviewed physician information; reviewed medical conditions; and watched videos.
19 Defendants unlawfully intercepted and collected such data along with her personal identifiers. As
20 a result of Defendants' actions, Plaintiff suffered harm.

21 **V. TOLLING, CONCEALMENT, AND ESTOPPEL**

22 106. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

23 107. The applicable statutes of limitations are tolled as a result of Defendants' knowing
24 and active concealment of their conduct alleged above.

25 ¹⁸ Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY,
26 <https://time.com/4588104/medical-data-industry/> (last visited Dec. 29, 2022).

1 108. As alleged above, Plaintiff and Class Members did not know and could not have
2 known when they used the Kaiser Website that the Defendants' SDKs were (and still are)
3 implemented on the Kaiser Website and that Defendants' SDKs would collect and intercept
4 Plaintiff's and the Class Members' Private Data, including PII and PHI. Plaintiff and the Class
5 Members could not have discovered Defendants' unlawful conduct with reasonable due diligence.

6 109. Defendants' SDKs were secretly implemented on the Kaiser Website, and no
7 indication was provided to Kaiser Members that their Private Data, including PII and PHI, would
8 be collected and intercepted by Defendants' SDKs.

9 110. Defendants had exclusive and superior knowledge that Defendants' SDKs
10 implemented on the Kaiser Website would collect and intercept Kaiser Members' personal
11 information, including PII and PHI, yet failed to disclose to Kaiser Members that by interacting with
12 the Kaiser Website their Private Data, including PII and PHI, would be collected and intercepted by
13 Defendants.

14 111. Plaintiff and Class Members could not with due diligence have discovered the full
15 scope of Defendants' conduct because the implementation of Defendants' SDKs on the Kaiser
16 Website is highly technical and there were no disclosures or other indications by Kaiser or
17 Defendants that would inform a reasonable consumer or user of the Kaiser Website that Defendants
18 were collecting and intercepting the Private Data, including PII and PHI, of Kaiser Members.

19 112. The earliest Plaintiff and Class Members could have known about Defendants'
20 conduct was shortly before the filing of this Complaint.

21 113. And when the action was filed, Defendants were under duty to disclose the true
22 character, quality, and nature of their activities to Plaintiff and the Class Members. Defendants are
23 therefore estopped from relying on any statute of limitations.

24 **VI. CLASS ACTION ALLEGATIONS**

25 114. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(1)(A)
26 and/or 23(b)(3), individually and on behalf of the following Classes.

1 First Nationwide Class: All natural persons residing in the United States who
2 are current or former Kaiser Members and had their PHI taken by Defendants
while using the Kaiser Website.

3 First California Subclass: All natural persons residing in California who are
4 current or former Kaiser Members and had their PHI taken by Defendants
5 while using the Kaiser Website.

6 Second Nationwide Class: All natural persons residing in the United States
7 who are current or former Kaiser Members and had their Private Data, other
than PHI, taken by Defendants while using the Kaiser Website.

8 Second California Subclass: All natural persons residing in California who
9 are current or former Kaiser Members and had their Private Data, other than
PHI, taken by Defendants while using the Kaiser Website.

10 115. **Numerosity:** The exact number of members of the Classes are unknown and
11 unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Classes
12 likely consist of millions of individuals, and the members can be identified through Defendants'
13 records.

14 116. **Predominant Common Questions:** The Classes' claims present common questions
15 of law and fact, and those questions predominate over any questions that may affect individual Class
16 Members. Common questions for the Classes include, but are not limited to, the following:

17 (a) Whether Defendants collected Plaintiff and Class Members' Private Data,
18 including PHI and PII, when they used the Kaiser Website;

19 (b) Whether Defendants' acts and practices violated the California Invasion of
20 Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

21 (c) Whether Defendants' acts and practices violated California's Constitution,
22 Art. 1, § 1;

23 (d) Whether Defendants' acts and practices violated Class Members' common
24 law privacy rights and/or intruded upon their seclusion;

25 (e) Whether Defendants acts and practices violated the Computer Fraud and
26 Abuse Act, 18 U.S.C. §§ 1030, *et seq.*;

1 (f) Whether Defendants were unjustly enriched;

2 (g) Whether Defendants' acts and practices violated California's Business and
3 Professions Code §§ 17200, *et seq.*;

4 (h) Whether Defendants' acts and practices violated California Penal Code §
5 496(a) and (c);

6 (i) Whether Defendants' acts and practices constitute conversion under
7 California law;

8 117. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the
9 Class. The claims of Plaintiff and the members of the Class arise from the same conduct by
10 Defendant and are based on the same legal theories. Defendant acted or refused to act on grounds
11 generally applicable to the class, and Defendant's policies and practices challenged herein apply
12 equally and uniformly to each class member, including Plaintiff.

13 118. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately
14 represent and protect the interests of the Class. Plaintiff has retained counsel competent and
15 experienced in complex litigation and class actions, including litigations to remedy privacy
16 violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant
17 has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously
18 prosecuting this action on behalf of the members of the Class, and they have the resources to do so.
19 Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of
20 the Class.

21 119. **Substantial Benefits:** This class action is appropriate for certification because class
22 proceedings are superior to other available methods for the fair and efficient adjudication of this
23 controversy and joinder of all members of the Class is impracticable. This proposed class action
24 presents fewer management difficulties than individual litigation, and provides the benefits of single
25
26

1 adjudication, economies of scale, and comprehensive supervision by a single court.¹⁹ Class
2 treatment will create economies of time, effort, and expense and promote uniform decision-making.

3 120. A class action is a particularly efficient and appropriate procedure in this case
4 because absent a class action Defendant would gain an unconscionable economic advantage.
5 Individual plaintiffs have limited resources and could be outspent many times over by Defendant.
6 Moreover, the recovery in each individual suit would not cover the cost of litigation.

7 121. Defendant's course of conduct described herein is common to each Class Member;
8 maintaining individual actions would create a risk of inconsistent results.

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

12 **VII. CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS**

13 123. California substantive law applies to every member of the Class. California
14 substantive law may be constitutionally applied to the claims of Plaintiff and the Classes under the
15 Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S.
16 Constitution. California has significant contact, or significant aggregation of contacts, to the claims
17 asserted by Plaintiff and Class Members, thereby creating state interests to ensure that the choice of
18 California state law is not arbitrary or unfair.

19 124. Defendant Microsoft's principal executive offices are located at One Microsoft Way,
20 Redmond, Washington 98052. Microsoft also maintains several offices in California and conducts
21 substantial business in California, such that California has an interest in regulating Microsoft's
22 conduct under its laws. Microsoft's decision to have offices in California and avail itself of

23 _____
24 ¹⁹ As to Fed. R. Civ. Proc. 23(b)(3)(B), Plaintiff acknowledges that a case concerning the use of SDKs on the Kaiser
25 Website was recently filed in the U.S. District Court for the Northern District of California, captioned *Doe v. Kaiser*
26 *Foundation Health Plan, Inc., et al.*, Case No. 4:23-cv-02207-DMR. However, that action is brought on behalf of
putative classes different from those defined herein, and that action does not name Microsoft or Qualtrics as
defendants.

1 California’s laws renders the application of California law to the claims herein constitutionally
2 permissible.

3 125. Defendant Qualtrics’ co-headquarters are located at 1201 2nd Ave., Suite 2700,
4 Seattle, Washington 98101 and at 333 West River Park Drive, Provo, Utah 64604. Qualtrics also
5 maintains an office in Palo Alto, California and conducts substantial business in California, such
6 that California has an interest in regulating Qualtrics’ conduct under its laws. Qualtrics’ decision to
7 have offices in California and avail itself of California’s laws renders the application of California
8 law to the claims herein constitutionally permissible.

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

13 **VIII CLAIMS FOR RELIEF**

14 **FIRST CLAIM FOR RELIEF**

15 **Violation of the California Invasion of Privacy Act**

16 **Cal. Penal Code §§ 630, 631, et seq. (“CIPA”)**

17 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

18 127. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
19 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

20 128. Defendants violated CIPA by intentionally reading or attempting to read, and/or
21 learning the contents of the online communications between (i) Plaintiff, Class Members and
22 Subclass Members, on the one hand, and (ii) the Kaiser Website, on the other, without Plaintiff,
23 Class Members, and Subclass Members’ consent. These online communications include, but are not
24 limited to, Plaintiff, Class Members, and Subclass Members’ Private Data, including PHI and PII.
25 Such data includes, among other items, search queries, medical conditions, videos, webpages
26 visited, prescriptions, immunization records, allergies, and doctor searches.

1 129. The California Legislature enacted CIPA finding that “advances in science and
2 technology have led to the development of new devices and techniques for the purpose of
3 eavesdropping upon private communications and that the invasion of privacy resulting from the
4 continual and increasing use of such devices and techniques has created a serious threat to the free
5 exercise of personal liberties and cannot be tolerated in a free and civilized society.” Cal. Penal
6 Code § 630. Thus, the intent behind CIPA is “to protect the right of privacy of the people of this
7 state.” *Id.*

8 130. Cal. Penal Code § 631(a) provides a remedy against “[a]ny person who, by means of
9 any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any
10 unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise,
11 with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or
12 instrument of any internal telephonic communication system, or who willfully and without the
13 consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to
14 read, or to learn the contents or meaning of any message, report, or communication while the same
15 is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place
16 within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to
17 communicate in any way, any information so obtained, or who aids, agrees with, employs, or
18 conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts
19 or things mentioned above in this section.”

20 131. Defendants violated § 631(a) by intercepting, storing, reading, attempting to read,
21 attempting to learn, using, and attempting to use Plaintiff, the Class Members, and the Subclass
22 Members’ Private Data, including PHI and PII, without “the consent of all parties,” while the same
23 was in transit or passing over any wire, line, or cable, or was being sent from, or received at any
24 place within California.

25 132. Unbeknownst to Plaintiff, the Class Members and the Subclass Members, the Kaiser
26 Website contains Defendants’ SDKs, which intercept, collect, and use the Private Data, including

1 PHI and PII. Such data includes, among other items, search queries, medical conditions, videos,
2 webpages visited, prescriptions, immunization records, allergies, and doctor searches.

3 133. The Private Data, including the PHI and PII, is individually identifiable health
4 information and other sensitive information that is transmitted by electronic media, maintained in
5 electronic media, or transmitted or maintained in other form or medium.

6 134. Plaintiff, Class Members, and Subclass Members' Private Data, including their PHI
7 and PII, has economic value.

8 135. Because Plaintiff, Class Members, and Subclass Members are unaware that
9 Defendants are intercepting, collecting, and using their Private Data, including PHI and PII, through
10 Defendants' SDKs, Plaintiff, Class Members, and Subclass Members could not have consented to
11 the interception, collection, and use of their Private Data, including PHI and PII, by Defendants.

12 136. On information and belief, Defendants' interception, collection, and use of Plaintiff,
13 Class Members, and Subclass Members' Private Data, including PHI and PII, is knowing and
14 intentional.

15 137. The information communicated between Plaintiff, Class Members, and Subclass
16 Members, on the one hand, and Kaiser's Website, on the other, was transmitted to and/or from the
17 state of California.

18 138. Plaintiff, Class Members, and Subclass Members seek statutory damages in
19 accordance with § 637.2(a), which provides that any person who has been injured by a violation of
20 this chapter (including § 632) may bring an action for the greater of: (1) \$5,000 per violation; or (2)
21 three times the amount of damages sustained by Plaintiff, the Class Members, and the Subclass
22 Members, in an amount to be proven at trial, as well as injunctive or other equitable relief. Plaintiff,
23 Class Members, and Subclass Members are therefore entitled to at least \$5,000 per violation.

24 139. Section 637.2(b) provides that any person may "bring an action to enjoin and restrain
25 any violation of this chapter." Plaintiff, Class Members, and Subclass Members further seek
26 injunctive relief, as they have suffered irreparable injury from Defendants' misconduct. Plaintiff,

1 Class Members, and Subclass Members' Private Data, including personal, private, and sensitive
2 medical information, has been intercepted, collected, viewed, read, learned, accessed, stored, used,
3 and transmitted by Defendants, and has not been destroyed, and due to the continuing threat of such
4 injury, Plaintiffs, Class Members, and Subclass Members have no adequate remedy at law.

5 **SECOND CLAIM FOR RELIEF**
6 **Violation of the California Invasion of Privacy Act**
7 **Cal. Penal Code §§ 632, et seq. ("CIPA")**
8 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

9 140. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
10 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

11 141. Defendants violated CIPA by using their SDKs and receiving servers (where the data
12 is saved and recorded) which are recording devices under CIPA, to eavesdrop upon the confidential
13 communications between Plaintiff, Class Members, and Subclass Members, on the one hand, and
14 Kaiser's Website, on the other.

15 142. Cal. Penal Code § 632 prohibits use of "a recording device to eavesdrop upon or
16 record [a] confidential communication" without consent of all parties to the communication. For the
17 purposes of the statute, 'confidential communication' means a communication carried on in
18 circumstances that may reasonably indicate a participant wishes the communication be confined to
19 the parties thereto. *Id.* § 632(c).

20 143. Defendants violated Cal. Penal Code § 632 by intercepting, accessing, recording,
21 eavesdropping, and transmitting Plaintiff, Class Members, and Subclass Members' Private Data,
22 including sensitive medical information, communicated with the Kaiser Website through searches
23 and clicks on that website.

24 144. Unbeknownst to Plaintiff, Class Members and Subclass Members, the Kaiser
25 Website contains Defendants' SDKs that intercept, collect, and use Plaintiff, Class Members, and
26 Subclass Members' Private Data, including PHI and PII. Such data includes, among other items,

1 search queries, medical conditions, videos, webpages visited, prescriptions, immunization records,
2 allergies, and doctor searches.

3 145. The Private Data, including PHI and PII, is individually identifiable health
4 information and other sensitive information that is transmitted by electronic media, maintained in
5 electronic media, or transmitted or maintained in other form or medium.

6 146. Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and
7 PII, has economic value.

8 147. Because Plaintiff, Class Members, and Subclass Members are unaware that
9 Defendants are collecting their Private Data, including PHI and PII, through Defendants' SDKs,
10 Plaintiff, Class Members, and Subclass Members could not have consented to the interception,
11 collection, and use of Plaintiff, Class Members, and Subclass Members' Private Data, including PHI
12 and PII, by Defendants.

13 148. On information and belief, Defendants' interception, collection, and use of Plaintiff,
14 Class Members, and Subclass Members' Private Data, including PHI and PII, is knowing and
15 intentional.

16 149. Plaintiff, Class Members, and Subclass Members seek statutory damages in
17 accordance with § 637.2(a), which provides that any person who has been injured by a violation of
18 this chapter (including § 632) may bring an action for the greater of: (1) \$5,000 per violation; or (2)
19 three times the amount of damages sustained by Plaintiff, Class Members, and Subclass Members,
20 in an amount to be proven at trial, as well as injunctive or other equitable relief. Plaintiff, Class
21 Members, and Subclass Members are therefore entitled to at least \$5,000 per violation.

22 150. Section 637.2(b) provides that any person may "bring an action to enjoin and restrain
23 any violation of this chapter." Plaintiff, Class Members, and Subclass Members further seek
24 injunctive relief, as they have suffered irreparable injury from Defendants' misconduct. Plaintiff,
25 Class Members, and Subclass Members' Private Data, including personal, private, and sensitive
26 medical information, has been intercepted, collected, viewed, read, learned, accessed, stored, used,

1 and transmitted by Defendants, and has not been destroyed, and due to the continuing threat of such
2 injury, Plaintiffs, Class Members, and Subclass Members have no adequate remedy at law.

3 **THIRD CLAIM FOR RELIEF**

4 **Violation of the Right to Privacy – California Constitution**
5 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

6 151. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
7 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

8 152. Defendants violated Article I of the California Constitution by intercepting, reading,
9 collecting, and using Plaintiff, Class Members, and Subclass Members' Private Data, including PHI
10 and PII, without Plaintiff, Class Members, and Subclass Members' consent.

11 153. The California Constitution expressly provides for a right to privacy: "All people are
12 by nature free and independent and have inalienable rights. Among these are enjoying and defending
13 life and liberty, acquiring possessing and protecting property, and pursuing and obtaining safety,
14 happiness and privacy." Cal. Const., art. I § 1.

15 154. Plaintiff, Class Members, and Subclass Members have a legally protected privacy
16 interest in their Private Data, including PHI and PII, that Defendants have intercepted, collected,
17 and used.

18 155. Plaintiff, Class Members, and Subclass Members have a reasonable expectation of
19 privacy concerning their Private Data, including PHI and PII, under the circumstances.

20 156. The reasonableness of Plaintiff, Class Members, and Subclass Members' expectations
21 of privacy are supported by the clandestine nature of Defendants' taking of Plaintiff, Class Members,
22 and Subclass Members' Private Data, including PHI and PII. Defendants acted with disregard for
23 Plaintiff, Class Members, and Subclass Members' privacy.

24 157. Defendants' conduct violated Plaintiff, Class Members, and Subclass Members'
25 privacy interests, is highly offensive to a reasonable person, and constitutes an egregious breach of
26 social norms. Defendants intentionally violated Plaintiff, Class Members, and Subclass Members'

1 privacy interests by intentionally designing their SDKs to surreptitiously intercept, collect, and use
2 Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII.

3 158. Defendants' intrusions are highly offensive to a reasonable person, as evidenced by
4 substantial research, literature, and governmental enforcement and investigative efforts to protect
5 consumer privacy against surreptitious technological intrusions.

6 159. Plaintiff, Class Members, and Subclass Members were harmed by the intrusions.

7 160. Defendants' conduct was a substantial factor in causing the harm suffered by
8 Plaintiff, Class Members, and Subclass Members.

9 161. Plaintiff, Class Members, and Subclass Members seek actual, nominal and punitive
10 damages as a result of Defendants' actions. Punitive damages are warranted because Defendants'
11 malicious, oppressive, and willful actions were calculated to injure Plaintiff, Class Members, and
12 Subclass Members, and were made in conscious disregard of Plaintiff, Class Members, and Subclass
13 Members' rights. Punitive damages are also warranted to deter Defendants from engaging in future
14 misconduct.

15 162. Plaintiff, Class Members, and Subclass Members seek restitution and disgorgement
16 for Defendants' violation of their privacy rights. A person acting in conscious disregard for the
17 rights of another must disgorge all profit because disgorgement both benefits the injured parties and
18 deters the perpetrator from committing the same unlawful actions again. Disgorgement is available
19 for conduct that constitutes "conscious interference with a claimant's legally protected interests,"
20 including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of
21 Restitution and Unjust Enrichment, §§ 40, 44.

22 **FOURTH CLAIM FOR RELIEF**
23 **Invasion of Privacy/Intrusion Upon Seclusion**
24 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

25 163. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
26 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

1 164. Defendants violated Plaintiff, Class Members, and Subclass Members' common law
2 privacy rights by intercepting, reading, collecting, and using Plaintiff, Class Members, and Subclass
3 Members' Private Data, including PHI and PII, without Plaintiff, Class Members, and Subclass
4 Members' consent.

5 165. Defendants' interception, collection, and use of this Private Data, including PHI and
6 PII, without consent is highly offensive to a reasonable person, and caused harm to Plaintiff, Class
7 Members, and Subclass Members.

8 166. Plaintiff, Class Members, and Subclass Members have a legally protected privacy
9 interest in the Private Data, including PHI and PII.

10 167. Plaintiff, Class Members, and Subclass Members reasonably expected their Private
11 Data, including PHI and PII, would remain private, and would not be intercepted, collected, or used
12 for any improper purpose or by any unauthorized parties.

13 168. Unbeknownst to Plaintiff, Class Members, and Subclass Members, the Kaiser
14 Website contains Defendants' SDKs that intercept, collect, and use Plaintiff, Class Members, and
15 Subclass Members' Private Data, including PHI and PII. Such data includes, among other items,
16 search queries, medical conditions, videos, webpages visited, prescriptions, immunization records,
17 allergies, and doctor searches.

18 169. The Private Data, including PHI and PII, is individually identifiable health
19 information and other sensitive information that is transmitted by electronic media, maintained in
20 electronic media, or transmitted or maintained in other form or medium.

21 170. Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and
22 PII, has economic value.

23 171. Because Plaintiff, Class Members, and Subclass Members are unaware that
24 Defendants are intercepting, collecting, and using their Private Data, including PHI and PII, through
25 Defendants' SDKs, Plaintiff, Class Members, and Subclass Members could not have consented to
26 the interception, collection, and use of their Private Data, including PHI and PII, by Defendants.

1 172. On information and belief, Defendants’ interception, collection, and use of Plaintiff,
2 Class Members, and Subclass Members’ Private Data, including PHI and PII, is knowing and
3 intentional.

4 173. Defendants violated Plaintiff, Class Members, and Subclass Members’ privacy rights
5 by intercepting, collecting and using such Private Data, including PHI and PII, in an unauthorized
6 manner.

7 174. Defendants did these acts without the consent of Plaintiff, Class Members, and
8 Subclass Members, and with reckless disregard for their privacy rights.

9 175. Defendants violated Plaintiff, Class Members, and Subclass Members’ privacy rights
10 guaranteed under California law, including under Article 1 Section 1 of the California Constitution
11 and California common law.

12 176. Defendants’ unlawful invasions of Plaintiff, Class Members, and Subclass Members’
13 Private Data, including PHI and PII, intruded upon and frustrated Plaintiff, Class Member, and
14 Subclass Members’ reasonable expectations of privacy. This conduct directly and proximately
15 caused Plaintiff, Class Members, and Subclass Members’ injuries.

16 177. Plaintiff, Class Members, and Subclass Members are entitled to actual and punitive
17 damages, and injunctive relief.

18 **FIFTH CLAIM FOR RELIEF**
19 **Violation of the Computer Fraud and Abuse Act (“CFAA”)**
20 **18 U.S.C. § 1030, et seq.**
21 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

22 178. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
23 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

24 179. Plaintiff, Class Members, and Subclass Members’ computer devices are, and at all
25 relevant times were, used for interstate communication and commerce and are therefore “protected
26 computers” under 18 U.S.C. § 1030(e)(2)(B).

1 180. Defendants intentionally accessed Plaintiff, Class Members, and Subclass Members
2 protected computers and obtained information thereby, and in doing so exceeded any authority
3 granted by Plaintiffs, Class Members, and Subclass Members to access the protected computers in
4 violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C). Plaintiff, Class Members, and Subclass Members have
5 a civil cause of action for violation of the CFAA under 18 U.S.C. § 1030(g) and have suffered
6 damage or loss.

7 181. Defendants violated the CFAA by intercepting, reading, collecting, and using
8 Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII, without
9 Plaintiff, Class Members, and Subclass Members' consent.

10 182. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . .
11 aggregating at least \$5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I) because the unauthorized
12 access and collection of data caused a diminution in value of Plaintiff, Class Members, and Subclass
13 Members' Private Data, including PHI and PII, both of which occurred to millions of Class
14 members, easily aggregating at least \$5,000 in value.

15 183. The interception, collection, transmission, and use of the Private Data, including PHI
16 and PII, constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV).

17 184. Plaintiff, Class Members, and Subclass Members are therefore entitled to "maintain
18 a civil action against the violator to obtain compensatory damages and injunctive relief or other
19 equitable relief." 18 U.S.C. § 1030(g).

20 **SIXTH CLAIM FOR RELIEF**
21 **Unjust Enrichment.**

22 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

23 185. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
24 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

25 186. Plaintiff, Class Members, and Subclass Members have conferred substantial benefits
26 on Defendants by virtue of their use of the Kaiser Website. These benefits include Defendants'
interception, collection, and use of Plaintiff, Class Members, and Subclass Members' Private Data,

1 including PHI and PII, and the revenues and profits resulting from targeted advertising and other
2 uses of such data by Defendants.

3 187. Defendants have knowingly and willingly accepted and enjoyed these benefits.

4 188. Defendants either knew or should have known that the benefits conferred by Plaintiff,
5 Class Members, and Subclass Members were given and received with the expectation that
6 Defendants would not intercept, collect, and use the Private Data, including PHI and PII, that
7 Defendants have intercepted, collected, and used without Plaintiff, Class Members, and Subclass
8 Members' consent. For Defendants to retain those benefits under these circumstances is inequitable.

9 189. Through deliberate violation of Plaintiff, Class Members, and Subclass Members'
10 privacy interests and statutory and constitutional rights, Defendants reaped benefits that led to each
11 Defendant wrongfully receiving profits.

12 190. Equity demands disgorgement of Defendants' ill-gotten gains. Defendants will be
13 unjustly enriched unless they are ordered to disgorge those profits for the benefit of Plaintiff, Class
14 Members, and Subclass Members.

15 191. As a direct and proximate result of Defendants' wrongful conduct and unjust
16 enrichment, Plaintiff, Class Members, and Subclass Members are entitled to restitution from
17 Defendants and the institution of a constructive trust disgorging all profits, benefits, and other
18 compensation obtained by Defendants through this inequitable conduct.

19 **SEVENTH CLAIM FOR RELIEF**
20 **Violation of the California Unfair Competition Law**
21 **Cal. Bus. & Prof. Code § 17200, et seq.**

22 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

23 192. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
24 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

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

1 194. Defendants engaged in unfair and unlawful business practices by intercepting,
2 collecting, viewing, accessing, storing, improperly using, and transmitting Plaintiff, Class Members,
3 and Subclass Members' Private Data, including PHI and PII, in violation of the UCL.

4 195. Without the consent of Plaintiff, Class Members, and Subclass Members, Defendants
5 intercepted, collected, and used this Private Data, including PHI and PII, for unauthorized purposes.
6 Defendants failed to meet legal and industry standards for protection of Plaintiff, Class Members,
7 and Subclass Members' Private Data, including PHI and PII.

8 196. The acts and omissions of Defendants constitute "business practices" within the
9 meaning of the UCL.

10 197. The Private Data, including PHI and PII, is individually identifiable health
11 information and other sensitive information that is transmitted by electronic media, maintained in
12 electronic media, or transmitted or maintained in other form or medium.

13 198. Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and
14 PII, has economic value.

15 199. Because Plaintiff, Class Members, and Subclass Members are unaware that
16 Defendants are intercepting, collecting, and using their Private Data, including PHI and PII, through
17 Defendants' SDKs, Plaintiff, Class Members, and Subclass Members could not have consented to
18 the interception, collection, and use of their Private Data, including PHI and PII, by Defendants.

19 200. On information and belief, Defendants' collection of Plaintiff, Class Members, and
20 Subclass Members' Private Data, including PHI and PII, is knowing and intentional.

21 201. Defendants violated the unlawful prong of the UCL by violating Plaintiff, Class
22 Members, and Subclass Members' constitutional rights to privacy, and state and federal privacy
23 statutes including the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the
24 Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030, *et seq.*; and California Penal Code § 496(a) and
25 (c).
26

1 202. Defendants violated the unfair prong of the UCL because their acts, omissions and
2 conduct contravened the well-established public policy interest in securing consumers’ privacy in
3 and control over their personally identifiable information, as well as the well-established public
4 policy interest in securing medical patients’ privacy in and control over their private medical and
5 health information. These interests are clearly articulated in the above referenced statutes.
6 Defendants’ conduct was immoral, unethical, oppressive and unscrupulous, and caused substantial
7 injury, including to Plaintiff, Class Members, and Subclass Members.

8 203. The harm caused by Defendants conduct outweighs any potential benefits derived
9 from such conduct. Moreover, there were reasonably available alternatives to this conduct that
10 would have allowed Defendants to achieve any legitimate business interest.

11 204. As a result of Defendants’ violations of the UCL, Plaintiff, Class Members, and
12 Subclass Members have suffered injury in fact, including lost consideration for provision of access
13 to their Private Data, including PHI and PII, and diminished value of that data.

14 205. Alternatively, Plaintiff, Class Members, and Subclass Members are entitled to
15 equitable relief to restore them to the position they would have been in had Defendants not engaged
16 in unfair and unlawful competition, and to prevent future privacy invasions. Plaintiff, Class
17 Members, and Subclass Members are entitled to an injunction, restitution, and disgorgement of all
18 profits gained as a result of Defendants’ unlawful and unfair practices.

19 **EIGHTH CLAIM FOR RELIEF**
20 **Violation of the California Penal Code § 496(a) and (c) – Statutory Larceny**
21 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

22 206. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
23 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

24 207. Pursuant to California Penal Code Section 484, “[e]very person who shall feloniously
25 steal, take, carry, lead, or drive away the personal property of another, . . . is guilty of theft.”
26

1 208. Under California law, Plaintiff, Class Members, and Subclass Members' Private
2 Data, including PHI and PII, constitutes property that may be the subject of theft. See *Calhoun v.*
3 *Google LLC*, 526 F. Supp. 3d 605 (N.D. Cal. 2021).

4 209. Defendants surreptitiously intercepted, collected, used, and exercised dominion and
5 control over Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII,
6 through Defendants' SDKs, thereby constituting theft. Such data includes, among other items,
7 search queries, medical conditions, videos, webpages visited, prescriptions, immunization records,
8 allergies, and doctor searches.

9 210. Defendants knew that this data was obtained in a manner constituting theft.

10 **NINTH CLAIM FOR RELIEF**

11 **Conversion**

12 **(On Behalf of Plaintiff, the Classes, and the Subclasses Against All Defendants)**

13 211. Plaintiff, Class Members, and Subclass Members re-allege and incorporate the
14 preceding allegations of this Complaint with the same force and effect as if fully restated herein.

15 212. Property is the right of any person to possess, use, enjoy, or dispose of a thing,
16 including intangible things such as data or communications. Under California law, Plaintiff, Class
17 Members, and Subclass Members' Private Data, including PHI and PII, constitutes property that
18 may be the subject of theft. See *Calhoun v. Google LLC*, 526 F. Supp. 3d 605 (N.D. Cal. 2021).

19 213. Defendants unlawfully intercepted, collected, used, and exercised dominion and
20 control over Plaintiff, Class Members, and Subclass Members' Private Data, including PHI and PII,
21 without authorization.

22 214. Defendants wrongfully exercised dominion and control over Plaintiff, Class
23 Members, and Subclass Members' Private Data, including PHI and PII, and have not returned it.

24 215. Plaintiff, Class Members, and Subclass Members have been damaged as a result of
25 Defendants' unlawful conversion of their property.
26

PRAYER OF RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, requests that this Court:

A. Certify the Classes and Subclasses as a class action pursuant to Federal Rule of Civil Procedure Rule 23, designate Plaintiff as the Class Representative and name the undersigned as Class Counsel;

B. Award compensatory damages, including all applicable statutory damages, for damages caused by Defendants’ wrongdoing;

C. Award punitive damages to deter Defendants from committing similar wrongdoing in the future;

D. Permanently enjoin Defendants from intercepting, collecting, and using the Private Data, including PHI and PII, without consent;

E. Order Defendants to destroy the Private Data, including PHI and PII, in their possession;

F. Award pre-judgment interest to Plaintiff, Class Members, and Subclass Members to the fullest extent allowed by law;

G. Award Plaintiff, Class Members, and Subclass Members the costs of bringing this action, including the payment of reasonable attorneys’ fees and administrative and litigation costs and expenses; and

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

1 DATED this 15th day of May, 2023.

2 Respectfully submitted,

3 SUMMIT LAW GROUP, PLLC

4 By s/ Alexander A. Baehr

5 Alexander A. Baehr, WSBA No. 25320

6 315 Fifth Avenue S, Suite 1000

7 Seattle, WA 98104

8 Telephone: (206) 676-7000

9 Email: alexb@summitlaw.com

10 BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
11 DROOKS, LINCENBERG & RHOW, PC

12 Ekwon E. Rhow (pro hac vice forthcoming)

13 Marc E. Masters (pro hac vice forthcoming)

14 Barr Benyamin (pro hac vice forthcoming)

15 1875 Century Park East, 23rd Floor

16 Los Angeles, California 90067

17 Telephone: (310) 201-2100

18 Email: erhow@birdmarella.com

19 mmasters@birdmarella.com

20 bbenyamin@birdmarella.com

21 GLANCY PRONGAY & MURRAY LLP

22 Jonathan Rotter (pro hac vice forthcoming)

23 Kara M. Wolke (pro hac vice forthcoming)

24 Pavithra Rajesh (pro hac vice forthcoming)

25 1925 Century Park East, Suite 2100

26 Los Angeles, California 90067

Telephone: (310) 201-9150

Facsimile: (310) 201-9160

Email: jrotter@glancylaw.com

kwolke@glancylaw.com

prajesh@glancylaw.com

Counsel for Plaintiff

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Microsoft, Qualtrics 'Vacuumed Up' Private Data of Kaiser Permanente Website Users, Class Action Says](#)
