

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

-----oo0oo-----

JOANNE MAGLIOCCA, individually
and on behalf of all others
similarly situated,

Plaintiffs,

v.

UNITED HEALTHCARE SERVICES,
INC., and DOES 1-100, inclusive,

Defendants.

No. 2:25-cv-3388 WBS SCR

MEMORANDUM AND ORDER RE:
DEFENDANT'S MOTION TO DISMISS
THE FIRST AMENDED COMPLAINT

-----oo0oo-----

Plaintiff brought this putative class action in Yuba County Superior Court against defendant United Healthcare Services ("UHC"), alleging violations of state and federal law in connection with UHC's purported use of third-party tracking software on its website. (Docket No. 1 at 2.) UHC timely removed the action and moved to dismiss all claims. (Docket No. 13-1.) The court granted UHC's motion to dismiss and provided plaintiff leave to amend in its order. (Docket No. 21.)

1 Plaintiff subsequently filed its First Amended Complaint ("FAC")
2 (Docket No. 23), which defendant now moves to dismiss. (Docket
3 No. 28.) Plaintiff opposes the motion. (Docket No. 29.)

4 The court granted defendant's motion to dismiss in its
5 prior order on the grounds that plaintiff lacked standing to
6 assert its claims against defendant. (See Docket No. 21 at 10.)
7 Specifically, the court held that plaintiff had failed to allege
8 a constitutionally sufficient injury-in-fact. (See id); see
9 Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

10 In her FAC, plaintiff offers new allegations describing
11 her alleged injuries resulting from UHC's third-party tracking
12 activities. For the following reasons, these allegations are
13 still not sufficient to confer standing.

14 I. UHC's Website and Plaintiff's Allegations¹

15 UHC owns and operates the website <https://www.uhc.com>
16 (the "website"). (FAC at 1.) The website utilizes third-party
17 tracking software technologies provided by the following
18 companies: Google Ads/DoubleClick, Adobe and Adobe Audience
19 Manager, Qualtrics, SessionCam, Shape Security, Datadog,
20 LivePerson, and Branch/App.link (together, the "trackers" or
21 "tracking software"). (Id.) Defendant used a "combination" of
22 sophisticated technological methods to share users' data with the
23 trackers "by deploying tools and scripts developed by these
24 companies that collected, transmitted, and processed information
25 from users who accessed the Website." (Id. at 4-9.)

26 ¹ The court summarized the facts in this matter in its
27 previous order (Docket No. 21 at 2-4) and will therefore only
28 discuss additional facts raised by plaintiff in the FAC as
necessary.

1 Plaintiff has provided new information in the FAC
2 concerning her specific experience with the website. She now
3 alleges she visited the website sometime in July 2025 after
4 clicking on a Facebook advertisement "to research Medicare
5 supplement coverage." (FAC at 15-16.) Plaintiff then clicked on
6 the website's Medicare coverage section; entered her ZIP code in
7 Yuba County, California; proceeded to click "View Plans"
8 available in Yuba County; clicked on "Plan G; clicked on
9 "Medicare plans endorsed by AARP"; and finally clicked on a
10 button to "Learn More" about Plan G. (Id. at 16.) Plaintiff
11 "ultimately chose not to enroll or begin the enrollment process,"
12 thus ending her brief engagement with the website. (Id.)

13 Plaintiff alleges that by visiting the website, "the
14 website's code . . . caused the Trackers to be installed on [her]
15 browsers." (Id. at 17.) Plaintiff states that the communication
16 of information collected from this website visit by third-party
17 trackers constituted an invasion of her privacy. She also
18 alleges downstream effects, "including advertisements for
19 UnitedHealthcare and other health-insurance offerings on websites
20 and social media platforms, which reinforced that her private
21 coverage inquiry had been translated into a targeted advertising
22 profile." (Id.)

23 In her FAC, plaintiff also alleges two new tracking
24 modalities used by defendant to communicate plaintiff's data with
25 trackers: (1) a "session recorder," and (2) "canvas
26 fingerprinting." (Id. at 9-10.)

27 Session recorders "capture and replay user interactions
28 on websites" by "[monitoring] mouse movements. . .scrolling. .

1 .form inputs. . .page navigation. . .and time spent on each
2 element.” (Id. at 8.) Plaintiff alleges that defendant deployed
3 a session recorder operated by SessionCam Ltd. (“SessionCam”),
4 which “provided confirmed screen recording, confirmed keystroke
5 capture, confirmed mouse tracking, confirmed scroll tracking, and
6 likely form-input capture” of user’s data. (Id. at 9.)
7 Plaintiff does not, however, claim that any of her *inputs*
8 subjected to such SessionCam recordings revealed anything more
9 than her clicks on a prospective Medicare insurance program and
10 the entry of a ZIP Code in Yuba County.

11 Plaintiff also claims that defendant deployed a certain
12 type of “device fingerprinting” on its Website to track her
13 activity. (Id. at 5.) Device fingerprinting refers to “a broad
14 category of techniques that are used to identify a user’s device
15 across visits” by extracting data about user’s hardware and
16 software, “such as browser type, operating system, screen
17 resolution, installed fonts, and time zone and language
18 settings,” the unique combination of which becomes one’s “device
19 fingerprint.” (Id.) Specifically, plaintiff alleges that
20 defendant deployed canvas fingerprinting, which is a “specific
21 type of device fingerprinting” that “[identifies] and track a
22 user’s device by downloading a [program] that communicates a
23 user’s unique fingerprint to a server.” (Id.) She identifies
24 “at least nine distinct fingerprinting instances.” (Id. at 10-
25 11.) Nevertheless, plaintiff does not allege that the canvas
26 fingerprinting here has extracted information beyond connecting
27 her insurance inquiry to her browser or device across website
28 sessions. (Id. at 11.)

1 In total, plaintiff now claims that defendant deployed
2 "155 third-party trackers, including 47 cookies, 19 different
3 canvas fingerprints, and 1 session recorder" on its website.
4 (Id. at 9.) She alleges that information collected by her clicks
5 and page transitions on the website included "the full or partial
6 page URLs, page titles, event names, clickstream events, ZIP-
7 code-associated location signals, plan-selection signals, rate-
8 review flow signals, persistent identifiers, and browser and
9 device identifiers corresponding to the pages and actions just
10 described."² (Id. at 16.)

11 As with her initial complaint, plaintiff brings four
12 claims challenging the website's use of trackers pursuant to four
13 statutes: the California Invasion of Privacy Act ("CIPA"), the
14 federal Electronic Communications Privacy Act ("ECPA"), the
15 California Computer Data Access and Fraud Act ("CDAFA"), and the
16 California Constitution. (Id. at 20-28.)³

17 II. Third Party Tracking and Privacy Claims

18 As the court explained in its prior order, the
19 presence of a statutory right of action for an invasion of
20

21 ² As discussed in the following section, plaintiff has neither
22 duly defined nor shown that these sophisticated tracking methods
23 and identifiers have extracted *sensitive* health information such
24 that they can be considered embarrassing, invasive, or otherwise
private. See Popa v. Microsoft Corporation, 153 F. 4th 784, 792
(9th Cir. 2025).

25 ³ As the court stated in its prior order, plaintiff makes only
26 a single reference in the FAC to an alleged "loss of money" as a
27 result of UHC's conduct, suggesting an economic harm. (FAC at
28 23.) Plaintiff has not provided new information to describe the
alleged loss of money. (Id.) As before, this conclusory
allegation remains without factual support in the FAC and does
not confer standing. (Docket No. 23 at 4.)

1 privacy claim does not relieve the court of its independent
2 obligation to determine whether there is a case or controversy,
3 as required by Article III of the Constitution. (See Docket No.
4 21 at 6.) To that end, the Supreme Court has articulated that
5 "an injury in fact must be concrete and particularized," even
6 where a plaintiff sues under a statute providing a cause of
7 action and damages. Spokeo, Inc. v. Robins, 578 U.S. 330, 339
8 (2016); U.S. Const. art. 3, § 2, cl. 1.

9 The court previously determined that merely alleging
10 that a defendant "collect[ed] . . . user and device identifiers"
11 is insufficient to establish a constitutionally sufficient
12 injury-in-fact. (Docket No. 21 at 5); see also Xu v. Reuters
13 News & Media Inc., No. 24-cv-2466 PAE, 2025 WL 488501, at *3-4
14 (S.D.N.Y. Feb. 13, 2025) (collecting cases).⁴

15 Intangible harms -- such as a harm to one's privacy --
16 may constitute injuries in fact, but they must "bear a close
17 relationship to traditionally recognized harms." Wooten v.
18 BioLife Plasma Services L.P., 807 F. Supp. 3d 1139, 1144 (E.D.
19 Cal. 2025) (Sherriff, J.) (citing Spokeo, 578 U.S. at 341). As
20 such, plaintiff must show that the "the nature of the specific
21 information" collected was such that it could rightly be
22 considered injuriously invasive or private. Wooten, 807 F. Supp.
23 3d at 1143-44 (citing I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034,

24
25 ⁴ User and device identifiers are unique strings or values
26 (e.g., numbers, letters, or encoded data) that can be assigned to
27 a given user, account, device, browser, or session so the tracker
28 can identify the user. But identification -- or disclosure of
said identification -- absent the communication of content that
results in concrete injury is not enough to confer standing. Xu,
No. 24-cv-2466 at *3-4.

1 1050 (N.D. Cal. 2022). But where the information collected is
2 more akin to “a store clerk’s observing shoppers,” no such
3 privacy injury will arise. Popa v. Microsoft Corporation, 153 F.
4 4th 784, 791 (9th Cir. 2025).

5 In Popa, the Ninth Circuit deemed generalized pleadings
6 of privacy injury constitutionally insufficient to confer
7 standing. 153 F.4th, at 792. Plaintiff now alleges discrete
8 torts at common law as contemplated in Popa, those of intrusion
9 upon seclusion and unauthorized disclosure of private
10 information, both of which are required to be “highly offensive
11 to a reasonable person.” (FAC at 17.); Popa, 153 F.4th at 791.
12 The information collected by the defendant[s] in Popa was
13 comprised of routine website interaction data, such as “mouse
14 movements, clicks, keystrokes, URLs of pages visited, and/or
15 other electronic communications.” (Id. at 786.) The plaintiff
16 in Popa “identifie[d] no embarrassing, invasive, or otherwise
17 private information collected,” and thus failed to adequately
18 allege “harm that is remotely similar to the ‘highly offensive’
19 interferences or disclosures that were actionable at common law.”
20 (Id. at 791.) Moreover, district courts have found that tracking
21 software that monitors IP addresses and rudimentary browsing
22 activity is insufficient to give rise to an Article III injury-
23 in-fact. See Wooten, 807 F. Supp. 3d at 1144 (holding that
24 “collection and dissemination of plaintiffs’ IP and email
25 addresses” was insufficient to constitute a privacy injury).

26 In those cases where the courts have found the
27 information collected to be “embarrassing, invasive, or otherwise
28 private,” there have been demonstrable concrete injuries. Popa,

1 153 F.4th at 791. This is often the case when the trackers go
2 far beyond observing activity on a single website and instead
3 compile what the Ninth Circuit has described as “a cradle-to-the-
4 grave profile” of sensitive, personally revealing information
5 gathered across the internet and over a significant period of
6 time. In re Facebook, Inc. Internet Tracking Litigation, 956 F.
7 3d 589, 599 (9th Cir. 2020). As previously noted, in Semien v.
8 PubMatic, Inc., the court found a concrete privacy injury where
9 the plaintiffs alleged the collection of “sensitive information
10 like health status and treatment, travel plans, political
11 affiliation, sexual orientation, and more.” No. 25-cv-3164, 2026
12 WL 216333, at *5 (N.D. Cal. Jan. 27, 2026); see also Riganian v.
13 LiveRamp Holdings, Inc., 791 F. Supp. 3d 1075, 1087 (N.D. Cal.
14 2025) (finding concrete harm where plaintiff alleged “the
15 tracking of individuals’ activity across thousands of websites,
16 combined with extensive offline records gathered over decades, to
17 generate uniquely identifying profiles.”).

18 Plaintiff has now detailed her clicking on a specific
19 AARP-endorsed Medicare health insurance plan associated with her
20 ZIP code in Yuba County and clicking to “Learn More” About a
21 certain plan. (FAC at 15.) In so doing, she alleges she
22 “communicat[ed] private health-insurance interests and financial-
23 coverage preferences to a health insurer's website.” (Id. at
24 16.)

25 But beyond plaintiff’s listing these collection
26 methods, she does not explain how the actual *contents* of the
27 information collected revealed -- or in turn, were disclosed
28 without authorization -- any health-related information that

1 resemble "past, present, or future physical or mental health or
2 condition of an individual." Smith v. Facebook, Inc., 262 F.
3 Supp. 3d 943, 954 (N.D. Cal. 2017), aff'd, 745 F. App'x 8 (9th
4 Cir. 2018). Indeed, despite the sophistication of the tracking
5 methods alleged, plaintiff has not shown that the collected user
6 information communicated anything but "publicly available health
7 information" concerning the generic terms of a UHS-offered
8 insurance plan that she did not ultimately enroll in. Smith v.
9 Facebook Inc., 745 F. Appx. 8, 9 (9th Cir. 2018). As in the
10 court's prior order, the mere collection of plaintiff's generic
11 insurance browsing data is not enough to demonstrate the concrete
12 harm necessary to reach an Article III injury-in-fact. (Docket
13 No. 21 at 9.)

14 Plaintiff's newly alleged information thus still fails
15 to rise to the level of the detailed, sensitive data at issue in
16 In re Facebook, Semien and Riganian. Namely, plaintiff's
17 newfound emphasis on the vaguely health-related nature of her
18 information does not reflexively render that information
19 "embarrassing, invasive, or otherwise private." Popa, 153 F. 4th
20 at 791; see also Smith, 745 F. App'x 8 (9th Cir. 2018) (finding
21 that collected data involving the search and viewing of "publicly
22 available health information that cannot, in and of itself,
23 reveal details of an individual's health status or medical
24 history". . .is not "sensitive."). Unlike in Smith, plaintiff
25 does not allege that she provided any concrete details concerning
26 her health profile beyond an age-related inference. (FAC at 15-
27 16.) Indeed, plaintiff alleges far less than the plaintiff in
28 Smith; she has only cursorily searched for generic health

1 insurance information and provided a single ZIP code.

2 In Harrill v. Emmanuel Medical Center, the court found
3 a disclosure of sensitive medical information where plaintiffs
4 have made personalized searches "related to the provision of
5 healthcare, as opposed to 'general health information [regarding
6 conditions, symptoms, and doctors] accessible to the public at
7 large.'" No. 23-cv-1672, 2025 WL 1635428, at *4 (E.D. Cal. June
8 9, 2025). This is not such a case. Here, plaintiff does not
9 allege that the trackers captured searches for physician names,
10 actual conditions, appointments, personal medical history, use of
11 individual patient portals, user-inputs that are personal with
12 respect to medical status (FAC at 16), or any other information
13 that "courts have found to be sufficient to demonstrate
14 disclosure of [personal health information]." Harrill, 2025 WL
15 1635428 at *5.

16 Rather, the only user input by the plaintiff in this
17 case was her ZIP code. All other provided information
18 constituted browsing activity of "publicly available health
19 information that cannot in and of itself reveal details of an
20 individual's health status or medical history." Smith, 745 F.
21 Appx at *9. Further, plaintiff has not alleged that her specific
22 URL, session data, IP address, or any other digital information
23 has resulted in or otherwise led to the collection or disclosure
24 of sensitive medical information. See Harrill, 2025 WL 1635428
25 at *5.

26 The information plaintiff alleges the trackers
27 collected -- button clicks, page visits, scrolls, session
28 lengths, keystrokes, canvas fingerprints, URLs, and IP addresses

1 -- collected following one visit to the UHC website in July 2025
2 remains within the kind of "non-sensitive browsing activity on a
3 single website" that courts have repeatedly found insufficient to
4 establish a concrete injury. Semien, 2026 WL 216333 at *5
5 (internal citation omitted). Plaintiff has not made any new
6 allegations about the content of information collected that would
7 meet the requirements for concrete injury set forth in Popa and
8 its progeny. See 153 F. 4th at 791.

9 Plaintiff's emphasis on the demographic and age-related
10 character of the information collected fares no better.
11 Plaintiff emphasizes that she clicked on Medicare plans "endorsed
12 by the AARP," which enabled UHC to construct a "targeted
13 advertising profile" of plaintiff based on her age and region.
14 (FAC at 16-17.) But even here, plaintiff has not entered a
15 birthday, let alone specific health or demographic-related
16 information that could reasonably be deemed the kind of "cradle-
17 to-the-grave profile" sufficient to establish an Article III
18 injury-in-fact. See In re Facebook, Inc., 956 F. 3d at 599.

19 Finally, unlike in Jones v. Skullcandy, Inc., cited by
20 plaintiff's counsel for the first time during argument, plaintiff
21 has not alleged that she provided extensive personal, behavioral,
22 psychographic, or consumer-related information. No. 25-cv-1759,
23 2026 WL 699819, at *5 (S.D. Cal. Mar. 12, 2026). That case
24 involved a significantly more extensive collection of information
25 that bore on: "[d]etailed browsing histories and product
26 preferences," "[s]hopping cart contents and purchase behavior,"
27 "[p]ersonally identifiable information including names, email
28 addresses, and Facebook/Google account identifiers," "[r]eal-time

1 behavioral data showing consumer interests and purchasing
2 patterns," and "[d]emographic and psychographic profiles that
3 enable targeted marketing." 2026 WL 699819, at *5.

4 Instead, plaintiff requests that this court make the
5 inference that one who generically searches for AARP-endorsed
6 Medicare plans in a specific region has revealed sensitive age-
7 related information about themselves (instead, for example, of a
8 relative on whose behalf they are searching). Such a generic,
9 depersonalized search is not enough to establish a concrete
10 invasion of privacy injury. Cf. In re Facebook, Inc., 956 F. 3d
11 at 599 (finding that the collection of an "an individual's likes,
12 dislikes, interests, and habits over a significant amount of
13 time" . . . is sufficient to allege an invasion of the
14 "historically recognized right to privacy.").

15 For the foregoing reasons, the court must again grant
16 defendant's motion to dismiss without reaching the merits of
17 plaintiff's claims. See Righthaven LLC v. Hoehn, 716 F. 3d 1166,
18 1172 (9th Cir. 2013). As before, the court lacks jurisdiction to
19 consider the merits of plaintiff's claims in its FAC because
20 plaintiff again fails to allege a concrete injury sufficient to
21 satisfy Article III standing. Spokeo, 578 U.S. at 339-340.
22 Because of that failure, "[t]his case begins and ends with
23 standing." Dep't of Educ. v. Brown, 600 U.S. 551, 560-61 (2023).
24 When asked at the hearing whether plaintiff would be able to
25 further amend her complaint to add any new factual allegations to
26 cure the above deficiencies, counsel represented that she would
27 not. Accordingly, the court will not permit further amendment.
28 See Intri-Plex Techs., Inc. v. Crest Grp., Inc., 499 F.3d 1048

1 (9th Cir. 2007) (citation omitted).

2 IT IS THEREFORE ORDERED that defendant's Motion to
3 Dismiss Plaintiff's First Amended Complaint (Docket No. 28) be,
4 and the same hereby is, GRANTED, and this action is hereby
5 DISMISSED with prejudice.

6 Dated: August 19, 2026

7 

8 **WILLIAM B. SHUBB**
9 **UNITED STATES DISTRICT JUDGE**
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28