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.)

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

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

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

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

I. UHC's Website and Plaintiff's Allegations[1]

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

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

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

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

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

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

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

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

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

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

II. Third Party Tracking and Privacy Claims

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

---

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

[3] As the court stated in its prior order, plaintiff makes only a single reference in the FAC to an alleged "loss of money" as a result of UHC's conduct, suggesting an economic harm. (FAC at 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.)

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

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

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

[4] User and device identifiers are unique strings or values (e.g., numbers, letters, or encoded data) that can be assigned to a given user, account, device, browser, or session so the tracker 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.

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

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

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

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

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

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

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

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

insurance information and provided a single ZIP code.

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

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

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

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

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

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

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

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

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

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

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

Dated: August 19, 2026

WILLIAM B. SHUBB
UNITED STATES DISTRICT JUDGE