

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ARNY ASERCION,
Plaintiff,

v.

ULTA SALON, COSMETICS &
FRAGRANCE, INC.,
Defendant.

Case No. 26-cv-02442-RFL

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION FOR
JUDGMENT ON THE PLEADINGS
WITH LEAVE TO AMEND**

Re: Dkt. No. 13

Plaintiff alleges that Ulta embedded code into its website that causes Internet tracking technology to be installed on the browsers of website visitors. These trackers allegedly allow both Ulta and third parties to track users as they browse Ulta's website and across the Internet. The information gathered allegedly facilitates targeted advertising and allows the creation of detailed user profiles. Plaintiff alleges that he visited the website in May 2025 and that the website installed the trackers on his browser. He commenced this action to recover for the alleged invasion of privacy that followed. (*See* Dkt. No. 1-2 (the "Complaint" or "Compl.")). Ulta now moves for judgment on the pleadings. For the reasons set forth below, the motion is **GRANTED IN PART** and **DENIED IN PART WITH LEAVE TO AMEND**. This Order assumes that the reader is familiar with the facts of the case, the applicable legal standards, and the parties' arguments.

A. California Invasion of Privacy Act (the "CIPA")

1. Section 631(a)

Ulta argues that this claim fails because: (1) no third-party interception is sufficiently alleged; and (2) aiding and abetting is not sufficiently alleged. Beginning with interception, the

statute prohibits “willfully and without the consent of all parties to the communication, or in any unauthorized manner, read[ing], or attempt[ing] to read, or to learn[ing] the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state.” *See* Cal. Penal Code. § 631(a). According to Ulta, Plaintiff does not allege the interception of any contents.

Interception requires “acquisition contemporaneous with transmission.” *See Semien v. PubMatic*, No. 25-cv-03164-SI, 2026 WL 216333, at *8 (N.D. Cal. Jan. 27, 2026) (citation omitted). Plaintiff’s allegations satisfy this definition because Plaintiff alleges that the trackers collected and transmitted browser activity “in real time.” (*See* Compl. at 6 ¶ 12, 15 ¶ 70)¹; *see, e.g., McClung v. AddShopper, Inc.*, No. 23-cv-01996-VC, 2024 WL 189006, at *3 (N.D. Cal. Jan. 17, 2024). At the pleading stage, that is sufficient to support a plausible inference that the information was acquired while the communication was in transit to its intended recipient.

Contents “refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication.” *See D’Angelo v. FCA US, LLC*, 726 F. Supp. 3d 1179, 1199 (S.D. Cal. Mar. 28, 2024) (citation omitted). Under this definition, Plaintiff sufficiently alleges interception of contents (*e.g.*, product views). (*See* Compl. at 13 ¶ 62.) Ulta argues that Plaintiff must allege that she engaged in some “substantive communication” while on Ulta’s website beyond merely visiting the website. (*See* Dkt. No. 13 at 13.) Because Plaintiff alleges that he visited the website “to browse for Mother’s Day gifts” (Compl. ¶ 92), it can be reasonably inferred that he engaged in some form of substantive communication beyond merely visiting the website (*e.g.*, typing in a search field, clicking on product pages).

Turning to aiding and abetting, Ulta argues that Plaintiff’s allegations do not satisfy the scienter requirement. “At the very least, [aiding and abetting under Section 631(a)] requires both knowledge of the conduct that will violate the statute and a purpose of aiding, agreeing with, or

¹ All citations to page numbers in filings on the docket refer to ECF page numbers.

employing the third party to commit those acts.” *See Smith v. YETI Coolers, LLC*, 754 F. Supp. 3d 933, 942 (N.D. Cal. 2024). Plaintiff alleges that Ulta affirmatively “causes” installation of third-party trackers (*see* Compl. at 3 ¶ 2, 14 ¶ 68 18 ¶¶ 93, 98) and then uses the trackers to collect information and transmit the information to third parties (*see id.* at 15 ¶ 70), so it is reasonable to infer both knowledge of the trackers’ operations and a purpose of aiding or agreeing with the third parties’ operations. *See, e.g., M.H. v. Done Glob. Inc.*, No. 24-cv-03040-RFL, 2025 WL 629613, at *2 (N.D. Cal. Feb. 26, 2025).

2. Section 638.51(a)

“The CIPA prohibits installing or using ‘pen registers’ without prior court approval. . . . A pen register is ‘a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.’” *Deivaprakash v. Condé Nast Digit.*, 798 F. Supp. 3d 1100, 1104 (N.D. Cal. 2025) (citing Cal Penal Code §§ 638.50(b), 638.51(a)). Ulta raises five arguments in support of dismissal of the pen register claim.

First, Ulta argues that the collection by the trackers of contents places them outside the definition of pen register because pen registers collect only recording information and not contents. But some components of the trackers allegedly collected contents (and accordingly were not pen registers), while other components allegedly collected IP addresses (and accordingly were pen registers). (*See, e.g.,* Compl. at 13 ¶¶ 58-59, 62.) Section 638.51(a) covers not only a “device” but also a “process,” which would appear by its plain language to cover an individual component of a tracker. Thus, if one component of the tracker collects contents, and another component collects addressing information without contents, the latter component would appear to fall within the statutory pen register definition. Ulta does not provide any argument to the contrary.

Second, Ulta argues that Plaintiff does not specifically allege the use of any pen register during Plaintiff’s sole visit to the website. But Plaintiff alleges that the website installs

numerous trackers when users visit, so it is reasonable to infer that the trackers falling into the definition of pen register were installed during Plaintiff’s sole visit. (*See, e.g., id.* at 3 ¶ 2, 14-15 ¶ 69.)

Third, Ulta argues that the pen register statute applies only to telephone technology and not Internet technology. Its own authority counsels otherwise. *See D’Antonio v. Smith & Wesson Inc.*, 820 F. Supp. 3d 928, 936-37 (N.D. Cal. 2026); *see also Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 930-31 (N.D. Cal. 2024).

Fourth, Ulta argues that Plaintiff does not satisfy the statutory standing requirements of the CIPA. “The CIPA confers statutory standing to bring a private right of action on persons injured by a violation of the statute.” *Deivaprakash*, 798 F. Supp. 3d at 1106 (citation and quotation marks omitted). Plaintiff sufficiently alleges injury because the pen register trackers enable the building of detailed profiles of those being tracked, and it is reasonable to infer that that happened to Plaintiff. (*See* Compl. at 6 ¶¶ 9-10, 10 ¶¶ 36-38, 12-13 ¶¶ 53, 59); *see, e.g., Deivaprakash*, 798 F. Supp. 3d at 1106-07.

Fifth, Ulta argues that Plaintiff does not sufficiently allege that Ulta intended to install a pen register. Nothing in the text of Section 638.51(a) suggests there is an intent requirement, and Ulta cites no authority for this proposition.

3. Consent

Ulta argues that both of Plaintiff’s CIPA claims fail because he allegedly consented. *See* Cal. Penal Code §§ 631(a) (interception occurs “without the consent of all parties to the communication, or in any unauthorized manner”), 638.51(b)(5) (use of pen register permitted “[i]f the consent of the user . . . has been obtained”). Plaintiff alleges that he did not consent to the collection of the data at issue. (*See* Compl. at 3 ¶ 4, 15 ¶¶ 72-73, 18 ¶ 95.) In Ulta’s view, its website privacy policy establishes consent because the policy disclosed use of the trackers. Even if the Court considers the policy as properly subject to judicial notice or incorporated by reference into the Complaint, the mere existence of the policy does not equate to consent without any indication that the user saw the policy or agreed to it, and Ulta offers no argument otherwise.

Cf. Hubbard v. Google LLC, No. 19-cv-07016-SVK, 2025 WL 82211, at *5 (N.D. Cal. Jan. 13, 2025) (mere disclosure of data collection practices in privacy policies and terms of service does not indicate “whether these terms would have been conspicuously presented to Plaintiffs,” and “the Court will not presume awareness or notice . . . merely because these terms existed”). Moreover, Plaintiff alleges that Ulta’s website installed the trackers when Plaintiff visited. Accordingly, it is reasonable to infer that this installation, which led to the subsequent tracking, occurred *before* Plaintiff could have possibly been aware of the privacy policy and the disclosures it contained. To the extent Ulta argues that it is implausible that there would have been no “mechanism” to provide consent upon visiting the website in light of the privacy policy disclosures, that presents a factual inquiry improper for resolution at this stage.

In sum, dismissal of the CIPA claims is denied.

B. Federal Wiretap Act

Ulta raises four arguments in support of dismissal of the federal Wiretap Act claim. The first two arguments mirror the contents and interception arguments already rejected above; Plaintiff sufficiently alleges interception of contents. The third argument is that “the Complaint does not identify what specific vendor allegedly intercepted what specific communication from Plaintiff, and it pleads no facts showing that any vendor acted as an independent interceptor rather than as a software provider operating on Ulta’s site.” (*See* Dkt. No. 13 at 18.) The Complaint, however, identifies specific trackers, including by specific vendor, that allegedly were used on Ulta’s site and that meet the statutory requirements (*see* Compl. at 12-14 ¶¶ 52-64), and it is plausibly inferred that at least some of those were installed on Plaintiff’s browser during his visit.

The fourth argument is that the “party exception” to interception liability applies. *See* 18 U.S.C. § 2511(2)(d). The party exception is itself subject to an exception, known as the “crime-tort exception”:

The crime-tort exception has two relevant components. First, there is a temporal component whereby the intercepting party must have the independent criminal or

tortious purpose at the time the [interception] was made. Second, there is a separate and independent component whereby the crime or tort intended must be beyond the act of [intercepting] itself. Thus, at the time of the interception, a defendant must have had an independent prohibited purpose beyond the act of interception itself for the crime-tort exception to apply.

Smith v. Rack Room Shoes, Inc., No. 24-cv-06709-RFL, 2025 WL 2210002, at *4 (N.D. Cal. Aug. 4, 2025) (citations and quotation marks omitted). Under the allegations of the Complaint, the crime-tort exception applies because Plaintiff sufficiently alleges that Ulta intended to collect information and distribute it to third parties for targeted advertising, which is an independent tortious purpose beyond the act of interception itself, and as discussed above, it allegedly violated the CIPA in doing so. (*See* Compl. at 11 ¶ 46, 15 ¶¶ 70-71, 18 ¶¶ 91, 94); *see, e.g., Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) (crime-tort exception satisfied where “Plaintiffs have alleged that Google intercepted their communications for the purpose of associating their data with preexisting user profiles,” and doing so allegedly “violated state law, including CDAFA, intrusion upon seclusion, and invasion of privacy”).

In sum, dismissal of the federal Wiretap Act claim is denied.

C. Comprehensive Computer Data Access and Fraud Act (the “CDAFA”)

Ulta raises three arguments in support of dismissal of the CDAFA claim. First, Ulta argues that Plaintiff does not satisfy the statute’s injury requirement. *See* Cal. Penal Code § 502(e)(1). Plaintiff alleges that Ulta unjustly enriched itself by using Plaintiff’s information that it accessed in violation of the CDAFA (*see* Compl. at 27 ¶ 155), which is sufficient to plead a CDAFA injury. *See, e.g., Rack Room*, 2025 WL 2210002, at *3.

Second, Ulta argues that Plaintiff does not satisfy the statute’s “without permission” requirement. *See* Cal. Penal Code §§ 502(c)(1), (2), (4), (6), (7). In Ulta’s view, without permission “require[s] allegations that the defendant circumvented a technical or code-based barrier restricting access.” (*See* Dkt. No. 13 at 19.) This Court has previously rejected that argument:

The plain meaning of the term without permission does not require [a plaintiff] to plead that the acting party overc[ame] technical or code-based barrier[s] It is

enough that [the defendant] allegedly inserted third-party code into its website that allowed third parties to use technological means to access that data without permission.

Smith v. Rack Room Shoes, Inc., No. 24-cv-06709-RFL, 2025 WL 1085169, at *6 (N.D. Cal. Apr. 4, 2025) (citations and quotation marks omitted). Ulta offers no reason why the Court should depart from this interpretation.

Third, Ulta argues that Plaintiff does not allege “what Ulta specifically accessed, altered, or used without permission, how it supposedly provided a means of access, or how any alleged conduct violated any particular subsection.” (See Dkt. No. 13 at 20.) As to the first two points, the Complaint is clear that Ulta, through its website, allegedly installed trackers on Plaintiff’s browser, without his permission, to collect information about his Internet browsing. As to the third point, the CDAFA provisions in question provide as follows:

- **Subsection (c)(1).** *Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.* Prong (B) is satisfied because Ulta allegedly wrongfully obtained Plaintiff’s data using his computer system.
- **Subsection (c)(2).** *Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.* This is satisfied because Ulta allegedly “ma[de] use of [Plaintiff’s] data” from his computer system.
- **Subsection (c)(4).** *Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.* This is satisfied because Ulta “add[ed] . . . computer software” or “computer programs” by causing installation of the trackers.
- **Subsection (c)(6).** *Knowingly and without permission provides or assists in providing a*

means of accessing a computer, computer system, or computer network in violation of this section. Access “means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.” Cal Penal Code § 502(b)(1). In light of that definition, this provision is satisfied because, by installing the trackers, Ulta “cause[d] output from” Plaintiff’s computer, as the trackers transmitted Plaintiff’s information to third parties. (*See* Compl. at 13 ¶ 62.)

- **Subsection (c)(7).** *Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.* This is satisfied because Ulta accessed Plaintiff’s computer by causing its website to install trackers on Plaintiff’s browser.

In sum, dismissal of the CDAFA claim is denied.

D. Invasion of Privacy Under the California Constitution

“A claim for invasion of privacy under the California Constitution involves similar elements [to an intrusion upon seclusion claim]. Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is so serious . . . as to constitute an egregious breach of the social norms such that the breach is highly offensive.” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (citation and quotation marks omitted). Ulta argues that Plaintiff did not maintain a reasonable expectation of privacy and that any privacy intrusion was not highly offensive.

Beginning with reasonable expectation of privacy, the Ninth Circuit directs courts to consider “whether a defendant gained unwanted access to data by electronic or other covert means, in violation of the law or social norms,” “the amount of data allegedly collected,” whether “this amount of information can be easily collected without user knowledge,” the “nature of the allegedly collected data,” and “the sensitivity of the collected information.” *See id.* at 601-06. This presents a factual inquiry often inappropriate for resolution as a matter of

law. *See YETI Coolers*, 754 F. Supp. 3d at 945. Plaintiff’s allegations of Internet-wide tracking that resulted in the creation of detailed profiles of Internet users (including him) suffices. *See, e.g., Gilligan v. Experian Data Corp.*, No. 25-cv-02873-RFL, 2026 WL 32259, at *2 (N.D. Cal. Jan. 6, 2026). *Popa v. Microsoft Corporation*, 153 F.4th 784 (9th Cir. 2025), does not require a different result. *See Gilligan*, 2026 WL 32259, at *2. Nor does Ulta’s privacy policy. As explained above, under the allegations of the Complaint, it is reasonable to infer that Ulta’s website installed the trackers before Plaintiff could have possibly been aware of the privacy policy and the disclosures it contained.

Turning to whether the alleged privacy intrusion was highly offensive, “[a]ssessing the degree of offensiveness [] presents a policy question that often evades resolution at the pleading stage.” *Hubbard*, 2025 WL 82211, at *4 (citing *Facebook*, 956 F.3d at 606). Plaintiff’s allegations of Internet-wide tracking that resulted in the creation of detailed profiles of Internet users (including him) suffices. *See, e.g., Rack Room*, 2025 WL 1085169, at *3. The large number of trackers allegedly installed (201) bolsters this conclusion. (*See* Compl. at 11 ¶ 47.)

In sum, dismissal of the California constitutional privacy claim is denied.

E. UCL

Ulta argues that Plaintiff does not satisfy the UCL’s statutory standing requirement. Statutory standing under the UCL “requires a plaintiff to demonstrate some form of economic injury” *See Hinojos v. Kohl’s Corp.*, 718 F.3d 1098, 1104 (9th Cir. 2013) (citations and quotation marks omitted). Plaintiff argues that his data has economic value, and “Ulta allegedly appropriated identifiable browsing, product interest, purchase intent, device, and persistent identifier data; treated that data as a monetizable asset; sold/shared it through ad-tech systems; and deprived Plaintiff of the ability to control, withhold, or exchange that data on his own terms.” (*See* Dkt. No. 15 at 19.) Those conclusory allegations do not satisfy the economic injury requirement. *See, e.g., Rack Room*, 2025 WL 1085169, at *6.

Accordingly, Plaintiff fails to state a UCL claim. In light of the lack of statutory standing as alleged, this Order does not reach Ulta’s other arguments for dismissal of the UCL claim.

F. Conclusion

For the foregoing reasons, the motion is **GRANTED IN PART** and **DENIED IN PART** as follows:

- The UCL claim is dismissed with leave to amend.
- The remaining claims survive dismissal.

If Plaintiff wishes to file an amended complaint correcting the deficiencies identified in this Order, he shall do so by **September 11, 2026**. The amended complaint may not add new claims or parties, or otherwise change the allegations except to correct the identified deficiencies, absent leave of the Court or stipulation by the parties pursuant to Federal Rule of Civil Procedure 15. By **October 2, 2026**, Ulta shall either respond to the amended complaint, or, if no amended complaint is filed, respond to the Complaint.

The paragraphs of the Complaint are not sequentially numbered. If Plaintiff files an amended complaint, the paragraphs shall be sequentially numbered, and if Plaintiff does not file an amended complaint, then by **September 11, 2026**, he shall file a corrected version of the Complaint with sequentially numbered paragraphs. *See* Fed. R. Civ. P. 10(b).

IT IS SO ORDERED.

Dated: August 21, 2026



RITA F. LIN
United States District Judge