

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

Present: **Honorable JOSEPHINE L. STATON, UNITED STATES DISTRICT JUDGE**

Kelly Davis
Deputy Clerk

N/A
Court Reporter

Attorneys Present for Plaintiffs:

Attorneys Present for Defendant:

Not Present

Not Present

**PROCEEDINGS: (IN CHAMBERS) ORDER GRANTING MOTION TO
DISMISS (Doc. 13)**

Before the Court is a Motion to Dismiss filed by Defendant Blackhawk Network, Inc. (Mot., Doc. 13.) Plaintiff Silvia Garcia opposed, and Defendant responded. (Opp., Doc. 16; Reply, Doc. 17.) Having held a hearing on the motion and taken the matter under submission, the Court GRANTS Defendant’s motion.

I. BACKGROUND

Defendant owns and operates the website giftcards.com (the “Website”), which allows visitors to purchase gift cards. (First Amended Complaint, “FAC” ¶¶ 1, 22–23.) The Website displays a cookie consent banner that allows users to select “Required only” cookies. (*Id.* ¶ 1, 58.) The banner, in full, reads: “This site uses third party cookies and related technologies, which may include ads personalization. Choose whether to allow all cookies (and related technologies) or the minimum set of required cookies. For more options and information visit [cookie settings](#).” (*Id.* ¶ 57.)

Plaintiff alleges that this banner represents that the Website will not share user data with non-essential third parties—including data brokers and advertising platforms—when a user selects the “Required only” option. (*Id.* ¶¶ 1–2, 59–60.) However, Plaintiff

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

alleges that the Website “causes users’ devices to store and/or transmit both first-party and third-party tracking cookies,” which enable the Website “to identify the device making the requests, and record a session showing how the user interacts with the website.” (*Id.* ¶ 17; *see also* ¶¶ 61–62.)

First-party cookies are placed by a webserver with which the user is directly communicating and track users when they repeatedly visit the same website; third-party cookies are set by a third-party webserver and are used by the third-party to “recognize individual users across websites . . . and across browsing sessions.” (*Id.* ¶¶ 18–19.) Plaintiff therefore alleges that Defendant enabled third parties to collect users’ personal information about their interactions with Defendant, including: browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behavior, device information, referring URL, session information, user identifiers, and geolocation data. (*Id.* ¶ 20.) Plaintiff alleges that third parties use the collected data to build consumer profiles, develop audience segments, conduct targeted advertising and marketing analytics, and share user information with other entities. (*Id.* ¶¶ 4, 89–90.) Plaintiff contends that Defendant knowingly enabled this data collection and derived financial benefits from it. (*Id.* ¶ 93.)

Specifically, Plaintiff alleges that these third-party cookies were placed on users’ devices even when they selected the “required-only” cookie option. (*Id.* ¶ 62.) Plaintiff conducted an investigation of the website on June 9, 2025, and detected code from multiple third parties on “a user’s browser.” (*Id.* ¶ 34; *see also id.* ¶ 63.) Those third parties included databrokers, advertisers, and social media companies like LiveRamp, Magnite, Nielson Marketing, Tru Optik Data Corp. (Trans Union), Adobe Audience Manager, Google Ads, TheTradeDesk, and Xandr. (*Id.* ¶¶ 35–57.) Plaintiff alleges that on other occasions, the website installed cookies from similar entities including ComScore, Conversant, Dstillery, TripleLift, Addthis.com/Oracle, Rakuten Advertising, and Xavis. (*Id.* ¶¶ 64–85.)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

Plaintiff visited the Website herself on April 3, 2025. (*Id.* ¶ 94.) In addition to being “genuinely interested in the goods, services, and information” available on the website, Plaintiff is “a consumer privacy advocate who works as a ‘tester’ to ensure that companies abide by the privacy obligations imposed by California law.” (*Id.*) Plaintiff selected the “Required only” cookie option upon arrival, believing that this would allow her to opt out of cookies that cause the disclosure of user data to third-party advertising networks, analytics services, and/or social media companies. (*Id.* ¶¶ 96–97.) She alleges, however, that Defendant had already caused third-party cookies and tracking technologies to load on her device before she made that selection and before the consent banner appeared. (*Id.* ¶¶ 95, 99.) In doing so, Plaintiff alleges that Defendant “permitted [several third parties] to track and collect Plaintiff’s Private Communications as Plaintiff browsed the Website.” (*Id.* ¶ 100.)

Plaintiff alleges that she relied on Defendant’s cookie consent representations when she continued to browse the Website and that she would have used the Website differently—or not at all—had she known that non-essential cookies were already operating. (*Id.* ¶¶ 98, 100–101.) She further alleges that Defendant’s representations led her, and similarly situated users, to believe that third parties could not access their interactions with the Website once they rejected non-essential cookies. (*Id.* ¶ 60.)

Plaintiff filed this action in Los Angeles Superior Court on June 30, 2025. (Ex. C to Notice of Removal, Doc. 1-3.) Defendant removed the action on August 13, 2025, asserting federal question jurisdiction. (*Id.* ¶ 1.) Plaintiff filed her FAC on October 3, 2025. (FAC, Doc. 11.) The FAC asserts seven causes of action: (1) violation of the Federal Wiretap Act (part of the Electronic Communications Privacy Act, “ECPA”), 18 U.S.C. § 2511; (2) invasion of privacy under Article I, section 1 of the California Constitution; (3) intrusion upon seclusion; (4) violation of the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 631; (5) violation of CIPA, Cal. Penal Code § 638.51; (6) common-law fraud; and (7) unjust enrichment. Defendant filed this motion to

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

dismiss the FAC for failure to state a claim under Rule 12(b)(1) & (6) of the Federal Rules of Civil Procedure. (Mot.)

The Court held a hearing on this motion at which the Parties addressed whether Plaintiff had Article III standing under the Ninth Circuit’s recent decision in *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025). Because the Court now concludes that it lacks subject matter jurisdiction, it grants Defendant’s Motion to Dismiss pursuant to Federal Rule of Civil Procedure Rule 12(b)(1). Accordingly, the Court does not reach Defendant’s Motion to Dismiss for failure to state a claim pursuant to Rule 12(b)(6).

II. LEGAL STANDARD

A. Rule 12(b)(1)

A defendant may move to dismiss an action for lack of subject-matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1). Fed. R. Civ. P. 12(b)(1). “Dismissal for lack of subject matter jurisdiction is appropriate if the complaint, considered in its entirety, on its face fails to allege facts sufficient to establish subject matter jurisdiction.” *In re Dynamic Random Access Memory (DRAM) Antitrust Litig.*, 546 F.3d 981, 984–85 (9th Cir. 2008). When considering a Rule 12(b)(1) motion, the Court “is not restricted to the face of the pleadings, but may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction.” *McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir. 1988). “The party asserting [] subject matter jurisdiction bears the burden of proving its existence.” *Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1122 (9th Cir. 2010).

B. Standing

“Article III confines the federal judicial power to the resolution of ‘Cases’ and ‘Controversies.’ For there to be a case or controversy under Article III, the plaintiff must

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

have a ‘personal stake’ in the case—in other words, standing.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (citations omitted). “[T]o establish standing, a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief.” *Id.* “Since they are not mere pleading requirements but rather an indispensable part of the plaintiff’s case, each element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992).

III. ANALYSIS

A. ECPA Claim

On August 26, 2025, the Ninth Circuit issued its decision in *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025), addressing standing’s concrete injury requirement in the context of privacy violations. At issue in *Popa* was an alleged violation of Pennsylvania’s Wiretapping and Electronic Surveillance Control Act (“WESCA”), which, in relevant portion, allowed for suits against any person who acquires “the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” 18 Pa. Cons. Stat. §§ 5702, 5725. The “single issue” was whether the plaintiff alleged a “concrete injury” sufficient for Article III standing. 153 F.4th at 788.

To answer this question, the court turned to the Supreme Court’s decision in *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). There, a group of plaintiffs sued because they had incorrect, reputationally damaging information on their credit reports in violation of the Fair Credit Reporting Act of 1970 (“FCRA”). *TransUnion*, 594 U.S. at 418–21. While all plaintiffs had damaging information on their reports, the Court held

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

that only those whose reports had actually been disclosed to third-parties had suffered a sufficiently concrete injury for Article III purposes. *TransUnion*, 594 U.S. at 439. While Congress may create a statutory cause of action, “[o]nly those plaintiffs who have been *concretely harmed* by a defendant’s statutory violation may sue that private defendant over that violation in federal court.” *Id.* at 426–27 (“[U]nder Article III, an injury in law is not an injury in fact.”)

The *Popa* panel therefore needed to determine whether the plaintiff had suffered a concrete injury sufficient to sue for a violation of WESCA in federal court. In *TransUnion*, the Court “identified history as the touchstone for concreteness.” *Id.* Thus, the panel reasoned that the plaintiff needed to have “suffered a harm that has traditionally been actionable in our nation’s legal system.” *Id.* at 791. Courts must now therefore assess whether plaintiffs have “identified a close historical or common-law analogue for their asserted injury.” *Id.* (quoting *TransUnion*, 594 U.S. at 424). For cases alleging violations of privacy rights, this may not be a “free-roaming privacy right at common law” but rather one of a few “discrete torts that protected specific kinds of privacy-related harms.” *Id.* at 792.

The Plaintiff in *Popa* argued that “because the Pennsylvania legislature enacted a statute protecting a substantive policy right, any plaintiff alleging a violation of that statute will satisfy Article III.” *Id.* at 792. The Ninth Circuit rejected this argument under *TransUnion*, which it reasoned rejected a “one-size-fits-all approach,” meaning that “some plaintiffs had standing to bring a claim under the statute while others did not.” *Id.* at 792. Instead, the *TransUnion* Court “considered carefully the key elements that shape the harm proscribed by the common-law tort . . . , and assessed whether the *specific* plaintiffs had experienced harm of that nature.” *Id.* Thus, following *Popa* and *TransUnion*, statutory privacy violations do not create concrete injuries in and of themselves for the purposes of Article III standing. 153 F.4th at 794. Plaintiffs instead must show that their specific, individualized harms are analogous to a common law tort, giving them standing to bring a suit under the statutory cause of action.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

Applying *Popa*, two kinds of wiretapping proscribed by the ECPA are at issue here. The ECPA imposes liability against any person who: “intentionally intercepts, endeavors to intercept, or procures any other person to intercept, any wire, oral, or electronic communication;” or who “intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.” 18 U.S.C. § 2511(a), (d).

Like the provisions of WESCA at issue in *Popa*, ECPA liability is broader than that of common-law privacy torts. Just as the *Popa* court required that the plaintiff there allege a concrete harm beyond a defendant merely acquiring “the contents of any wire, electronic or oral communication,” so, too, must this Court require that Plaintiff show she has suffered a harm beyond an “intentional interception” or unauthorized “use.” 18 Pa. Cons. Stat. §§ 5702, 5725; 18 U.S.C. § 2511(a), (d). To have Article III standing to bring her ECPA claim, like WESCA and the FCRA, Plaintiff must show that she has suffered a harm traditionally actionable under common law.

The *Popa* court also provided guidance on what kinds of privacy harms are sufficiently concrete. There, the court addressed “session replay” tracking technology on a pet-supply website, which collected information about a user’s interactions with the website like: “mouse movements, clicks, keystrokes . . . , URLs of web pages visited, and/or other electronic communications in real-time.” *Id.* at 786. The plaintiff identified two common law analogues for this kind of violation: intrusion upon seclusion or public disclosure of private facts, both of which require “highly offensive” intrusions or disclosures. *Id.* at 791. Ultimately, the Court held that the “session replay” technology did not meet the “highly offensive” bar because the plaintiff identified “no embarrassing, invasive, or otherwise private information collected by [Defendant].” *Id.* In fact, the court reasoned that “the monitoring . . . seem[ed] most similar to a store clerk’s observing shoppers in order to identify aisles that are particularly popular or spot problems that disrupt potential sales.” *Popa*, 153 F.4th at 791.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

Accordingly, Plaintiff must plead that Defendant’s tracking technology caused her to suffer an injury that is analogous to a common-law privacy tort. Here, Plaintiff argues that the common-law analogue is intrusion upon seclusion, which she has also pled as a separate claim. (Opp. at 21.)

At common law, intrusion by seclusion meant the intentional intrusion “upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person.” Restatement (Second) of Torts § 652B (1977). Thus, an action for invasion of privacy by intrusion upon seclusion has two elements: (1) an intrusion into a private place, conversation, or matter, (2) in a manner highly offensive to a reasonable person. *Smith v. Capital One Fin. Corp.*, No. C 11-3425 PJH, 2012 WL 1669347, at *3 (N.D. Cal. May 11, 2012) (citing *Taus v. Loftus*, 40 Cal. 4th 683, 725 (2007)); *see also Deteresa v. Am. Broad. Cos., Inc.*, 121 F.3d 460, 465 (9th Cir. 1997) (“One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”). The intrusion must be intentional. *Smith*, 2012 WL 1669347, at *3. “In addition, the plaintiff must have had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.” *Id.* (citing *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 232 (1998)).

On the first element, Plaintiff has made allegations sufficient to meet *Popa*’s threshold. Generally, Plaintiff may not have an expectation of solitude while browsing an online shopping platform, as Plaintiff would certainly not have such an expectation within the four walls of a real-world store. Here, however, Defendant created an expectation of privacy when it asked whether she wished to be tracked, and after selecting only “required” cookies, she felt secure in browsing. (See FAC ¶¶ 97–101.)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

Having established that she had an expectation of solitude, Plaintiff must also allege that the actual intrusion was “highly offensive to the reasonable person.” Restatement (Second) of Torts § 652B (1977). Plaintiff primarily argues that Defendant’s “highly offensive” conduct was a misrepresentation that unnecessary third-party tracking cookies would not be placed on her device. (*See, e.g.*, FAC ¶ 133.) But Defendant’s misrepresentation goes only to the first element: whether there was an intrusion into a private place. More narrowly, whether Plaintiff had “an objectively reasonable expectation of seclusion or privacy in . . . the data.” *Smith*, 2012 WL 1669347, at *3. The Court is aware that some other Courts have held that the misrepresentation alone is enough to meet the highly offensive bar, but the Court does not find the reasoning persuasive. *See, e.g., Wiley v. Universal Music Grp.*, 2025 WL 3654085, at *6 (N.D. Cal. Dec. 17, 2025); *but see Shah v. MyFitnessPal, Inc.*, 2026 WL 216334, at *3 (N.D. Cal. Jan. 27, 2026) (reaching the same conclusion but considering also that the collected information was from a “sensitive sphere”).

So, to determine whether a privacy violation creates an injury sufficient for Article III standing, the Court must examine the actual tracking technologies at issue. For example, in *Popa* the court ultimately held that the session replay technology was not highly offensive because “the monitoring . . . seem[ed] most similar to a store clerk’s observing shoppers in order to identify aisles that are particularly popular or spot problems that disrupt potential sales.” *Popa*, 153 F.4th at 791. Thus, information collected only within the bounds of a single website about Plaintiff’s activity on that website is not sufficient to create an injury.

There are thus at least two ways tracking technologies may result in highly offensive conduct. First, the information collected could be especially sensitive, for example health or financial information. *Cf. Semien v. PubMatic Inc.*, 2026 WL 216333, at *4 (N.D. Cal. Jan. 27, 2026) (finding standing where Defendant intercepted communications that could include “health status and treatment, travel plans, political affiliation, sexual orientation, and more”); *Gabrielli v. Haleon U.S. Inc.*, 2025 WL

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

2494368, at *7 (N.D. Cal. Aug. 29, 2025). Second, the scope of the collection may be so broad, for example by tracking a Plaintiff’s activity across other websites, that it renders the tracking highly offensive. *See In re Facebook, Inc. Internet Tracking Litigation*, 659 F.3d 589, 598–99 (9th Cir. 2020) (privacy violation for plug-in that tracked consumers off the defendant platform); *Popa*, 153 F.4th at 794 (declining to revisit *In re Facebook* because the privacy violations accounted for “the individual circumstances giving rise to the plaintiffs’ alleged injuries”).

Here, the FAC suffers from multiple deficiencies. First, Plaintiff has not made any allegations that the information collected, or its reach, would have been highly offensive. As in *Popa*, Plaintiff identifies “no embarrassing, invasive, or otherwise private information” that was shared. 153 F.4th at 791. The information the FAC alleges third parties were able to track largely regard Plaintiff’s interactions with Defendant, who sold gift cards. (*See* FAC ¶ 20.) The FAC primarily alleges that Defendant’s website dropped cookies that could be used by third-party websites to build expansive visitor profiles with aggregated data from other non-parties. However, in cases like *In re Facebook*, the “cradle to grave” consumer profiles at issue that tracked activity across browsing sessions and websites were created by the Defendant. 659 F.3d at 599; *see also Semien*, 2026 WL 216333, at *4 (“[Defendant, a databroker,] tracked plaintiffs’ future web-browsing activity across the internet”). At best, the FAC alleges that Defendant’s conduct amounted to informing a third party about Plaintiff’s interactions with its website. This argument is not sufficient to show that Defendant caused any injury Plaintiff may have suffered as a result of visitor data aggregated by those third parties. *See Dawidzik v. Tesla, Inc.*, 2025 WL 3786963, at *1, 4 (C.D. Cal. Dec. 25, 2025) (reaching the same conclusion about similar tracking technology).

Even so, the FAC is further deficient because it contains few allegations about what tracking technologies were actually installed on Plaintiff’s computer, and what those technologies were capable of. Though she indicates that the website dropped cookies generally, and on “a user’s” browser, the FAC does not contain the same detailed

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

allegations about Plaintiff’s own experience. The allegations in the FAC are largely “vague and generalized allegations of the type of data the [tracking software] is capable of collecting from website visitors.” *Rodriguez v. Brushfire Records*, 2025 WL 3692144, at *7 (C.D. Cal. Dec. 15, 2025). Nowhere does the FAC allege what cookies were dropped on Plaintiff’s computer following her visit to the website, for what purpose the third parties dropped those cookies, and how those cookies were ultimately used. In order to satisfy *Popa*’s standing requirement, Plaintiff must allege facts that indicate: (1) Defendant used tracking technologies that collected especially sensitive or wide-reaching information; and (2) those tracking technologies were actually installed on Plaintiff’s computer. *See Kishnani v. Royal Carribbean Cruises, Ltd.*, 2025 WL 1745726, at *4 (N.D. Cal. Jun 24, 2025) (“though Plaintiff alleges that Defendants . . . *could* intrude on Plaintiff’s right to privacy, he fails to convert that hypothetical into concrete harm to *him*”).

Accordingly, the Court DISMISSES Plaintiff’s ECPA claim for lack of standing.

B. Remaining Claims

Having held that Plaintiff lacks standing to bring her ECPA claim, the Court also lacks subject matter jurisdiction over the remaining claims. The basis for jurisdiction in this case is federal question jurisdiction under 28 U.S.C. § 1331, with the Court exercising supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367(a). Having dismissed the sole federal claim in this case, the Court lacks jurisdiction to consider the remaining claims.

IV. CONCLUSION

For the above reasons, the Court concludes that it lacks subject matter jurisdiction over the SAC. Plaintiff may amend the pleading consistent with this Order to correct the deficiencies identified herein. No new parties or claims may be added. Any amended

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No. 2:25-cv-07550-JLS-SSC

Date: April 01, 2026

Title: Silvia Garcia v. Blackhawk Network, Inc.

complaint shall be filed on or before **April 15, 2026**. Alternatively, by that same date, Plaintiff may notify the Court that it does not intend to amend, and the Court will remand the action to state court.

Initials of Deputy Clerk: kd