

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TONY D'ANTONIO, et al.,
Plaintiffs,
v.
SMITH & WESSON INC.,
Defendant.

Case No. 5:25-cv-03085-PCP

**ORDER DENYING MOTION TO
DISMISS**

Re: Dkt. No. 51

In this putative class action complaint, plaintiffs Tony D'Antonio, Thomas Thayer, and Reina Cuevas Garcia allege that defendant Smith & Wesson violated their privacy rights by placing certain cookies on their devices even though they had expressly opted out of receiving such cookies. The Court granted defendant's motion to dismiss the original complaint's claims of wiretapping in violation of the California Invasion of Privacy Act (CIPA), use of a pen register in violation of CIPA, breach of contract, breach of the implied covenant of good faith and fair dealing, and trespass to chattels.¹ The Court also dismissed Garcia's common law fraud claim. The Court denied the motion to dismiss plaintiffs' invasion of privacy and intrusion upon seclusion claims and D'Antonio and Thayer's common law fraud claims. Plaintiffs thereafter filed an amended complaint, which Smith & Wesson again moves to dismiss for failure to state a claim. The amended complaint is substantially similar to the original one, though plaintiffs added additional factual allegations and dropped their breach of implied contract, breach of the covenant of good faith and fair dealing, and trespass to chattels claims.² For the reasons stated below, the

¹ *D'Antonio v. Smith & Wesson Inc.*, 820 F. Supp. 3d 928, 940 (N.D. Cal. 2026).

² The Court's previous order provides extensive background on both the facts and history of the case. *See D'Antonio*, 820 F. Supp. 3d at 932–33.

1 Court denies Smith & Wesson’s motion to dismiss.

2 LEGAL STANDARD

3 Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include a “short and plain
4 statement of the claim showing that the pleader is entitled to relief.” Under Federal Rule of Civil
5 Procedure 12(b)(6), a defendant may move to dismiss a complaint for failure to state a claim upon
6 which relief can be granted. Dismissal is required if the plaintiff fails to allege facts allowing the
7 court to “draw the reasonable inference that the defendant is liable for the misconduct alleged.”
8 *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “Dismissal under Rule 12(b)(6) is appropriate only
9 where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable
10 legal theory.” *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). To
11 survive a Rule 12(b)(6) motion, a plaintiff need only plead “enough facts to state a claim to relief
12 that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

13 In considering a Rule 12(b)(6) motion, the Court must “accept all factual allegations in the
14 complaint as true and construe the pleadings in the light most favorable” to the nonmoving party.
15 *Rowe v. Educ. Credit Mgmt. Corp.*, 559 F.3d 1028, 1029–30 (9th Cir. 2009). While legal
16 conclusions “can provide the [complaint’s] framework,” the Court will not assume they are correct
17 unless adequately “supported by factual allegations.” *Iqbal*, 556 U.S. at 679. Courts do not “accept
18 as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable
19 inferences.” *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (quoting *Spewell*
20 *v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001)).

21 ANALYSIS

22 Plaintiffs’ amended complaint asserts claims for (1) invasion of privacy; (2) intrusion upon
23 seclusion; (3) wiretapping in violation of the California Invasion of Privacy Act (CIPA); (4) use of
24 a pen register in violation of CIPA; (5) common law fraud, deceit, or misrepresentation; and
25 (6) unjust enrichment. Smith & Wesson moves to dismiss all plaintiffs’ CIPA claims, Thayer’s
26 pre-2024 claims, and Garcia’s common law fraud claim.

27 I. Thayer’s pre-2024 claims are not barred by the statute of limitations.

28 CIPA is subject to a one-year statute of limitations, invasion of privacy and intrusion upon

seclusion to a two-year statute of limitations, and common law fraud to a three-year statute of limitations. *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 134 (N.D. Cal. 2020); *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1069 (N.D. Cal. 2021); CCP §338(d). “[A] complaint cannot be dismissed unless it appears beyond doubt that the plaintiff can prove no set of facts that would establish the timeliness of the claim.” *Von Saher v. Norton Simon Museum of Art at Pasadena*, 592 F.3d 954, 969 (9th Cir. 2010) (citing *Supermail Cargo, Inc. v. United States*, 68 F.3d 1204, 1206 (9th Cir. 1995)).

Thayer alleges that he visited Smith & Wesson’s website in 2019 to purchase a firearm, and then again “several times over the next few years” to search for accessories. He visited the website again in or around November 2024 to search for a new firearm, where he allegedly rejected all cookies on defendant’s website. Thayer filed the instant action on April 4, 2025. Smith & Wesson argues that any claims arising from Thayer’s visits preceding 2024 are barred by the relevant statute of limitations.

“The discovery rule ‘postpones accrual of a cause of action until the plaintiff discovers, or has reason to discover, the cause of action.’” *Yetter v. Ford Motor Co.*, 428 F. Supp. 3d 210, 222 (N.D. Cal. 2019) (citing *WA Southwest 2, LLC v. First Am. Title Ins. Co.*, 240 Cal. App. 4th 148, 156 (2015)). If a defendant causes a claim to grow stale through its own deceptive conduct, then the doctrine of fraudulent concealment tolls the statute of limitations. *Id.* at 223 (citing *Aryeh v. Canon Bus. Sols., Inc.*, 292 P.3d 871, 876 (Cal. 2013)). “It is generally inappropriate to resolve the fact-intensive allegations of fraudulent concealment at the motion to dismiss stage.” *Brown*, 525 F. Supp. 3d at 1070 (citations omitted).

For the purposes of defendant’s motion, the Court must accept as true plaintiffs’ allegation that they were reasonably unable to discover the wrongful conduct earlier, and that defendant’s misrepresentations prevented plaintiffs from having actual or constructive knowledge of the facts giving rise to their claims. There is nothing “on the face of the complaint” that would affirmatively bar Thayer from invoking these doctrines. *Chastain v. Howard*, 716 F. Supp. 3d 740, 748 (N.D. Cal. 2024). Accordingly, the Court cannot conclude from the face of the complaint that the statute of limitations precludes Thayer from raising any of the claims asserted therein.

II. Wiretapping

Section 631(a) prohibits “three distinct and mutually independent patterns of conduct: intentional wiretapping, willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (Cal. 1978). The last clause prohibits any person from aiding or abetting another to commit any of the three acts above. Cal. Pen. Code § 631(a). Plaintiffs sufficiently allege a predicate act of section 631(a) such that they plead an aiding-and-abetting violation.

A third party may violate § 631(a) by tracking website interactions, user input data, shopping behaviors, and referring URLs (depending on what information is communicated through the URL title) if the tracking of such data conveys information about the website user’s communications with the website. *Wiley v. Universal Music Grp., Inc.*, 826 F. Supp. 3d 1121, 1135–1136 (N.D. Cal. 2025). Plaintiff D’Antonio alleges that he visited Smith & Wesson’s website to search for a t-shirt. He navigated to the “Gear” section of the website, clicked on different t-shirts, and input “t-shirts and other merchandise” on the website’s search bar. *Id.* Plaintiff Thayer alleges that he searched for the Smith & Wesson 9mm M&P Shield, as well as for “accessories, including holsters, cleaning equipment, branded gear ..., cleaning mats, and [t-shirts].” Plaintiff Cuevas Garcia “research[ed] multiple firearms and firearm accessories,” and used the website’s search bar to search for “firearms, calibers of firearms, and accessories.” These interactions with the website all included specific search inquiries communicated from plaintiffs to the website and thus involved the “contents” of their communications with the website. *Wiley*, 826 F.Supp.3d at 1136; *see also Brown*, 685 F. Supp. 3d at 936 (citing *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 605 (9th Cir. 2020) (holding that a URL constituted content where it “divulge[ed] a user’s personal interests queries, and habits”)).

Smith & Wesson relies on *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073 (C.D. Cal. 2021), to argue that plaintiffs’ proffered “contents” failed to convey an “intended message” and thus fall outside § 631(a). But *Yoon* supports plaintiffs. In *Yoon*, the plaintiff generally alleged what was tracked (“keystrokes, mouse clicks, pages viewed, and shipping and billing information

1 ... [and] the date and time of the visit, the duration of the visit, Plaintiff’s IP address, her location
2 at the time of the visit, her browser type, and the operating system on her device”), but did not
3 include details like what those keystrokes were or the pages viewed. *Id.* at 1082. Here, plaintiffs
4 specify the contents of their searches. While only Thayer’s allegations include a particularized
5 search term, each plaintiff provides enough specificity about their searches to survive a motion to
6 dismiss.

7 Smith & Wesson also argues that because plaintiffs fail to connect their interactions to
8 “any specific cookies, any specific transmission, or any specific third party that allegedly received
9 their communications” their claim must be dismissed. Smith & Wesson reads a level of specificity
10 into the pleading requirements that is unrealistic. Plaintiffs sufficiently allege that third parties
11 used tracking software to obtain their communications. Requiring more at the motion to dismiss
12 stage—before discovery has been completed—would essentially require that a plaintiff be aware
13 of the concealment so that she can simultaneously track it, all for the purpose of pleading details of
14 the alleged violations that, at this point, are only available to the defendant.

15 Finally, Smith & Wesson argues that plaintiffs fail to allege any facts showing that these
16 communications were intercepted while in transit. But plaintiffs sufficiently allege that the data
17 was transmitted from consumers’ browsers to defendant’s website “in real time” and before the
18 data was processed and stored. Smith & Wesson’s arguments that plaintiffs fail to allege the
19 processing platform used by Smith & Wesson and that plaintiffs fail to establish that their
20 communication was actually intercepted are factual issues that are best resolved at a later stage in
21 the case.

22 **III. Use of a Pen Register**

23 California Penal Code § 638.51(a) prohibits “install[ing] or us[ing] a pen register” without
24 a court order under specific circumstances. Section 638.50(b) defines a “pen register” as “a device
25 or process that records or decodes dialing, routing, addressing, or signaling information
26 transmitted by an instrument or facility from which a wire or electronic communication is
27 transmitted, but not the contents of a communication.” *Cf. Mitchener v. CuriosityStream, Inc.*, 815
28 F. Supp. 3d 845, 851 (N.D. Cal. 2025), *appeal dismissed*, No. 25-4990, 2025 WL 3191910 (9th

1 Cir. Oct. 23, 2025) (“A trap and trace device captures identifying information *about* a
2 communication *but not the contents* of a communication.”) (cleaned up).

3 The Court previously dismissed plaintiffs’ pen register claim, holding that they had not
4 alleged that they ever communicated with the website and therefore could not allege that the
5 “dialing, routing, addressing, or signaling information” relating to any such communication was
6 unlawfully tracked. *D’Antonio*, 820 F. Supp. 3d at 937. As noted above, plaintiffs now sufficiently
7 allege that they communicated with the website. They also allege that the cookies installed on their
8 devices enabled tracking of TCP and/or UDP port numbers, protocol-level metadata, and HTTP
9 request header metadata. In plaintiffs view, these three categories of data involving addressing,
10 signaling, and dialing information for their communications with the website are thus are covered
11 by the pen register statute.³

12 Smith & Wesson appears to concede that this type of information may technically fall
13 within the pen register statute but argues that the allegations are still too general to support the
14 claim. It is true that the examples of metadata provided by plaintiffs could include any connection
15 between a device and website. That does not mean, however, that plaintiffs must plead exactly
16 how metadata regarding their communications with the website was tracked. This level of
17 specificity is not required at the pleading stage. *See Wiley*, 826 F. Supp. 3d at 1138 n.4 (noting that
18 Rule 9(b) does not apply to CIPA claims.). Instead, whether the cookies installed on plaintiffs’
19 devices enabled the tracking of information falling within the pen register statute is best
20 determined on the basis of a complete factual record regarding not only what was tracked but also
21 where the purported pen register device was installed and whether it tracked the “dialing, routing,
22 addressing, or signaling information” for outgoing communications from that device.

23 **IV. Cuevas Garcia’s Common Law Fraud Claim**

24 Common law fraud in California requires “(a) misrepresentation (false representation,
25

26
27 ³ The Court notes that some HTTP request header metadata could conceivably involve the
28 contents of a communication rather than addressing, signaling, or dialing information. *See Wiley*,
826 F. Supp. 3d at 1135.

concealment, or nondisclosure); (b) knowledge of falsity (or ‘scienter’); (c) intent to defraud, i.e., to induce reliance; (d) justifiable reliance; and (e) resulting damage.” *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1126 (9th Cir. 2009) (emphasis removed). A state law fraud claim being pursued in federal court must also satisfy Federal Rule of Civil Procedure 9(b)’s particularity requirement by pleading “the who, what, when, where, and how of the misconduct alleged.” *Id.* at 1126. One of the purposes of the specificity required of Rule 9(b) is to “provide defendants with adequate notice to allow them to defend the charge and deter plaintiffs from the filing of complaints as a pretext for the discovery of unknown wrongs.” *Id.* at 1125 (internal quotation marks omitted). The Court previously dismissed plaintiff Cuevas Garcia’s fraud claim because she failed to allege her claim with the required particularity. *D’Antonio*, 820 F. Supp. 3d at 938 (holding that allegations that other plaintiffs visited the website during November 2024 and February 2025 were adequately pleaded while allegations that Garcia visited the website “in or around 2024” were not). Cuevas Garcia now alleges that she visited the website multiple times over a three-month period between June and August of 2024.

Rule 9(b) requires that claims sounding in fraud are pleaded with particularity, but not absolute particularity. *United States v. United Healthcare Ins. Co.*, 848 F.3d 1161, 1180 (9th Cir. 2016) (holding that a time frame ranging two years was sufficient to meet 9(b) standards). A complaint is not doomed by failing to allege “a precise time frame.” *Id.* (citation omitted). As long as the plaintiffs plead enough detail to give adequate notice to an opposing party, they may satisfy Rule 9(b) even when alleging fraud that occurred over a period of time. *See Choi v. 8th Bridge Cap., Inc.*, No. 217CV08958CASA FMX, 2018 WL 3469053, at *8 (C.D. Cal. July 16, 2018) (noting that Rule 9(b) particularity requirements are relaxed for fraud that occurred over a period of time.) Finally, “the rule ‘may be relaxed as to matters within the opposing party’s knowledge.’” *Evans v. Sleep No. Corp.*, No. 1:24-CV-01136-KES-SAB, 2025 WL 1093332, at *4 (E.D. Cal. Apr. 11, 2025) (citing *Moore v. Kayport Package Exp., Inc.*, 885 F.2d 531, 540 (9th Cir. 1989)).

The timeframe alleged by plaintiff Cuevas Garcia is sufficiently specific. Smith & Wesson possesses the knowledge of what cookies were used and how they were used during those months. Garcia alleges that Smith & Wesson made a misleading statement (that she could “Reject All”

1 tracking cookies), explains how it was misleading (in that certain cookies allowing third parties to
2 track her activity were still installed), and identifies when it occurred (between June and August
3 2024). If Smith & Wesson can make any factual showing that during that period of time it either
4 suspended the use of cookies, did not offer a “Reject All” button, or did anything else that could
5 defeat plaintiff’s claim, it now has sufficient information to present that defense. Smith & Wesson
6 therefore has been provided with the adequate notice of Garcia’s claim required by Federal Rule
7 9(b).

8 CONCLUSION

9 For the foregoing reasons, defendant’s motion to dismiss is DENIED.

10
11 **IT IS SO ORDERED.**

12 Dated: September 8, 2026

13
14 
15 P. Casey Pitts
16 United States District Judge
17
18
19
20
21
22
23
24
25
26
27
28