UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DEMETRIUS SMITH, et al.,

Plaintiffs,

v.

RACK ROOM SHOES, INC.,

Defendant.

Case No. 24-cv-06709-RFL

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS AND TO STRIKE

Re: Dkt. No. 59, 83

I. INTRODUCTION

Plaintiffs bring this putative class action against Rack Room Shoes, Inc. after Rack Room allegedly permitted Meta, Attentive, and other third parties to intercept Plaintiffs' personally identifiable communications without consent via trackers that Rack Room embedded in its own website. Rack Room moves to dismiss the Second Amended Complaint for failure to state a claim, and to strike certain portions of that complaint.

For the reasons discussed below, Rack Room's motion to dismiss is **DENIED** as to Plaintiffs' California Comprehensive Computer Data and Access Fraud Act ("CDAFA") and federal Wiretap Act claims, and **GRANTED WITHOUT LEAVE TO AMEND** as to Plaintiffs' California Unfair Competition Law ("UCL") and Consumers Legal Remedies Act ("CLRA") claims. Rack Room's motion to strike is **DENIED**, and its request for judicial notice is **DENIED AS MOOT**. Plaintiffs' motion to extend the deadline to amend the pleadings is **GRANTED**.

II. BACKGROUND

This lawsuit centers around allegations that Rack Room has embedded the code of several third-party companies into its website, and that the third parties' code directs the browser

of a person visiting the Rack Room website to send a message to the relevant third party's server. *See Smith v. Rack Room Shoes, Inc.*, No. 24-cv-06709-RFL, 2025 WL 1085169, at *1 (N.D. Cal. Apr. 4, 2025) ("*Smith I*").

Meta Pixel, one of the allegedly embedded codes, will send messages that can contain a URL revealing the visitor's search queries; the name of the button clicked and the name of the webpage; items viewed and placed in cart; and hashed values corresponding to the visitor's name, address, phone number, and email. *Id.* (citations omitted). If the Rack Room website visitor has a Facebook profile, the Meta Pixel messages will also allegedly contain the visitor's Facebook ID in many circumstances. *Id.* Attentive Tag, another embedded code, will allegedly send messages that can contain the full URL string visited, the product purchased, and the unencrypted phone number and email that the visitor entered when making a purchase. *Id.* Plaintiffs allege that Meta and Attentive use this data to provide Rack Room with services and for Meta and Attentive's own commercial use. *Id.* Rack Room allegedly has a similar arrangement with several other third-parties, although the allegations regarding those products are less detailed. (*Id.* at *1 n. 2.).

Rack Room's motion to dismiss the original complaint was granted in part and denied in part. That prior order held that Plaintiffs had adequately alleged that Rack Room's privacy policy failed to disclose that a third party may "collect, store, and analyze a visitor's browsing and purchase history in a way that is personally identifiable" or that a third party could use that data for its own "commercial purposes." *Smith I*, 2025 WL 1085169, at *2. Therefore, the collection was plausibly done without consent. The prior order did not consider whether Plaintiffs had alleged that the third parties, including Meta and Attentive, were aware of Rack Room's privacy policy.

The prior order further found that Plaintiffs had stated claims for invasion of privacy under the California Constitution and CIPA violations under California Penal Code Sections 631 and 632. *Id.* at *3–5. Plaintiffs' claims under CDAFA, UCL, and CLRA were dismissed with leave to amend for failure to adequately allege an injury under the meaning of each of the

statutes. *Id.* at *6. The Wiretap Act claim was also dismissed with leave to amend because "Plaintiffs' claim that Rack Room violated the Wiretap Act when it 'procured' Meta and Attentive to intercept communication fail[ed] as a matter of law," and Plaintiffs did not "allege that Rack Room itself intercepted their communications." *Id.* at *7.

Plaintiffs then filed the Second Amended Complaint. (Dkt. No. 53 ("SAC").) The SAC contains additional allegations of injury. It adds allegations regarding the "financial value" of Plaintiffs' personally identifiable browsing activity—citing to various news and academic articles that discuss the valuation of browser history data—and alleges that Rack Room and the third parties "unjustly profit[ed]" from Plaintiffs' personal information and online activity. (*Id.* ¶¶ 143–148, 198–99, 224–26, 234–35.) The SAC also adds allegations regarding Rack Room's actions. It alleges that Rack Room "customized and deployed" the third party code, and as a result "played an active role in the use of the [] code to intercept Plaintiffs'" communications. (*Id.* ¶¶ 169, 175.) It further alleges that "once [the collected data is] received and processed by" the third party to include the additional information about the user, Rack Room "knowingly uses the intercepted communications" for its own commercial purposes, including to "run targeted advertisements." (*Id.* ¶¶ 85, 116, 135.) Rack Room now moves again to dismiss, arguing that the deficiencies identified in *Smith I* as to the CDAFA, UCL, CLRA, and Wiretap Act claims have not been cured.

III. LEGAL STANDARD

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court's decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009) and *Bell Atlantic Corporation v. Twombly*, 550 U.S. 544 (2007), a plaintiff's "factual allegations [in the complaint] 'must . . . suggest that the claim has at least a plausible chance of success.'" *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014). The court "accept[s] factual allegations in the complaint as true and construe[s]

the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But "allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Levitt*, 765 F.3d at 1135 (quoting *Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014)). "A claim has facial plausibility when the Plaintiff pleads factual content that allows the court to draw the reasonable inference that the Defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (quoting *Twombly*, 550 U.S. at 556).

IV. ANALYSIS

A. CDAFA

A person who "[k]nowingly 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" violates CDAFA. Cal. Penal Code § 502(c)(2). An "owner . . . of a computer . . . who suffers damage or loss by reason of a violation" of CDAFA "may bring a civil action against the violator." *Id.* § 502(e)(1). Damage or loss is not defined in the statute. The Court previously found that the requirements for pleading a CDAFA claim were met, except that the FAC did not contain non-conclusory allegations of damage or loss by reason of a CDAFA violation. *Smith I*, 2025 WL 1085169, at *6. In the SAC, Plaintiffs allege that they have "suffered economic injury because [Rack Room] caused numerous third parties—including Meta, Attentive, and six data brokers—to unjustly profit from Plaintiffs' . . . personal information and online activity." (SAC ¶¶ 198–99.) Plaintiffs also allege that Rack Room unjustly profited because Rack Room was allegedly able to run targeted marketing campaigns using customer profiles that integrated the customers' personally identifiable browsing history, which Rack Room had told its customers it would not collect. (*Id.* ¶¶ 175, 226.) Plaintiffs seek disgorgement under CDAFA, which is a remedy contemplated by the statute. (*Id.* ¶ 201); *see*

also Cal. Penal Code § 502(e)(1) (victims may seek "equitable relief").

The SAC plausibly pleads that Plaintiffs suffered compensable "damage or loss" under the meaning of CDAFA. "California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 600 (9th Cir. 2020). A disgorgement theory can "constitute[] an injury sufficient to establish [Article III] standing to bring [a plaintiff's] claims for CDAFA violations." *Id.* at 601. Plaintiffs have a "stake in the profits garnered" unjustly from their data, and "[u]nder California law, this stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable." *Id.* at 600. That logic applies equally to the issue of whether plaintiffs have suffered "damage" under CDAFA. Plaintiffs are damaged by not having received a share of the allegedly unjust profits generated from their data. That reading is also consistent with CDAFA's statutory purpose. The legislature found that the "protection of . . . lawfully created . . . computer data is vital to the protection of the privacy of individuals," Cal. Pen. Code § 502(a), and made available equitable relief. Cal. Penal Code § 502(e)(1). In light of that intent, Rack Room's alleged unjust profit from the use of Plaintiffs' private personal information, which holds at least some financial value to Rack Room, plausibly constitutes a "damage or loss" within the meaning of CDAFA. *See Rodriguez v. Google LLC*, 772 F. Supp. 3d 1093, 1109 (N.D. Cal. 2025) (plaintiffs stated a CDAFA claim under a disgorgement theory).

Therefore, Rack Room' motion to dismiss is denied with respect to the CDAFA claim.

B. UCL and CLRA

California law provides that only one "who has suffered injury in fact and has lost money or property as a result of the unfair competition" may bring suit under the UCL. Cal. Bus. & Prof. Code § 17204. Under the CLRA, plaintiffs must allege a "tangible increased cost or burden to the consumer." *See Meyer v. Sprint Spectrum L.P.*, 200 P.3d 295, 301 (Cal. 2009); *see*

also Rojas v. Bosch Solar Energy Corp., 386 F. Supp. 3d 1116, 1130 (N.D. Cal. 2019). The Court previously found that Plaintiffs had not adequately pled harm under the UCL or CLRA. *Smith I*, 2025 WL 1085169, at *6. The generalized allegations in the SAC regarding the value of web browsing data are still insufficient to support Plaintiffs' diminution of value theory, and therefore do not cure the deficiencies identified in the prior order. *See Lau v. Gen Digital Inc.*, No. 22-cv-08981-RFL, 2024 WL 1880161, at *4 (N.D. Cal. Apr. 3, 2024). Moreover, unlike in the CDAFA context, the unjust enrichment theory does not satisfy the statutory standing requirements of the UCL or CLRA, where a plaintiff must show "loss of money or property" or a "tangible increased cost or burden to the consumer," and not merely the general "damage" that must be shown under CDAFA. *See, e.g.*, *Hazel v. Prudential Fin., Inc.*, No. 22-cv-07465-CRB, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023).

Plaintiffs fail to state a claim under the UCL or CLRA. Because Plaintiffs have previously been granted leave to amend and failed to remedy the identified deficiencies, further amendment would be futile. Dismissal of the UCL and CLRA claims is therefore without leave to amend.

C. Wiretap Act

The federal Wiretap Act creates criminal liability for "any person who . . . intentionally intercepts . . . any wire, oral, or electronic communication," or who "intentionally uses" such content "knowing or having reason to know that the information was obtained through" interception. 18 U.S.C. § 2511(1)(a) & (d). "[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, . . . which engaged in that violation." *Id.* § 2520(a). "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). The statute exempts from liability interceptions where the person "is a party to the communication" or when "one of the parties to the communication" consents to the interception. *Id.* § 2511(2)(d). This is often referred to as the "party exception." *See, e.g.*, *In re*

Facebook, Inc. Internet Tracking Litig., 956 F.3d at 607. The party exception is itself subject to a further exception: it does not apply if the interception was "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d). This carveout is frequently called the "crime-tort exception."

The SAC plausibly alleges that Rack Room "intentionally used" "intercepted" communications in violation of 18 U.S.C. § 2511(1). First, use is adequately pled. The SAC alleges that after Rack Room customers' personally identifiable communications was collected by the third-party code at Rack Room's request, those communications (which included, for example, URL strings showing the customer's browsing history) were incorporated into consumer profiles that were provided by the third party back to Rack Room. (*See* SAC ¶¶ 169–70, 175.) Plaintiffs allege that Rack Room then used the consumer profiles, which it knew incorporated the intercepted communications, to guide its targeted advertisements. (*Id.*). Plaintiffs allege this was contrary to commitments in Rack Room's privacy policy. (*Id.*) At the pleading stage, this is sufficient to allege intentional use.

Second, Plaintiffs have plausibly pled that an actionable "interception" occurred. As an initial matter, Rack Room's motion does not contest that Plaintiffs have adequately pled that an interception within the meaning of Section 2510(4) has occurred. At the same time, Plaintiffs do not contest that, as alleged, Rack Room was both a party to the communications, and consented to the interception, triggering the party exception under Section 2511(2)(d). Therefore, the only question is as to whether Plaintiffs have adequately alleged that the crime-tort exception applies, thus rendering the interception unlawful. The Court finds that it does.

When determining the applicability of the crime-tort exception, "the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception—its intended use—was criminal or tortious." *R.S. v. Prime Healthcare Servs., Inc.*, No. 24-cv-00330, 2025 WL 103488, at *4 (C.D. Cal. Jan. 13, 2025) (citing *Sussman v. Am. Broad. Co., Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999)). 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." *Planned Parenthood Fed'n of Am., Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022) (citations omitted)). Second, there is a "separate and independent" component whereby the crime or tort intended must be "beyond the act of [intercepting] itself." *Caro v. Weintraub*, 618 F.3d 94, 98, 101 (2d Cir. 2010). 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. *See Sussman*, 186 F.3d at 1202.

Plaintiffs have adequately alleged that at the time of interception Rack Room had an "independent prohibited purpose" beyond the act of interception itself. Specifically, Plaintiffs allege that Rack Room intended to disclose its customers' personally identifiable communications—which it had promised not to collect or use—to third parties so that it could deliver targeted ads to its customers. Rack Room's alleged disclosure and use of Plaintiffs' personally identifiable information for advertising, in contradiction the commitments it made in its privacy policy, can plausibly constitute a further invasion of privacy beyond the act of intercepting the information alone. *See Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) ("Plaintiffs have adequately alleged that Google's association of their data with preexisting user profiles [without consent] violated state law, including CDAFA, intrusion upon seclusion, and invasion of privacy."); *see also Smith I*, 2025 WL 1085169, at *3. Therefore, Rack Room's alleged purpose was tortious. The allegations are analogous to the purpose of engaging in a HIPPA violation, which courts consistently find constitutes an independent prohibited purpose. *See*, *e.g.*, *R.S.*, 2025 WL 103488, at *5 (tortious intent existed because HIPAA prohibits healthcare providers from knowingly disclosing individually identifiable health information to another person).

It does not appear that Plaintiffs have adequately alleged that Attentive, Meta, or the other third-parties acted with tortious purpose, because Plaintiffs have not alleged that the third parties were aware that Rack Room had not obtained website visitors' consent to the interception in Rack Room's privacy policy or that Rack Room intended to use the data in contravention of

its commitments in its privacy policy. However, this is not fatal to Plaintiffs' claim. Plaintiffs have adequately alleged that Rack Room "customized and deployed" the third party code, and as a result "played an active role in the use of the [] code to intercept Plaintiffs' . . . electronic communications" and "knowingly and unlawfully used those intercepted communications to guide its advertising and marketing efforts." (SAC ¶¶ 169, 175.) Given Rack Room's alleged active role in the act of intercepting, the interception was not done just by Attentive, Meta, or the other third parties, but also alleged to have been actively done by Rack Room. As such, Rack Room's purpose in engaging in that interception is sufficient to satisfy the crime-tort exception. *See, e.g., Luis v. Zang*, 833 F. 3d 619, 637 (6th Cir. 2016).

Rack Room also argues that no tortious purpose can exist here because Rack Room and the third parties' purpose was to make money. Courts are divided as to whether a primary financial motivation shields an intercepting party from liability under the Wiretap Act. Some courts have found that the "crime-tort exception is inapplicable where a defendant's primary motivation is to make money rather than to injure plaintiffs tortiously or criminally." *Roe v. Amgen Inc.*, No. 23-cv-07448, 2024 WL 2873482, at *6 (C.D. Cal. June 5, 2024). However, other courts have held that the "even where a defendant is arguably motivated by monetary gain, the crime-tort exception may nonetheless apply if plaintiffs have adequately alleged that the defendant's conduct violated state law." *R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 901 (C.D. Cal. 2024) (collecting cases); *see also R.S.*, 2025 WL 103488, at *5 (same). Thus, for example, the crime-tort exception applies when a party uses intercepted communications to blackmail someone, even if the primary motivation for engaging in blackmail is to make money. The Court joins the majority courts that have held a monetary purpose does not insulate a party from liability under the Wiretap Act, at least at the motion to dismiss stage.[1]

[1] Rack Room argued for the first time at oral argument that only a violation of a federal law can satisfy the crime-tort exception. This position is contrary to the language of the exception which encompasses violations of the laws of "the United States *or of any State*." 18 U.S.C. § 2511(2)(d) (emphasis added). Furthermore, this argument was not briefed and therefore has been waived at the motion to dismiss stage.

Plaintiffs have adequately stated a claim under the Wiretap Act.

V. MOTION TO STRIKE AND REQUEST FOR JUDICIAL NOTICE

Before responding to a pleading, a party may move to strike from a pleading any "redundant, immaterial, impertinent, or scandalous matter." Fed. R. Civ. P. 12(f). Motions to strike are generally disfavored. *See Shaterian v. Wells Fargo Bank, N.A.*, 829 F. Supp. 2d 873, 879 (N.D. Cal. 2011). A motion to strike should only be granted if the matter sought to be stricken clearly has no possible bearing on the subject matter of the litigation. *See Colaprico v. Sun Microsystems, Inc.*, 758 F. Supp. 1335, 1339 (N.D. Cal. 1991); *Fantasy, Inc. v. Fogerty*, 984 F.2d 1524, 1527 (9th Cir. 1993) ("'Immaterial matter' is that which has no essential or important relationship to the claim for relief or the defenses being pleaded."), *rev'd on other grounds, Fogerty v. Fantasy, Inc.*, 510 U.S. 517 (1994). Statements that do not pertain to, and are not necessary to resolve, the issues in question are impertinent. *Fantasy, Inc.*, 984 F.2d at 1527. If there is any doubt whether the portion to be stricken might bear on an issue in the litigation, the court should deny the motion to strike. *Platte Anchor Bolt, Inc. v. IHI, Inc.*, 352 F. Supp. 2d 1048, 1057 (N.D. Cal. 2004). Just as with a motion to dismiss, the court should view the pleading sought to be struck in the light most favorable to the nonmoving party. *Id.*

Rack Room moves to strike allegations regarding third parties, aside from Meta and Attentive, who allegedly intercepted communications on Rack Room's websites. These allegations are not "redundant" or "immaterial." They relate to Plaintiffs' claims against Rack Room and, at minimum, pertain to Rack Room's intent with respect to Plaintiffs' CIPA claims. Furthermore, the group pleading doctrine (Dkt. No. 59-1 at 11) is inapplicable, as Rack Room is indisputably the only Defendant named in this lawsuit. Rack Room also moves to strike the Nationwide Wiretap Act Class, arguing that *Bristol-Myers Squib Co. v. Superior Court of Cal.*, 582 U.S. 255 (2017), prohibits an exercise of personal jurisdiction over a defendant as to non-resident plaintiffs in a class action. This request is premature because a class has not yet been certified, and all named Plaintiffs reside in California. *See Moser v. Benfytt, Inc.*, 8 F.4th 872, 878 (9th Cir. 2021). Rack Room's motion to strike is denied without prejudice to being re-raised

at class certification.

Finally, Rack Room's request for judicial notice is denied as moot because the Court did not rely on the documents to rule in Rack Room's favor on the UCL and CLRA claims, and the documents do not pertain to the Court's ruling on the CDAFA and Wiretap Act claims.

VI. CONCLUSION

For the reasons discussed above, Rack Room's motion to dismiss (Dkt. No. 59) is **DENIED** as to Plaintiffs' CDAFA and Wiretap Act claims, and **GRANTED WITHOUT LEAVE TO AMEND** as to Plaintiffs' UCL and CLRA claims. Rack Room's motion to strike is **DENIED**, and its request for judicial notice is **DENIED AS MOOT**. Plaintiffs' motion to extend the pretrial deadline to amend the pleadings (Dkt. No. 83) is **GRANTED**, and the deadline is extended to **August 18, 2025**.

IT IS SO ORDERED.

Dated: August 4, 2025

RITA F. LIN
United States District Judge