UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

Demetrius Smith, et al. v. Rack Room Shoes, Inc.

Smith v. Rack Room Shoes, Inc., No. 24-cv-06709-RFL (N.D. Cal. Jan. 23, 2026) · No. 24-cv-06709-RFL · Decided January 23, 2026

SUMMARY

The United States District Court for the Northern District of California partially granted and partially denied Rack Room Shoes, Inc.'s motion to dismiss claims arising from alleged third-party interception and use of consumers' electronic communications and personally identifiable information. The court allowed the plaintiffs' Electronic Communications Privacy Act, California Invasion of Privacy Act wiretap-use, and California Comprehensive Computer Data Access and Fraud Act claims to proceed, but dismissed the CIPA wiretap claim based on server-side technology for failure to adequately allege contemporaneous interception. The dismissal was without leave to amend, and a related motion to certify an earlier order for interlocutory appeal was denied as moot.

OPINION

Demetrius Smith, et al. v. Rack Room Shoes, Inc.
PER CURIAM.
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
DEMETRIUS SMITH, et al., Case No. 24-cv-06709-RFL Plaintiffs,
ORDER GRANTING IN PART AND
v. DENYING IN PART MOTION TO
DISMISS
RACK ROOM SHOES, INC.,
Re: Dkt. Nos. 100, 134 Defendant. 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. The Court has ruled on two prior motions to dismiss, finding that Plaintiffs have adequately stated several claims, including claims under the wiretapping provision of the Electronic Communications Privacy Act (“Wiretap Act”), the California Invasion of Privacy Act (“CIPA”), as well as a claim under the California Comprehensive Computer Data Access and Fraud Act (“CDAFA”). Rack Room now moves to dismiss certain claims in the Third Amended Complaint (Dkt. No. 128 (“TAC”)). In its Motion (Dkt. No. 130), Rack Room challenges Plaintiffs’ previously asserted Wiretap Act and CDAFA claims, and also challenges Plaintiffs’ CIPA wiretap “use” claim and their CIPA wiretap

claim based on “server-side” technology. For the reasons discussed below, Rack Room’s motion to dismiss is GRANTED as to the CIPA wiretap claim based on server-side technology, and is DENIED in all other respects. This order assumes the reader is familiar with the facts of the case, the applicable legal standards, and the arguments made by the parties. Standard of Review. Plaintiffs argue that the Court is bound by the “law of the case” as to the Wiretap Act and CDAFA arguments that Rack Room raises. But “permitting the filing of an amended complaint,” as the Court did here, “requires a new determination” if a subsequent motion to dismiss is filed. Askins v. U.S. Dep’t of Homeland Sec., 899 F.3d 1035, 1043 (9th Cir. 2018). A district court “may decide the [subsequent] motion to dismiss in the same way it decided the first,” but is also “free to correct any errors or misunderstandings without having to find that its prior decision was ‘clearly erroneous.’” Id. Therefore, the traditional motion to dismiss standard applies. Wiretap Act Claim. Rack Room argues that Plaintiffs fail to state a claim under the Wiretap Act because they fail to cite to the sub-section of the act they allege to have been violated. (Dkt. No. 130-1 at 10–11.)1 But the TAC provides sufficient notice of Plaintiffs’ legal theory, including by alleging that Rack Room “played an active role in the use of the computer code to intercept Plaintiffs’ and Class members’ electronic communications” and that Rack Room “knowingly and unlawfully used [the] intercepted communications to guide its advertising and marketing efforts.” (TAC ¶¶ 217, 223.) This is sufficient at the pleading stage. Rack Room argues that the intercepted communications that it allegedly “used” are not “content” under the meaning of the Wiretap Act. (Dkt. No. 130-1 at 11–12.) Plaintiffs have adequately alleged the interception of content for the reasons stated in Smith v. Rack Room Shoes, Inc., No. 24-cv-06709-RFL, 2025 WL 1085169, at *4 (N.D. Cal. Apr. 4, 2025) (“Smith I”). And Plaintiffs plausibly allege that the content is incorporated into the consumer profiles that Rack Room receives and uses. (See, e.g., TAC ¶¶ 101–107, 121.) This is sufficient at the pleading stage. Finally, Rack Room re-asserts its argument that there was no unlawful interception because Rack Room is a party to the alleged communication. The Wiretap Act exempts from liability interceptions where the person “is a party to the communication,” but this exception 1 All citations to page numbers refer to ECF pagination. applies only if the interception was not “for the purpose of committing any criminal or tortious act.” 18 U.S.C. § 2511(2)(d). Rack Room contends that the Wiretap Act’s crime-tort exception does not apply, because: (1) only the third parties’ purpose should be considered and not Rack Room’s; (2) Plaintiffs fail to allege an independent tortious purpose separate from the interception itself; and (3) where a defendant’s primary motivation is to make money, the exception is inapplicable. Each of these arguments fails for the reasons explained in Smith v. Rack Room Shoes, Inc., No. 24-cv-06709-RFL, 2025 WL 2210002, at *4–5 (N.D. Cal. Aug. 4, 2025) (“Smith II”). By Rack Room’s logic, a blackmailer could evade the crime-tort exception by simply arranging to have a listening device send intercepted communications to an unwitting third party, who would then send the information back to the blackmailer. Nothing in the statutory text requires such a perverse interpretation of the crime-tort exception. Plaintiffs have adequately alleged the applicability of

the crime-tort exception and have therefore stated a claim under the Wiretap Act. CDAFA. Rack Room argues that it cannot be liable under the CDAFA, California Penal Code § 502, because the statute does not create secondary liability and California Penal Code § 31 is inapplicable. (Dkt. No. 130-1 at 17–18; Dkt. No. 135 at 7–9.) Rack Room recognizes that this Court and others have applied section 31 in the context of CIPA § 632. See Smith I, 2025 WL 1085169, at *5; see also, e.g., Vera v. O'Keefe, 791 F. Supp. 2d 959, 963 (S.D. Cal. 2011). Rack Room, however, argues that the text of the CDAFA precludes such a result. But there is no material difference between the liability-creating language in section 632 and the CDAFA. Compare Cal. Penal Code § 632(a) (creating liability for "[a] person who, intentionally" and without consent "uses . . . [a] device to eavesdrop") with Cal. Penal Code § 502(c)(2) (creating liability for "any person who . . . [k]nowingly accesses and without permission takes").2 Nor does Rack Room identify any other basis for concluding that the California legislature intended 2 Also compare Cal. Penal Code § 637.2(a) (authorizing a private right of action under CIPA against "the person who committed the violation"), with Cal. Penal Code § 502(e)(1) (authorizing a private right of action under CDAFA against "the violator" of the statute). to exclude "the applicability of Penal Code § 31 with respect to" the CDAFA. Vera, 791 F. Supp. 2d at 963. Plaintiffs have adequately alleged their CDAFA claim. See Smith I, 2025 WL 1085169, at *6. CIPA § 631 "Use" Claim. Plaintiffs' "use" claim is adequately pled for the same reasons discussed above in the Wiretap Act Section. At the pleading stage, Plaintiffs have alleged both intercepted "content" and its subsequent use. CIPA § 631 Server-Side Tracking Claim. As an initial matter, Plaintiffs argue that the Court need not reach this argument at all because Rack Room did not challenge in full their section 631 client-side tracking claim. But the server-side allegations, which involve different technology than the client-side allegations, arise out of an independent set of alleged facts. As such, they constitute a separate claim. Therefore, this order reaches Rack Room's arguments. The TAC includes new allegations regarding server-side tracking. With respect to the server-side technology, the TAC contains the following factual allegations: Defendant also integrates server-side code from Zeta to help intercept consumers' communications and personally identifiable information. Unlike client-side tracking, server-to-server tracking operates akin to an automatic routing device, allowing Defendant to directly forward electronic communications and personally identifiable information to Zeta's servers as consumers navigate its website. Through client-side and server-side tracking tools, Defendant helps Zeta intercept the content of consumers' electronic communications—including full-string URLs, button clicks, and form-field entries—alongside personally identifiable information like hashed email addresses and universal user IDs ("UUIDs") that link to consumer profiles. (TAC ¶¶ 134–35.)3 Rack Room argues that Plaintiffs fail to state a section 631 claim based on the server-side technology because they have not alleged a contemporaneous interception. The Court agrees. Although the TAC alleges that the server-side tracker "directly forward[s]" communications and does so on an "automatic" basis, there is no information about how soon 3 The TAC also alleges that Rack Room "caused Salesforce to receive . . . information

by funneling intercepted communications into the Salesforce Marketing Cloud." (TAC ¶¶ 176, 186.) It is not clear if this refers in part to server-side tracking technology, but to the extent it does, this allegation is deficient for the same reasons explained in this section. this forwarding occurs or whether it is contemporaneous with the receipt. As pled, the TAC thus fails to allege that Zeta "reads, or attempts to read, or to learn the contents or meaning" of Plaintiffs' communications "in transit." Cal. Penal Code § 631(a). Rack Room asks the Court to go further, and find that automatic server-side routing occurring after a communication reaches its destination does not meet the "in transit" requirement of section 631 as a matter of law, even if the technology has the effect of permitting real-time eavesdropping on electronic communications. See, e.g., Doe v. Eating Recovery Ctr. LLC, No. 23-cv-05561-VC, 2025 WL 2971090, at *5 (N.D. Cal. Oct. 17, 2025) ("[T]he only commonsense meaning of transit, at least in the context of this statute, is the transit from the person sending the communication to its intended recipient."). Rack Room points to Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), where the Ninth Circuit adopted a technical interpretation of the Wiretap Act's contemporaneous interception requirement. See id. at 878 (holding that communications must be "acquired during transmission, not while [] in electronic storage"). The analysis in Konop is grounded in Congress's legislative intent—in enacting the Electronic Communications Privacy Act ("ECPA") in 1986—to afford different levels of protection to electronic communications in transit versus stored electronic communications. Id. at 874, 877–78 & n.6. Although courts frequently analyze the Wiretap Act and CIPA's wiretap provision together, see In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 598, 607 (9th Cir. 2020), it is not clear that the analysis in Konop is applicable here. Because CIPA's "in transit" requirement predates the enactment of the ECPA by nearly two decades, see Doe, 2025 WL 2971090, at *6 & n. 10, the congressional intent that shaped the ECPA is of limited value when interpreting CIPA's "in transit" requirement. This is especially true because the California legislature stated that the purpose of CIPA's wiretapping provision was to better address "new devices and techniques" that create a "serious threat to the free exercise of personal liberties." See Cal. Penal Code § 630. California courts have interpreted that directive as requiring a functional rather than hyper-technical approach that broadly applies the statute to new technologies. Ribas v. Clark, 696 P.2d 637, 639-41 (Cal. 1985). In any event, because this claim is already being dismissed based on the deficiencies in the allegations of the TAC, this order does not reach the more fundamental question of whether server-side tracking technology that results in contemporaneous eavesdropping on electronic communications can constitute a violation of California Penal Code § 631. Conclusion. For the forgoing reasons, Rack Room's Motion to Dismiss (Dkt. No. 130) is GRANTED as to the server-side CIPA wiretap claim, and DENIED in all other respects. Dismissal is without leave to amend, because Plaintiffs have already been given two prior opportunities to amend after being on notice that their third-party allegations generally lacked specificity. Rack Room's motion to certify the order in Smith I for interlocutory appeal (Dkt. No. 100) is DENIED AS MOOT. (See Dkt. No. 130-1 at 10 n. 3.) IT IS SO ORDERED.

Dated: January 23, 2026

RITA F. LIN

United States District Judge