Privacy & Cybersecurity Update

October 2025

Recent CDAFA and Wiretap Act Ruling Raises Website Litigation Concerns

Many businesses are already aware of the avalanche of website privacy claims arising from the California Invasion of Privacy Act (CIPA). In these cases, the plaintiffs often argue that their privacy rights have been violated through the use of third-party website tracking tags deployed on publicly available websites. However, in addition to CIPA violations, these plaintiffs now claim that the use of third-party website tracking tags violates their rights under the California Comprehensive Computer Data and Access Fraud Act (CDAFA) and the federal Wiretap Act, among other laws.

In *Smith v. Rack Room Shoes, Inc*. (24-cv-06709-RFL (Aug. 4, 2025)) the U.S. District Court for the Northern District of California issued an order that provides some merit to these types of website privacy claims. Accordingly, businesses should reassess their website compliance efforts to ensure they are protected against these claims. See our Website and Mobile App Compliance & Litigation Checklist for more information.

Background: The Procedural Issues

On September 24, 2024, a putative class action complaint was filed against Rack Room Shoes alleging that the company embedded software code from several third-party companies (e.g., Attentive, Facebook/Meta) into its website, and that the code directed end-user communications and data to the third parties – without the user's consent. The plaintiffs later filed an amended complaint, which contained allegations that were dismissed by Judge Rita F. Lin. However, the plaintiffs filed a second amended complaint (SAC) on April 25, 2025, which was the focus of Judge Lin's August 2025 order.

In the SAC, the plaintiffs alleged that their personally identifiable browsing activity has "financial value" to them and that Rack Room and the third parties "unjustly profit[ed]" from their personal information and online activity. The SAC separately 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'" communications. It further alleged that Rack Room "knowingly uses the intercepted communications" for its own commercial purposes, including to "run targeted advertisements."

In her August order, Judge Lin granted the defendant's motion to dismiss the plaintiffs' claims related to California's Unfair Competition Law and Consumers Legal Remedies Act. However, Judge Lin denied the defendant's motion to dismiss the plaintiffs' CDAFA and federal wiretap claims.

CDAFA Claims and Holding

Judge Lin began her CDAFA analysis by citing a core part of its provisions: 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 the CDAFA. She also noted that the terms "damage" and "loss" are not defined in the statute. The plaintiffs alleged that they "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" and "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." The plaintiffs sought disgorgement under the CDAFA.

According to Judge Lin, "[t]he SAC plausibly pleads that Plaintiffs suffered compensable 'damage or loss' under the meaning of CDAFA" and "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." She further noted that the 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**." Further, according to Judge Lin, the plaintiffs were "damaged by not having received a share of the allegedly unjust profits generated from their data."

Federal Wiretap Claims and Holding

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. The term "intercept" essentially means the acquisition of wire, electronic, or oral communication content. The law exempts from liability interceptions where the person "is party to the communication" or when "one of the parties to the communication" consents to the interception. However, the "party to the communication" exception does not apply if the interception was "for the purpose of committing any criminal or tortious act" in violation of federal or state law (i.e., the "crime-tort exception").

Here, Judge Lin found that the SAC adequately alleged that after Rack Room customers' personally identifiable communications (e.g., browsing history) were collected by the third-party code at Rack Room's request, those communications were incorporated into consumer profiles the third party provided back to Rack Room, and Rack Room used this data to guide its targeted advertisements, which (according to the plaintiffs) "was contrary to commitments in Rack Room's privacy policy."

Judge Lin also found that the crime-tort exception negates the "party exception" within the federal Wiretap Act. For the crime-tort exception to apply, "at the time of the interception, a defendant must have had an independent prohibited purpose beyond the act of interception itself." According to Judge Lin, "**Rack Room's alleged disclosure and use of Plaintiffs' personally identifiable information for advertising, in contradiction to the commitments it made in its privacy policy, can plausibly constitute a further invasion of privacy beyond the act of intercepting the information alone**. Therefore, Rack Room's alleged purpose was tortious."

Interestingly, Judge Lin found that the plaintiffs did *not* adequately allege within their SAC 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, according to Judge Lin, this finding was not "fatal" to the claims against Rack Room because of the independent actions taken by Rack Room to deploy third-party code on its website.

Conclusion

Organizations that deploy third-party cookies, pixels, and tags on their websites should continually evaluate the nature of their data processing activities, including whether they are obtaining opt-in consent for such activities. They should also examine the disclaimers in their website privacy statements and cookie policies to ensure they are not inadvertently creating data privacy risks for fraudulent disclosures or noncompliant business practices.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Kim Sim Sandell
310.382.1309
Kim.Sandell@ThompsonHine.com

Jenna Schneider
513.352.6633
Jenna.Schneider@ThompsonHine.com