

The Consumer Class Action Trend You've Never Heard of: State Wiretap Cases

FEBRUARY 26, 2021

Authors: [Mark S. Eisen](#)

While the consumer class action landscape has been dominated as of late with the usual suspects (Telephone Consumer Protection Act, Fair Credit Reporting Act, etc.) and the new twists on old standbys (current flavor of the month—vanilla false labeling cases), a new trend is bubbling just beneath the surface. Over the last year, plaintiffs' firms have been steadily filing variations of state law wiretap cases over so-called "session replay" technology. That is, technology that tracks consumer interactions, like keystrokes and mouse clicks, with websites.

So far, at least two dozen cases have been filed concerning this technology in California (under the California Invasion of Privacy Act ["CIPA"], Cal. Pen. Code §§ 631, 635) and in Florida (under the Florida Security of Communications Act, Fla. Stat. Ann. § 934.01). These cases essentially allege that the technology in question operates to create a recording of a website visitor's interactions with the site, including keystrokes and mouse clicks and tracks personal data. These cases focus on state classes (limited to the state under which the law the suit is filed) and portrays this online technology as the modern day equivalent of an unlawful wiretap.

The Florida cases are in the relative nascent stages, having been filed in recent months and have not yet been subject to any judicial opinions as to their legal viability. The California cases have, however, been progressing steadily through the court system with a handful passing the pleading stage, thanks in large part to a Ninth Circuit opinion allowing novel CIPA claims over website tracking claims to proceed. These cases turn on a variety of evolving legal issues that seem easy to apply in the context of traditional eavesdropping but awkward, if not bizarre, in the context of the internet. These issues include (i) whether clicks and the like are "communications," (ii) whether the party exception to eavesdropping claims (the notion that parties to a communication cannot eavesdrop on it) applies here and to what extent and (iii) whether the statute covers the technology at issue.

The California cases had their origins in a trio of cases brought in the Southern District of New York under federal law (the Electronic Communications Privacy Act and the Stored Communications Act), but were dismissed with prejudice for failure to state a claim under those laws. *Cohen v. Casper Sleep Inc.*, No. 17CV9325, 2018 WL 3392877, at *1 (S.D.N.Y. July 12, 2018). Since then, the focus has shifted to California and California law (with, now, some cases filed in Florida). At least one of the original CIPA cases in California that was dismissed as part of the New York proceedings moved deep into litigation after surviving a motion to dismiss. See *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827 (N.D. Cal.).

Notably, the technology at issue in these cases is pervasive. Watching the progress of these California and Florida cases will be critical, particularly as there appears to be a race to the courthouse to file claims against the biggest companies using the technology in question (the ever elusive deep pockets). Recent months have shown a dramatic uptick in cases, from the initial test cases filed in New York in 2018 to now a rash of filings over the last three months in California and Florida. It will likewise be important for companies to be cognizant of exactly what information they and their vendors are collecting online. As the push-both legislatively and through novel class actions-to shine a light on data collection increases, it is only a matter of time before plaintiffs' lawyers find their toehold.

For more information on this topic, contact a member of Benesch's [Class Action Practice Group](#).

Mark S. Eisen at meisen@beneschlaw.com or 312.212.4956.