JANUARY 18, 2023

For Your 2023 Worry List: Anti-Wiretap Class Actions Against Website Operators Surge, But Proper Consent Can Reduce Risk

by Vita E. Zeltser

Website session replay technology continues to fuel class action litigation alleging violations of anti-wiretap laws in all-party consent states. In 2021, we issued an alert highlighting that session replay lawsuits were beginning to gain traction. Plaintiffs filed even more cases in 2022, and such class actions present legal risk for any company using session replay technology or other technology that captures a website user's communications without their consent in states where all parties to a communication are required to give consent under applicable anti-wiretap laws. Collecting a consent for online tracking (including for a company's use of session replay technology) is the best way to reduce a company's risk of litigation alleging violation of anti-wiretap laws.

Session replay tools record a person's entire interaction with a website or mobile application, including details such as mouse movements, clicks, keystrokes, and even text entered in an entry field that is deleted before submission. While this technology is relatively new, the laws used by plaintiffs' lawyers to bring session replay cases are not.

The lawsuits allege that session replay technology used on websites/apps violates state anti-wiretapping laws in states like California, Florida, and Pennsylvania that require all parties to a communication (traditionally a telephone call) to consent to the communication being recorded. About a dozen states have all-party consent laws – the states potentially in play vary depending on the specific facts.

For now, let's keep our focus on California due to the surge of anti-wiretap cases there in 2022.

California's "Two-Party Consent" Anti-Wiretapping Statute

The session replay class action cases in California are generally brought under the California Invasion of Privacy Act ("CIPA"), among other causes of action. This 1967 law prohibits reading, attempting to read, or learning the contents of a communication without the consent of all parties to the communication. CIPA allows for a private right of action with no burden to prove actual damages, and allows for statutory damages, making CIPA an attractive mechanism for class action litigation.

In 2022, the Ninth Circuit Court of Appeals held that CIPA applies to internet communications, *Javier v. Assurance IQ, LLC*, 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022), thus greenlighting the plaintiff's bar to bring more lawsuits against website operators that intercept their users' interactions with the website without adequate consent.

Get Proper Consent to Reduce Legal Risk

If your website uses session replay technology or other technology that captures a website user's communications without their consent in states where all parties to a communication are required to

give consent under applicable anti-wiretap laws, obtaining website users' consent for such tracking reduces legal risk. Companies should obtain consent for session replay at the outset of a user's interaction with the website.

Companies may collect that consent by launching a pop-up banner that allows a user to opt in to the website's tracking technology. Such a consent banner should link to an updated cookie policy or privacy policy that describes session replay or other applicable technology to ensure that consent is linked to the website's use of such technology.

It is also important to ensure that a record of user consent is saved should the need arise to prove that user consent was given. Many companies outsource this task by selecting a vendor that will store consent on the website publisher's behalf.

Some Examples of Recent Litigation

Two recent cases (among others) demonstrate that collecting consent puts a company in a relatively better position to defeat anti-wiretap class actions than merely providing notice of the tracking.

In *Javier*, the defendant operated a website through which users could request life insurance quotes. The defendant used a product called "TrustedForm" to record users' interactions with its website. Mr. Javier, the plaintiff, visited the website to request a quote and answered questions about his demographic information and medical history. After filling out the questionnaire, a screen on the website stated that by clicking the "View My Quote" button, the user was agreeing to the defendant's Privacy Policy. In his lawsuit, Mr. Javier alleged that TrustedForm captured his interaction with the website in real time and created a video recording of that interaction. All without his consent.

The Ninth Circuit held that CIPA requires *prior* consent. By the time Mr. Javier had clicked the "View My Quote" button, the session replay software had already been recording his activities. His consent was given after-the-fact and, therefore, it was given too late. The case was remanded to the District Court for further proceedings. Earlier this month, the District Court dismissed the case, holding that the plaintiff's claim was time-barred, but allowed the plaintiff to amend his complaint to satisfy the statute of limitations.

A company's failure to obtain consent was outcome-determinative in *Yoon v. Lululemon USA, Inc*., 549 F.Supp.3d 1073 (C.D. Cal. 2021). The plaintiffs alleged Lululemon used session replay technology to capture website users' interactions with the Lululemon website, including mouse movements, clicks, keystrokes, scrolls, and pageviews. Users were not given the option to consent to the privacy policy. Rather, users could "learn more" about the policy when placing their order. In partially denying Lululemon's motion to dismiss, the District Court held that simply disclosing the use of session replay technology in a privacy policy does not constitute consent and privacy policies alone do not bind users, thereby not constituting consent.

Going Forward

Companies that use session replay technology should collect consent at least from users in all-party consent states like California, Florida, and Pennsylvania to reduce potential exposure under state anti-wiretap statues. Such companies should also monitor legal developments. The *Javier* case, if decided on the merits, will likely provide additional guidance on what proper consent looks like.