Privacy Ruling Highlights Risks Of Third-Party Web Tracking

By **Carol Lumpkin, Matthew Ball and Andrew Wu** (November 22, 2022)

Carol Lumpkin

Matthew Ball

Andrew Wu

Websites have become an essential means for retailers and businesses of all types to market their products and compete in the digital marketplace.

However, learning about customers can come at a price.

Major retailers and many other companies embed third-party session replay software into their websites to capture and analyze a website visitor's activities, keystrokes, and other behavior to improve online marketing and understand user experience, among other things.

But employing this strategy comes with a potential downside.

Companies using third-party session replay software have been the targets of a number of class actions asserting violations of Section 631(a) of the California Invasion of Privacy Act, or CIPA,[1] alleging that the use of this third-party software constitutes an illegal wiretap.

The U.S. Court of Appeals for the Ninth Circuit's recent unpublished decision in Javier v. Assurance IQ LLC highlights the potential risks for companies that implement third-party session replay software or other similar features into their websites to record users' activities and do not receive users' prior consent before recording takes place.

Section 631(a) of CIPA

CIPA is an anti-wiretapping statute that penalizes third-party eavesdroppers who secretly listen to or intercept an ongoing communication between two other parties. A number of putative class actions have been filed under CIPA, as it allows for a private right of action for civil damages.

In relevant part, Section 631(a) prohibits any person who

> willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable.[2]

Over the years, courts have interpreted this section to protect against unauthorized interception of electronic and internet communications.[3]

Because Section 631(a) broadly proscribes third-party interception of a communication, a party to a communication is exempt from liability under Section 631(a), even if that party records that communication, commonly referred to as the party exception rule.[4]

Cases have been dismissed where parties were exempted from liability because they were parties to the communication that formed the basis of a plaintiff's wiretapping claim.[5]

Section 631(a) also imposes liability on any person who "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts" in Section 631(a).[6]

Thus, as framed, if a company retains a third-party session replay provider, a company may be on the hook for aiding and abetting the provider's unauthorized interception of the plaintiff's communication.

Javier v. Assurance IQ

Assurance runs a website where users can request life insurance quotes. To operate its website, Assurance used a third-party session replay vendor to record users' website interactions.

Javier visited Assurance's website and provided his demographic and medical history information in response to an insurance quote questionnaire. Unbeknownst to Javier, the session replay vendor purportedly captured in real time Javier's interactions with the website, including when he was filling out the questionnaire.

After Javier filled out the questionnaire, a "View My Quote" button appeared, which stated that by clicking it, he agrees to Assurance's privacy policy, which disclosed the recording activity. Javier clicked the "View My Quote" button.

Javier later filed a class action against Assurance and the third-party session replay vendor, alleging that the defendants recorded him without his prior consent in violation of Section 631(a) of CIPA.

The U.S. District Court for the Northern District of California granted the defendants' motion to dismiss Javier's complaint without leave to amend because it held that Javier retroactively consented to the recording of his website interactions by agreeing to Assurance's privacy policy, which defeated Javier's Section 631(a) claim.

On appeal, the Ninth Circuit disagreed that retroactive consent is valid under Section 631(a) and reversed the district court's dismissal of Javier's complaint. The Ninth Circuit held that although "written in terms of wiretapping, Section 631(a) applies to Internet communications."[7]

In reaching its decision, the Ninth Circuit predicted how the California Supreme Court would interpret Section 631(a) because the California Supreme Court had not yet decided the issue of retroactive consent.

Although the text of Section 631(a) does not explicitly provide that prior consent is required, the Ninth Circuit held that — in light of other decisions reached by the California Supreme Court concerning CIPA and the broad statutory purpose of CIPA — the California Supreme Court would interpret Section 631(a) to require prior consent of all parties to a communication.[8]

The Ninth Circuit's ruling is narrow.

Because the district court dismissed Javier's complaint on the basis of retroactive consent, the Ninth Circuit did not address the other defenses presented at the motion to dismiss stage, including whether Javier impliedly consented to the recording of his website activity or whether a session replay vendor is considered a third-party eavesdropper under Section

631(a).[9]

Other Issues

The issues left unaddressed by the Ninth Circuit in Javier have been litigated in other cases.

Consent to the interception of a communication is typically a complete defense to a wiretapping claim, and consent can be either express or implied.[10]

For implied consent, courts typically look at the totality of circumstances of a particular communication and assess whether the parties to the communication had adequate notice of the interception.[11]

As for the issue of whether a third-party session replay vendor is an eavesdropper under Section 631(a), there is some disagreement among courts in the Ninth Circuit.

Specifically, courts have grappled with the issue of whether a third-party session replay vendor is an eavesdropper under Section 631(a) or simply an extension of a company — that retained the vendor — that communicates with consumers, excepting it from liability under Section 631(a).

As noted above, parties to communications are not eavesdroppers for purposes of establishing liability under Section 631(a).

This distinction is critical because, if a court determines that a session replay vendor is simply an extension of a company that retained it, then that vendor would technically be a party to the company-consumer communication, excepting it from liability, and the company that retained the vendor would therefore not be liable for aiding and abetting any third-party eavesdropping under Section 631(a).

A few courts have held that a session replay vendor could be considered a third-party eavesdropper under Section 631(a), and one court has held that such a question is better left for a jury to decide.[12]

On the other hand, one judge in the Northern District of California dismissed a few cases on the grounds that session replay vendors are mere extensions of a company because the vendor provides a service that allows the company to analyze the company's own data.

Therefore, a third-party vendor is considered a party to the company-consumer communications.

These cases have suggested that if third-party vendors mine, use or sell data for their individual gain, then the outcome may be different.[13]

Post-Javier Class Actions

Dozens of recent class actions involving Section 631(a) have been filed after the Javier decision.

Some of these lawsuits involve session replay software and have defined the proposed class to include, for example, all persons who used or visited the defendant's website and whose electronic communications were intercepted, recorded, or shared by the defendant "without prior express consent."

Outside the session replay context, some class action complaints involve claims related to internet communications with chatbots, where a consumer provides sensitive personal information to a chatbot without supposedly knowing or consenting to that information being recorded or otherwise used by the defendants.

Many of these new class actions cite Javier for the proposition that Section 631(a) applies to internet communications, and they include allegations that the plaintiff did not provide express prior consent or prior consent.

Takeaways and Perspectives

In light of Javier, there are potential risks associated with utilizing third-party session replay software, chatbots and other similar functions on websites without obtaining the prior consent of website visitors.

Companies should remain proactive and comprehensively review all technologies that collect information from their websites to understand when consent to collect the information is required, confirm that express consent is timely obtained, revisit their privacy policies to confirm that they accurately disclose the collection of information and evaluate the risks associated with collecting or otherwise using information without obtaining prior consent.

To mitigate risk and exposure, companies should ensure that express prior consent is obtained before any monitoring or recording of information occurs.

Finally, from a global perspective, the European Union's General Data Protection Regulation and its U.K. counterpart have been strictly enforcing requirements for consent — which, in addition to being explicit and prior, must also be specific, informed and freely given — to any tracking technologies, whether through cookies or other means.[14]

Considering the GDPR's extraterritorial reach, which makes it inter alia applicable to any monitoring of EU-based individuals, regardless of where a company is established, stakeholders should strive to comply with the various consent requirements and, as the case may be, abide by the stricter rule applicable to their website in view of their effective audience.

Carol Lumpkin and Matthew G. Ball are partners, and Andrew J. Wu is an associate, at K&L Gates LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Cal. Penal Code § 631(a).

[2] Cal. Penal Code § 631(a) (emphasis added).

[3] See Bradley v. Google, Inc., 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006); Javier v. Assurance IQ, LLC, et al., 2022 WL 1744107, at *1 (9th Cir. May 31, 2022).

[4] See, e.g., In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607 (9th Cir. 2020).

[5] See, e.g., In re Google Cookie, 806 F.3d 125, 152 (3d Cir. 2015) (applying California law).

[6] Cal. Penal Code § 631(a).

[7] Javier v. Assurance IQ, LLC, et al., 2022 WL 1744107, at *1 (9th Cir. May 31, 2022).

[8] Id. at *2.

[9] After the Ninth Circuit remanded the Javier case back to the district court, the parties filed renewed motion to dismiss briefing. The case should be monitored as it may impact future litigation.

[10] See, e.g., Campbell v. Facebook Inc., 77 F. Supp. 3d 836, 846 (N.D. Cal. 2014).

[11] Id.

[12] See Revitch v. New Moosejaw LLC, 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019) ("[I]t cannot be that anyone who receives a direct signal escapes liability by becoming a party to the communication. Someone who presses up against a door to listen to a conversation is no less an eavesdropper just because the sound waves from the next room reach his ears directly. That person remains a third party, even as a direct recipient of the speaker's communication."); Saleh v. Nike, 562 F. Supp. 3d 503, 521 (C.D. Cal. 2021) ("[A]s in [Moosejaw], [third-party vendor] does not become a 'party' to the communication simply because it was providing recording and transmission services for Nike."); Yoon v. Lululemon USA, Inc., 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) ("[I]s [the third-party vendor] a tape recorder held by Lululemon, or is it an eavesdropper standing outside the door? This is a question of fact for a jury best answered after discovery ... .").

[13] See Graham v. Noom, Inc., 533 F. Supp. 3d 823, 832 (N.D. Cal. 2021) (unlike vendors who "aggregat[e] [] data for resale, there are no allegations here that [vendor] intercepted and used the [company's] data itself. Instead, as a service provider, [vendor] is an extension of [the company]."); Johnson v. Blue Nile, Inc., 2021 WL 1312771, at *2 (N.D. Cal. Apr. 8, 2021) ("[F]or the reasons stated in Graham v. Noom, [vendor] is not a third-party eavesdropper. As a result, [company] is not liable for aiding and abetting [vendor's] wrongdoing because there is no wrongdoing."); Yale v. Clicktale, Inc., 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) ("[F]or the reasons stated in Noom, [vendor] is not a third-party eavesdropper. It is a vendor that provides a software service that allows its clients to monitor their website traffic.").

[14] See our previous alert here.