ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / Litigation ADVISORY ■

FEBRUARY 3, 2023

2022's Unwelcome Trend of Lawsuits Challenging Website Technology Is Here to Stay

by *Rachel Lowe*, *Donald Houser*, *Dan Felz*, and *Ashley Escoe*

If your company's website is capturing user sessions, has a chat feature, tracks who watches videos on it, or collects biometrics data, your company is at risk of being hit with a class action alleging your website is an illegal wiretap or violating other state and federal statutes, including the California Invasion of Privacy Act (CIPA) and the federal Video Privacy Protection Act (VPPA). The risk is real, and the number of lawsuits and arbitrations being filed is growing.

Session Replay and Website Litigation

Many companies' websites use session replay and similar analytics technology. Among other things, this technology allows retailers to reconstruct a user's website experience and seamlessly fix bugs behind the scenes.[1] Even though this commonplace technology benefits both companies and consumers, the plaintiffs' bar has launched a series of lawsuits challenging this technology as violating state wiretapping and similar statutes.

The trend can be traced to privacy decisions from the Northern District of California. In one of the first session replay cases, *Revitch v. New Moosejaw*, in October 2019, the Northern District of California held that the plaintiff adequately stated a claim for violation of CIPA, California's wiretapping statute, against retailer Moosejaw and its session replay services provider, NaviStone. The court declined to address Navistone's many arguments against wiretapping liability on a motion to dismiss. Following *Revitch* and other California district court rulings, many session replay suits were filed against retailers in California—a state requiring all parties' consent to recording communication. California is not the only all-party consent state, and many session replay technology lawsuits have also been brought in Florida and Pennsylvania, for example.

Not all California judges have agreed with the *Revitch* court's interpretation of CIPA. Some courts held that it was plain that session replay technology vendors were participants to the communications, if any, and there was no third-

[1] Even PACER—the website providing public access to federal court records—tracks users' IP addresses, pages they visit, and addresses of referring websites, ostensibly "for the purpose of evaluating and maintaining our site" to "offer our visitors the best site possible."

party eavesdropper. Other courts held that the content tracked by session replay technology was not the "contents of communications" for purposes of CIPA.

There was also a flare-up of session replay lawsuits filed in Florida. Despite the mixed rulings in California, federal courts in Florida resoundingly rejected session replay lawsuits on 12(b) motions. Those courts held, rightly so, that the retailers had not potentially violated Florida's Security of Communications Act because mouse clicks, site navigation, and other activities potentially tracked by analytics are not the "contents of communications" for the purposes of the statute and dismissed nearly all the Florida cases.

Most recently, this trend has been shaped by two federal appellate decisions. In May 2022, the Ninth Circuit reversed the Northern District of California's dismissal of a session replay technology case in *Javier v. Assurance IQ*. There, the Ninth Circuit held that *prior* consent to wiretapping is required to avoid CIPA liability and that what the court considered to be after-the-fact or retroactive consent (for example, by agreeing to a cookie policy at checkout) does not satisfy CIPA's prior consent requirement. The court specifically noted at the end of its opinion, however, that it had not ruled on the many other arguments raised by the defendant, including implied consent. Indeed, *Javier* was recently dismissed by the trial court on remand, citing CIPA's one-year statute of limitations.

The Third Circuit addressed this technology shortly thereafter. As we described in a recent blog post, in *Popa v. Harriet Carter Gifts*, the Third Circuit ruled that Harriet Carter's vendor, Navistone, was *not* a "direct party" under Pennsylvania's Wiretapping and Electronic Surveillance Control Act. The case was remanded for the district court to consider whether the plaintiff had impliedly consented by virtue of Harriet Carter's privacy policy, which disclosed the sharing of information with third parties.

It is important to note that most of these court opinions were ruling on the defendants' Rule 12(b)(6) motion to dismiss, where the defendants were limited in what factual evidence they could present. The application of the state wiretapping laws to session tracking technologies is still taking shape. Following *Javier* and *Popa*, in late 2022, plaintiffs' firms, including some newer players, filed a number of new session replay lawsuits, primarily in California, Pennsylvania, and Massachusetts.

Website Chat Feature Lawsuits

Likely emboldened by the recent wiretapping rulings from the Ninth and Third Circuits, a new variation of website lawsuits launched. Within the last three months, more than 75 lawsuits have been filed in state and federal courts in California against retailers, insurers, and other companies alleging that they have violated California's wiretapping statute—CIPA—by their alleged use of chat features operated by vendors on their websites. A handful of plaintiffs, acting as "testers," purport to have visited company websites and "had a conversation" via a chat feature—sometimes an AI chatbot—and then later learned that the defendant had allowed a third-party vendor to observe or perform analytics on the chat. These suits allege violations under two CIPA provisions: Penal Code Sections 631 and 632.7. Most of these cases are now pending in federal court after being removed under the Class Action Fairness Act.

Despite the sheer volume of these suits and the statutory damages potentially available under CIPA, many defendants are bullish in fighting against these allegations. Among other reasons, California's wiretapping statute, dating back to 1967, simply was not designed to address this fact pattern—these routine commercial website features bear no similarity to dropping a recording device on a phone line to engage in corporate espionage.

Analytics and chat tools are almost universally used and are designed to help consumers and help retailers engage with them. Further, many consumers impliedly or expressly consent to these website features. Moreover, many chat

features have specific privacy disclaimers or introductory statements for consumers. And the technology vendors are not "third party" participants to the alleged communications; rather, they are parties to the communications and facilitate them. Plus, the defendant retailers' vendors are not mining chat data for their own gain.

Claims under Section 632.7 are especially subject to a challenge in chat technology cases because this statute does not appear to apply when there is no call between two phones being tapped. With these arguments in hand, many retailers moved to dismiss; those motions are currently pending.

Website VPPA Lawsuits

Another trend is Video Privacy Protection Act (VPPA) lawsuits. The VPPA prohibits the knowing disclosure without prior written/electronic consent by a videotape service provider of information that identifies an individual that has requested or obtained specific videos. Congress enacted the VPPA in 1988 after a newspaper published the video rental history for then-Supreme Court nominee Robert Bork. In a spate of recent lawsuits, plaintiffs' firms have been trying to leverage the VPPA to apply to website analytics that track videos watched on company websites. In the last few months, plaintiffs' firms in California, Georgia, and New York have challenged the alleged disclosure of individual viewer information from videos on websites, such as PBS, CNN, and HBO, to analytics providers like Google's Anvato. Some of these suits are paired with state wiretapping claims.

As with the wiretapping statutes, consent is key. The narrow scope of the VPPA is also important to understand. Courts have held "that 'personally identifiable information' means only that information that would 'readily permit an ordinary person to identify a specific individual's video-watching behavior,'" and that likely does not include device serial numbers, for example.[2] And, in a recent ruling, the Northern District of California dismissed a complaint, holding that live broadcasts do not run afoul of the VPPA because "a video must be prerecorded to fall within the VPPA's definition of 'similar audio visual materials.'"[3] Retailers have additional defenses they can assert.

Website Biometrics Lawsuits

Companies that collect website visitors' biometrics data are also facing increasing litigation, especially in Illinois under the Illinois Biometrics Information Act (BIPA), which governs the collection and use of biometric data. Last October saw the first jury verdict for a BIPA lawsuit resulting in a judgment of $228 million against a company accused of collecting, using, and storing fingerprints without informed written consent. A number of companies opted to settle pending biometrics lawsuits in recent years, perhaps in light of the significant potential exposure under BIPA, which provides for statutory damages of up to $1,000 for each negligent violation and $5,000 for each reckless or intentional violation of the Act.

One successful defense of BIPA lawsuits has been the lack of conduct occurring in Illinois. Class actions alleging violations of BIPA brought against Amazon and Microsoft were dismissed on summary judgment in 2022 for lack of sufficient evidence showing that the companies' actions occurred primarily in Illinois. Like other website technology lawsuits, biometrics lawsuits are likely to increase in 2023, especially the recent jury verdict and settlement announcements that came at the end of 2022.

---

2 *Eichenberger v. ESPN Inc.*, 876 F.3d 979, 985 (9th Cir. 2017) (quoting *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 267 (3d Cir. 2016)).

3 *Stark v. Patreon Inc.*, No. 3:22-cv-03131 (N.D. Cal. Oct. 13, 2022).

But Illinois is not the only state where there is risk associated with biometric capturing. Biometrics suits have also recently been filed in California, including against vendors that allegedly capture "voice prints" at their call centers.

Key Takeaways

- Express, prior consent remains the first line of defense. Companies should revisit their privacy policies and the means by which they disclose their privacy policies and gain consent from website visitors.
- Aside from biometrics lawsuits, many website technology cases are only just starting to enter the fact discovery phase, which may provide strong arguments for summary judgment as the case law continues to develop.[4]
- Website technologies are aimed at improving user experiences and are here to stay. Companies should consider their vendor agreements and relationships to determine how vendors are collecting data to mitigate risk of liability exposure.[5]
- Companies should work with their in-house or outside counsel to chart the best path forward, which may include staying the course, while these lawsuits wind their way through the courts.

---

[4] Recall the *Revitch* case mentioned above? There, summary judgment was granted for the vendor because it learned in discovery that the challenged technology was not even on the plaintiff's computer. *Revitch v. New Moosejaw, LLC*, No. 3:18-cv-06827 (N.D. Cal. June 10, 2021).

[5] One distinction the California courts have drawn in CIPA cases is whether or not the vendor "aggregates" the recorded information and independently "uses" the data: "[A] key distinction is whether or not the alleged third-party software provider aggregates or otherwise processes the recorded information, which might suggest that the software vendor independently 'uses' the gathered data in some way." *Williams v. What If Holdings LLC*, No. 3:22-cv-03780 (N.D. Cal. Dec. 22, 2022).

You can subscribe to future ***Privacy, Cyber & Data Strategy*** and ***Litigation*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Rachel Lowe
+1 213 576 2519
rachel.lowe@alston.com

Donald Houser
+1 404 881 4749
donald.houser@alston.com

Daniel J. Felz
+1 404 881 7694
daniel.felz@alston.com

Ashley Escoe
+1 404 881 7756
ashley.escoe@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333