Your Third-Party Website Vendors Might Be Exposing Your Business to a New Theory of Liability: 3 Steps You Should Consider Right Now

Insights
4.15.24

What do a nearly 60-year-old statute on wiretapping and your website have in common? Enough to potentially impose liability on your organization, according to recent lawsuits. We have seen an astronomical increase in wiretapping suits filed against businesses that host third-party cookies, pixels, and other tracking technology on their websites. In fact, we've seen close to 700 lawsuits in California alone, and close to 200 lawsuits across 19 other states combined, since May 2022. That's when a federal appeals court opened the door to users claiming their interactions with websites may be susceptible to third-party interception – and therefore subject to state or federal wiretapping laws. So, what should you do? The key to preventing future litigation will be effectively managing third-party cookies and pixels on your website and ensuring that no data is collected or shared without the appropriate disclosure and consent process in place. Here's what you need to know about this litigation trend, and the three key steps you should consider taking now to protect your business.

Common Themes in Recent Lawsuits: Third Parties Create Havoc

The common theme in recent lawsuits is that website operators are allowing data brokers, ad trackers, social media platforms, chatbot vendors, and other third parties to collect personal data about website visitors without sufficient disclosure and consent. The lawsuits also claim that third parties are using this data for their own commercial purposes, including to sell and re-sell the data and to track the person across the internet to provide targeted ads.

Note These Key Technical Terms

There are a variety of tracking methods that can trigger potential wiretapping suits:

- **Cookies and pixels, beacons, tags, and any third-party software** are small pieces of technology that a website – when visited by a user – allows a third party to place on the user's device to remember information about the user, such as the user's language preference or login information. These tools are used to track your internet journey for specific websites, including for functionality and analytics like counting visitors or determining which pages have been accessed.

- **Session replay and keystroke monitoring** are tools that track user movements or keys pressed, whether that information is submitted to the website or not.
- The newest addition to the tracking lineup is based on the June 2023 decision in *Greenley v. Kochava*. In that case, a California federal judge allowed a claim to proceed alleging that a third-party beacon on a website qualifies as **a pen register or trap and trace device or process** under a law that prohibits their use except with a court order or express consent. These processes do not capture content of a communication, just metadata.
    - **"Pen register"** is a device or process that records outgoing signaling information transmitted by an instrument from which an electronic communication is transmitted.
    - **"Trap and trace device"** is a device or process that captures the incoming signaling information reasonably likely to identify the source of an electronic communication.

Understand the Legal Background

The California Invasion of Privacy Act (CIPA) has prohibited wiretapping for nearly six decades. Under the act, wiretapping occurs when any person "intentionally taps, or makes any unauthorized connection … with any telegraph or telephone wire, line, cable, or instrument … or who willfully and without the consent of all parties to the communication … attempts to read, or to learn the contents or meaning of any message, report, or communication." Penalties range from $5,000 per violation to three times actual damages.

Anyone who "reads, or attempts to read, or to learn the contents" of a communication "without the consent of all parties to the communication," including anyone "who aids, agrees with, employs, or conspires with any person or persons to unlawfully," is considered to have violated the CIPA.

New Trend Has Expanded Wiretapping to Websites

Website wiretapping claims are a new litigation trend. The seminal case that spawned this trend was the 9th Circuit's 2022 decision in *Javier v. Assurance IQ, LLC*. As of March 2024, our firm has identified approximately 683 website wiretapping lawsuits filed in California since the *Javier* decision, and approximately 190 filed in this time period across 19 other states (AZ, DE, FL, GA, IL, IN, MA, MO, NV, NY, NC, OH, OK, OR, PA, TN, TX, WA, and WI). The states with the largest number of wiretapping lawsuits besides California are Illinois, Massachusetts, New York, Pennsylvania, and Washington.

These numbers are just the tip of the iceberg. There are thousands of other wiretapping claims that never make it to the public court system. We've also seen many companies resolve these types of disputes before a lawsuit is ever filed, after receiving demand letters. We also have seen other companies face claims that are resolved through private arbitration (sometimes by multiple "tester" claimants represented by the same attorney filing multiple arbitration claims). We estimate the total claims asserted since *Javier* – whether through a lawsuit, arbitration, or demand letter – to be in the 2,500+ – 3,000

2,500 to 3,000 range.

Review These 3 CIPA Scenarios That Could be Coming for Your Website

Some of the most common situations that have led to website wiretapping claims involve online form managers, digital service vendors, and data brokers.

Online Form Manager

In the *Javier* case mentioned above, the dispute began when a customer filled out an insurance form online. He then alleged that, without his knowledge, a video recording of the entire session was captured in real-time by a third party that managed the form. He claimed the third party created a unique certificate for each user certifying that the user agreed to be contacted. The court held that when "interpreted in light of the broad privacy-protecting statutory purposes," CIPA applies to internet communications and the company's use of the third-party vendor to manage the form violated the law.

Digital Services Vendor

Another lawsuit alleged that Nike used a digital services vendor that allowed Nike to watch and record a visitor's every move on a website in real-time, including mouse clicks, keystrokes, and payment information. The court concluded that a customer alleged sufficient facts to allow his lawsuit against Nike and the vendor to proceed since it appeared the contents of the communication were "recorded." The court also held that Nike was a party to the communication and thus exempt under CIPA, but that the exemption did not apply to the digital services vendor. The court concluded the claim can be alleged against Nike to the extent that Nike is alleged to have aided, agreed, or conspired with the vendor, without plaintiff's knowledge, to provide plaintiff's communications with Nike to the vendor.

Data Broker

In the *Greenley* case, the plaintiff claimed that a data broker provided a software development kit (SDK) to app developers to assist them in developing their apps. In return, the app developers allegedly allowed the defendant to intercept the location data from — and app activity data about — the app users. The defendant then allegedly packaged that data and sold it to third parties for use in targeted advertising efforts. The court held that the plaintiff alleged sufficient facts to show that defendant had installed a "pen register" and allowed the lawsuit to proceed.

Consider Taking These 3 Essential Next Steps

The reality is that no industry will escape the reach of this potential liability – the better question is how to protect your organization. Every business that operates a website needs to take a close look at what pixels, web beacons, cookies, and other tracking technologies you have on your website. You also need to examine whether data from your website chat feature is being disclosed to third parties without restrictions on use and selling of the data.

Here are three specific steps you should consider:

1. Review Your Website

Take a close look at your website to evaluate what pixels, web beacons, cookies, and other tracking tools are in use. Identify what data each tracking tool is disclosing and who is receiving it. Ascertain what third parties are doing with your data once they receive it.

This requires robust scanning of your website to identify all this data and where it goes. Often the problem is that the right hand does not know what the left hand is doing. Sometimes there are cookies and pixels left over from past initiatives or vendors that remain active on the website. Sometimes you don't know the full extent of what cookies are installed as not all cookies are active at the same time. This is why deploying a scanning tool is a good place to start. But make sure you couple that with analysis and review, so you understand the results of the scan.

2. Display Appropriate Disclosures

Ensure your website includes disclosures that adequately describe the parties to the communication, to whom the data is disclosed, the further use (if any) of the data, and where your consumers can access your privacy practices – and all *before* the consumer enters or provides any information. For example, cookie banners should state that data is being disclosed to third parties for targeted ad purposes, if that is the case, instead of only stating that the website uses cookies to improve user experience.

3. Opt-In and Opt-Out Choices

Website visitors should have the option to choose whether they opt in or opt out of the use of data as described in the disclosures. Each of these options should be just as easy to accomplish as the other, known as symmetry of choice. This may involve turning off collection of data through cookies or pixels until a consumer opts-in by clicking a button.

Opt-in consent may not be required by applicable consumer privacy laws like the California Consumer Privacy Act (CCPA). But to avoid a wiretapping claim, your best bet may be installing an opt-in consent mechanism where no data is disclosed to third parties without a user's click on a button. That is, unless a court eventually (and hopefully) decides this is not actually required even under CIPA.

Conclusion

The best way to stay alert is to make sure you are subscribed to Fisher Phillips' Insight System. We will provide the most up-to-date information on data security and the workplace directly to your inbox. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Group.

Related People

Anthony Isola
Partner
415.490.9018
Email

Usama Kahf, CIPP/US
Partner
949.798.2118

Email

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber