

GROWING LEGAL THREAT

BUSINESSES SEE SURGE IN WEBSITE TRACKING LAWSUITS

A GROWING NUMBER of California businesses are finding themselves accused of “wiretapping” website visitors because of common online tracking tools many companies never realized were operating on their websites.

The lawsuits are being filed under the California Invasion of Privacy Act, or CIPA, a 1967 law originally written to combat telephone wiretapping and electronic eavesdropping.

Plaintiffs’ attorneys are using the law to target firms whose websites use tools like cookies that collect information about visitors’ online activity.

According to legal analysts, demand letters often seek settlements ranging from \$15,000 to \$40,000. Any business with a website could be targeted, but e-commerce firms are at particular risk.

The litigation wave has created confusion for businesses as courts have issued sharply different rulings on whether the law applies to modern website tracking technologies. Some judges have allowed lawsuits to move forward, while others have dismissed nearly identical claims.

Lawsuit allegations

In many cases, business owners first learn about the issue when they receive a demand letter alleging their website illegally tracked visitors without proper consent.

Many of the targeted businesses are smaller firms that may not know which tracking technologies are embedded in their websites.

In some cases, tools were added years earlier by website developers, plugins, advertising vendors or software updates. Session replay software, chatbots, advertising pixels, cookies and analytics platforms can collect information about visitors’ online activity.

What lawsuits are alleging

The lawsuits often focus on websites’ use of technologies such as:

- **Meta Pixel.** This is a snippet of tracking code that businesses install on their websites to measure, optimize and build audiences for their Facebook and Instagram ad campaigns.
- **Google Analytics.** This code is embedded in the website to track how a visitor interacts with the site.
- **Session replay software.** This tool reconstructs a visitor’s journey on a website or app by logging user interactions and playing them back as a video-like simulation.
- **AI-powered chat tools.** These include chatbots, which can monitor how users interact with a site.

Plaintiffs argue these tools function like illegal “pen registers” or “trap and trace” devices under CIPA by intercepting communications between website visitors and the business without first obtaining proper consent.



Diverging judgments and pushback

In April alone, several courts issued conflicting decisions involving nearly identical allegations over website tracking technologies.

- One federal court allowed claims against CNN to proceed, while another dismissed similar claims against USA Today.
- California state courts also split over lawsuits involving online retailer Wildflower Brands.
- Some judges have ruled that CIPA was intended for telephone surveillance and should not apply to websites.
- Others have concluded plaintiffs alleged enough privacy harm for lawsuits to proceed.

One federal judge described the statute as “a total mess” when applied to modern technology and called on lawmakers to rewrite it. Business groups have pushed lawmakers to clarify the law and curb what critics describe as abusive litigation tactics.

What you can do

The exposure can be significant because CIPA allows statutory damages of \$5,000 per violation. Plaintiffs’ attorneys often use the threat of class-action litigation and mounting legal costs to pressure businesses into settling quickly.

Privacy attorneys recommend that businesses:

- Conduct audits of all tracking technologies operating on their websites, particularly third-party tools that may begin collecting information without user consent.
- Review cookie banners, consent mechanisms and privacy policies to ensure they accurately disclose what information is collected and when tracking begins.
- Require visitors to affirmatively opt in before certain tracking tools activate.