Court Allows CIPA Claim Involving Third-Party Pixels To Proceed, Ignores Contrary Case Law: What Your Business Needs To Know

Insights
12.04.25

Businesses may be feeling a bit of whiplash from a recent federal court ruling on California's wiretapping law and should be on alert for whether their website tracking technology could be used to file a viable lawsuit. On November 18, the Southern District of California greenlit a lawsuit against sportswear company Adidas, alleging its use of pixels to collect private information violated the California Invasion of Privacy Act (CIPA). The company's disclosure of the data collection wasn't sufficient, the court found, because it failed to get affirmative consent from website visitors. The decision conflicts with the 9th Circuit other district courts that have reached the opposite conclusion when it comes to website tracking technology: that there is no reasonable expectation of privacy in IP addresses, browsing activity, and other device identifiers. Here's a summary of the case, why it's important, and how businesses should react in the constantly changing landscape of digital wiretapping litigation.

When Did All Of This Start?

The Adidas lawsuit involved a website visitor claiming that the sportswear company's use of pixels on its website violated CIPA because the pixels constituted an illegal "pen register." The lawsuit alleged that pixels were installed on their browser when consumers visited the Adidas website and collected their private information without their consent.

A "pen register" or "trap and trace" device is historically a law enforcement device that would be attached to a telephone line to gather outgoing or incoming metadata about callers. California's wiretapping law was amended long ago to prohibit anyone from installing such a device without a court order or consent. But more recently, plaintiffs' attorneys looking to bank on the prospect of statutory penalties across large classes of website users have started to argue that certain tracking technology commonly used by many websites may qualify as pen registers or trap and trace devices. You can track these lawsuits on FP's Digital Wiretapping Litigation Map.

The courts have been divided on whether such claims can proceed, with some finding that plaintiffs cannot allege any actual harm from use of such tracking technology on websites. Other courts have also dug into the legislative history and concluded that lawmakers never intended for CIPA's prohibition on pen registers and trap-and-trace devices to apply to commonly used website tracking

and analytics technology. But still, some judges have allowed these claims to survive dismissal without addressing other conflicting case law.

What Happened in *Camplisson v. Adidas?*

The court allowed the case to move forward, determining that the plaintiff had sufficiently alleged they were harmed by Adidas' data collection and established standing to sue. Even though the pixels on the sportwear company's website only collected IP addresses, the court also said the plaintiff successfully lodged a pen register claim.

Adidas had argued that the plaintiff consented to the use of pen registers, as its privacy policy indicated that the website used cookies and other tracking technology, and its Terms and Conditions, "which is binding on all visitors to the website," incorporates that privacy policy. But the court disagreed, finding that the sportwear company failed to get consent from website visitors because the privacy policy link was not presented to the plaintiff in a conspicuous manner and instead was placed in the footer of the website.

Even if the privacy policy link was conspicuous, the court found that Adidas could not establish that it gained consent to collect the data because the website didn't have a mechanism where a visitor could affirmatively agree to its terms and conditions. Notably, the court did take notice of the archival versions of Adidas' privacy policy and terms and conditions, suggesting the court could have been persuaded otherwise if the links to the policy were presented to each user through a prominent cookie banner.

California Court Split

The ruling breaks with other California-based courts, creating some confusion in the Golden State about what guardrails businesses should apply around the data they collect.

What counts as private information? Several recent decisions from California federal district courts have held that there is no expectation of privacy in IP addresses, device and browser information, geolocation data, among other identifiers, relying on years of past precedent. But, when determining that Adidas' website pixels constituted pen registers, the Southern District offered little analysis, stating only that other courts have found that website-based trackers can be pen registers.

When can I be sued for collecting data? The *Adidas* decision sidestepped a major 9th Circuit Court of Appeals ruling from August that said that the mere collection of data through website interaction isn't a concrete harm sufficient to establish standing. The sportswear company's case was distinct from the August decision, according to the Southern District, because that dispute involved "session replay" technology that only collected information on how the plaintiff interacted with the website. The complaint against *Adidas*, on the other hand, alleged that the pixels on the website could have

collected metadata, IP addresses, unique identifiers related to a user's device or browser, device details, and browser information.

The ruling also failed to address a Northern District of California decision from October that said without particular allegations about the type of browsing, "device fingerprints," and geolocation information disclosed, you can't establish a privacy injury. And the Central District of California came to a similar conclusion in *Price v. Converse*, finding that the collection of "device and browser information, geographic information, and referral tracking" used to "fingerprint the data and deanonymize" the plaintiff was insufficient to establish harm.

What Does This Mean For My Business?

The *Adidas* ruling made clear that merely placing privacy policy links in a website footer was an insufficient way to get consent from website visitors. Courts are also scrutinizing whether users are adequately informed about data collection, and outdated or vague policies may not provide sufficient notice or establish valid consent.

Here are five lessons your business can take away from the *Adidas* decision to better position yourself against CIPA claims and demonstrate a commitment to user privacy and legal compliance.

1. Implement Clear and Conspicuous Consent Mechanisms

- Affirmative consent – such as clicking "I agree" to terms or privacy policies – can help demonstrate that users were informed and agreed to data collection practices.
- Use prominent cookie banners or pop-ups that require users to affirmatively consent to the use of tracking technologies (such as pixels, cookies, and similar tools) before any data collection occurs. We refer to this as a "gatekeeper cookie banner," where a user is unable to access anything on the website without making a choice on the cookie banner, except for being able to view the privacy policy and terms of use.
- The wording of a cookie banner is also critical to establish consent. We recommend explicit language in the display disclosing the use of tracking technology, that data is being shared with third parties, and the purposes for which data is shared such as targeted advertising and analytics.

2. Regularly Review and Update Privacy Policies and Terms

- Ensure that privacy policies and terms of use are up-to-date, accurately describe all tracking technologies in use, and are easily accessible and understandable to users. Privacy counsel can assist in crafting a balanced privacy policy that is specific, but readable for the average consumer.

3. Limit Data Collection to What Is Necessary

- The court in *Camplisson v. Adidas* allowed claims to proceed based on the collection of personal information, even IP addresses. Minimizing data collection reduces exposure and risk under CIPA and similar laws.
- Evaluate the necessity of each third-party pixel or tracker on your website. Limit the collection of personal information (such as IP addresses, device identifiers, and metadata) to what is strictly necessary for business operations.

4. Conduct Regular Compliance Audits of Website Tracking Technologies

- Businesses are often unaware of all the data collection tools operating on their sites, especially those added by third-party vendors. Regular audits help maintain compliance and demonstrate good faith efforts to protect user privacy.
- Periodically audit your website to identify all active tracking technologies, including those deployed by third parties, and ensure they comply with applicable privacy laws and your own policies.
- Obtain legal advice regarding website audits rather than completely relying on a vendor or consultant to complete these audits. Outside counsel who are in the trenches of CIPA litigation will be more in tune with the factual issues that increase litigation risk, as well as new theories of liability being advanced or attempted by plaintiffs' counsel.

5. Monitor Legal Developments and Seek Legal Guidance

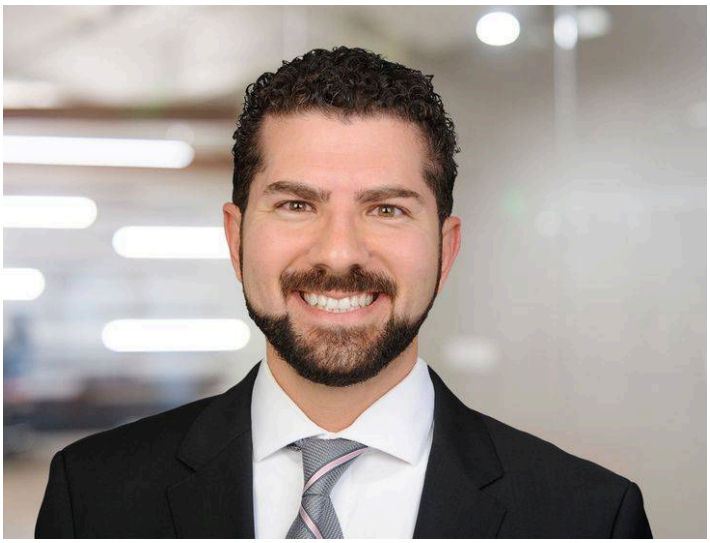
- The legal landscape is rapidly evolving, and courts may interpret statutes differently. Proactive monitoring and legal review can help businesses adapt quickly and avoid costly litigation.
- Stay informed about new case law, regulatory guidance, and legislative changes regarding CIPA and similar privacy statutes. Consult with legal counsel to assess risk and update practices as needed.

Conclusion

To stay informed, subscribe to Fisher Phillips' Insights System for timely updates on CIPA and other privacy-related trends. For personalized guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Digital Wiretapping Litigation Team. You can also explore additional resources on our U.S. Privacy Hub at any time.

Related People

Catherine M. Contino
Associate
610.230.6109
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

California Litigation and Appellate

Litigation and Trials

Digital Wiretapping Litigation

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills