Website Tracking Lawsuit Against Retailer Dismissed for Lack of Standing: What California Ruling Means for Your Business

Insights
10.23.25

A California federal court recently handed businesses another major victory in the ongoing wave of privacy lawsuits targeting website analytics and tracking tools. On September 30, Judge Fernando Aenlle-Rocha of the Central District of California dismissed a proposed class action against a national retailer for lack of Article III standing. The court found that the plaintiff failed to allege any specific, concrete harm stemming from the company's use of standard website data collection software – a decision that adds to a growing body of rulings limiting these suits. The *Price v. Converse, Inc.* case represents another data privacy win for businesses defending against the surge of lawsuits filed under the California Invasion of Privacy Act (CIPA) based on routine marketing and analytics tools – a trend led by a small number of plaintiff firms bringing near-identical complaints across industries.

The Case

This isn't the first time Converse has successfully defended against such claims. Earlier this year, the 9th Circuit Court of Appeals affirmed the company's victory in a similar CIPA website chat "wiretap" case, rejecting attempts to stretch the law beyond traditional surveillance contexts. You can read our coverage of that earlier decision here.

In the most recent case, a plaintiff claimed that Converse violated the California Trap and Trace Law (part of CIPA) by sharing data with a social media company's pixel through a software development kit. Plaintiff alleged that this "SDK" collects data that may be used as an electronic fingerprint to assist the social media company in profiling the user based on their activity on Converse's website. The plaintiff argued this "tracking tool" acted as an illegal "trap and trace device" by collecting browser, device, and location data to identify users without prior opt-in consent.

Weaponizing Data Privacy Claims

This also isn't the first time that the plaintiff's law firm has filed such a lawsuit. In fact, the Los Angeles-based plaintiffs' firm has filed over 550 such CIPA website pixel claims – the second-most prolific law firm in the country. It has likely sent thousands of demand letters that never resulted in litigation but have led companies to collectively pay out millions of dollars in settlements.

Given the dollars at stake, it's not surprising that many of these litigation factories are springing up to take advantage of these novel legal theories, with more plaintiffs' firms jumping on the bandwagon. They often file cookie-cutter complaints repeating the same allegations in the hopes of leveraging a quick settlement.

The Court's Decision

In this most recent case, Converse scored a win and the court dismissed the case for lack of standing. The judge found that:

- The plaintiff failed to allege a concrete, particularized injury as required by Article III of the US Constitution.
- Merely claiming a statutory violation of CIPA is not enough. There must be a harm closely related to traditional privacy torts like intrusion upon seclusion or disclosure of private facts.
- The alleged data collection through "device fingerprinting," while potentially undesirable, did not constitute the kind of "highly offensive" invasion of privacy recognized by courts.

The court found that plaintiff's allegations were insufficient to show any "concrete injury" comparable to traditional privacy harms. As Judge Aenlle-Rocha explained, the plaintiff failed to allege that the tracking software "caused her to experience any harm remotely similar to the highly offensive interferences or disclosures actionable at common law."

In reaching its conclusion, the court relied heavily on the 9th Circuit's recent decision in *Popa v. Microsoft*, emphasizing that an "injury in law is not an injury in fact."

5 Key Takeaways for Businesses

This case underscores a growing judicial recognition that many CIPA "pixel" lawsuits are overreaching – targeting ordinary marketing activity rather than genuine invasions of privacy. Here are some key lessons your business can apply to your data practices given this victory.

1. Standing Remains a High Bar for Web Tracking Claims

Courts are increasingly dismissing suits that allege technical privacy violations without real-world harm. Businesses that use tracking tools, analytics pixels, or similar code may face lawsuits, but plaintiffs need to show more than mere data collection and sharing in order to advance the ball.

2. Audit Your Website Tools, But Keep Perspective

Even though standing defenses can be successful, prevention is still the best defense:

- **Audit your site** for tracking tools and third-party integrations.

- **Regularly monitor cookie consent process.** You should regularly have an independent third party (whether a law firm or other vendor) test your website cookie consent mechanism to verify that the opt-in and opt-out choices continue to function as intended.
- **Disclose data collection** practices clearly in your privacy policy.
- **Obtain user consent** where required, particularly for behavioral tracking. Consider obtaining opt-in consent prior to firing up third party cookies on your website. Even though no California law currently requires such prior opt-in consent for website cookies, plaintiffs in CIPA litigation are claiming that it's a violation of CIPA to allow cookies to share date with third parties in real time without first obtaining opt-in consent. There is no controlling authority yet on whether plaintiff's theory of liability is correct, but the best way to avoid this litigation altogether is to do what plaintiffs' attorneys are saying you should be doing. Again, we're not saying they are right; rather, we're saying you don't need to be a target.

3. Stay Ahead of State Privacy Laws

CIPA-based suits are on the rise in California, and similar litigation is spreading across 29 other states under similar wiretapping laws (like in Illinois, New York, Colorado, Texas, and even Florida of all places). Businesses and retailers should ensure compliance with all applicable state privacy and wiretapping laws.

4. Keep Compliance Documentation Ready

Maintain records of:

- User consent mechanisms
- Vendor contracts governing data sharing; and
- Regular audits of cookies, analytics, and embedded code.

5. Expect Ongoing Divergence Between Courts

While this decision limits certain consumer claims in federal court, plaintiffs may refile in state court under broader standing doctrines or pursue other privacy statutes. Federal courts are split on whether website analytics data – like IP addresses or device identifiers – are private enough to support a claim. While this case falls on the business-friendly side, others have reached the opposite conclusion, so proactive compliance remains essential.

Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. You can also visit FP's Digital Wiretapping Litigation Map for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips

attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group or Digital Wiretapping Litigation Team.

Related People

Catherine M. Contino
Associate
610.230.6109
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Xuan Zhou, CIPP/US, CIPM, CIPP/E
Associate
858.597.9632
Email

Service Focus

Litigation and Trials

Privacy and Cyber

Digital Wiretapping Litigation

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills