Insights, News & Events

CALIFORNIA COURT LIMITS WEBSITE PRIVACY CLAIMS: KEY TAKEAWAYS FOR WEBSITE OPERATORS AND BUSINESS OWNERS

Insights
Jan 7, 2026

A new California court decision delivers welcome news for website operators and businesses caught in the surge of website privacy litigation. In the December 10 *Rodriguez v. Ink America International Group LLC decision*, an L.A. County state court pushed back on efforts to stretch the California Invasion of Privacy Act (CIPA) far beyond its original purpose. Enacted in 1967 to combat traditional wiretapping and eavesdropping in telephone calls, CIPA was never intended to regulate routine website technologies or modern internet analytics. Yet in recent years, plaintiffs' attorneys have increasingly invoked the statute to challenge common online tools such as cookies, pixels, chat features, and session replay technologies, labeling them as unlawful "wiretaps," "pen registers," or "trap and trace" devices. Last month's decision rejected this expansive interpretation, signaling a potential shift in favor of website operators and businesses.

The Case at a Glance

In *Rodriguez*, the plaintiff alleged that Ink America violated CIPA by operating a website that collected users' IP addresses and deployed analytics and beacon software. According to the complaint, these tools allegedly allowed third parties to collect and link identifiers such as IP addresses, browser and operating system data, geolocation information, and email addresses. Based on these allegations, the plaintiff claimed that Ink America's use of website analytics constituted a prohibited "pen register" or "trap and trace device" under CIPA.

Related People

Vivian Isaboke, CIPP/US, CIPM

Associate

908.516.1028

Usama Kahf, CIPP/US

Partner

949.798.2118

The Court's Holding: A Win for Website Operators

The court dismissed the claims without leave to amend, holding that the complaint failed to state a viable claim. In reaching its decision, the court emphasized several key points:

- **CIPA conflicts with the CCPA and Legislative Intent**. The court found that CIPA's statutory language is ambiguous when applied to modern internet technologies. To resolve that ambiguity, the court examined the California Consumer Privacy Act (CCPA) and concluded that the plaintiff's expansive reading of CIPA would effectively render the CCPA meaningless.

  The court reasoned that if routine website analytics tools were treated as criminal "pen registers" under CIPA, their use without a court order would be illegal. This result would directly conflict with the CCPA, which expressly contemplates the lawful use of such tools so long as businesses provide appropriate notice and honor opt-out and deletion rights.

  The court further emphasized that using CIPA to attack conduct already governed by the CCPA would "punish compliance" and defy legislative intent. Expanding CIPA in this manner would create confusion rather than enhance consumer protection, particularly where private settlements do not result in clearer rules or stronger safeguards. Ultimately, the court concluded that the pen register statute "did not, and does not, criminalize the process by which websites communicate with users who choose to access them."

- **Service Provider Exception.** In another notable win for business operators, the court held that website operators qualify as "electronic communication service providers" under CIPA Section 638.50(b). As a result, even if the collection of an IP address were considered a "pen register," Section 638.51(b) provides an exception allowing recording or use of such information to operate, maintain, test, or protect the service.

- **CIPA Is Limited to Telephonic Surveillance.** Finally, the court reaffirmed that CIPA's pen register provisions were intended to address telephonic-style surveillance, not the routine operation of commercial websites or commonly used analytics software. Given the statute's ambiguity in

Chelsea Viola
Associate
213.403.9626

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

this context, the court declined to extend CIPA to ordinary website analytics practices.

Why This Decision Matters

Rodriguez takes a different approach from many prior CIPA cases. Rather than treating the statute as unambiguous, the court found ambiguity, examined legislative intent, and dismissed the pen register and trap-and-trace claims outright.

If adopted more broadly, this reasoning could significantly narrow, or potentially eliminate, CIPA claims based on routine website analytics. However, because *Rodriguez* is just a trial court decision, it does not completely eliminate CIPA litigation risk. Until we get an appellate court to weigh in, other courts across the state may continue to apply broader interpretations.

What Website Operators and Businesses Should Do Next

While *Rodriguez* provides a strong defense, it is not a silver bullet. Nevertheless, the decision offers several practical takeaways for businesses. We recommend that website operators and businesses consider the following steps:

- **Ensure CCPA Compliance.** The court's reasoning reinforces that the CCPA remains the primary framework governing website data collection. Businesses should ensure that privacy notices, opt-out mechanisms, and vendor disclosures are accurate, complete, and up to date.
- **Audit Website Technologies.** Organizations should maintain a comprehensive inventory of analytics tools, tracking technologies, chat features, and third-party scripts deployed on their websites. Regular audits are essential to understand what data is collected, how it is used, and whether it is shared with third parties.
- **Review Service Provider Agreements.** Agreements with analytics and advertising service providers should clearly define permitted data uses, prohibit secondary uses, and align with CCPA service provider requirements where applicable. Strong contractual controls are critical to supporting the "service provider" defense relied upon by the court in *Rodriguez*.

- **Monitor CIPA Developments.** Although *Rodriguez* suggests a potential shift in how courts may evaluate CIPA claims based on website analytics, the legal landscape remains unsettled. Businesses should monitor subsequent trial court decisions and any appellate rulings that may reinforce or reject this reasoning.
- **Consult Experienced Legal Counsel.** Businesses should work with experienced privacy counsel to assess website data practices, evaluate potential exposure under CIPA and related privacy laws, and develop practical and defensible compliance and litigation strategies in light of evolving case law.

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.