Insights, News & Events

CALIFORNIA COURTS CREATE CONFUSION IN DIGITAL TRACKING CASES: HOW BUSINESSES CAN NAVIGATE CONFLICTING RULINGS

Insights
Mar 23, 2026

California Courts Create Confusion in Digital Tracking Cases: How Businesses Can Navigate Conflicting Rulings

Several recent California state court decisions have thrown companies into a state of confusion about whether they can face claims under the California Invasion of Privacy Act (CIPA) for use of tracking technologies on websites and apps. In two cases, courts dismissed the claims without leave to amend, while a third case – sitting in the same courthouse as one of the first two – allowed the claim to proceed. The two helpful court decisions concluded that CIPA's "trap and trace" provisions don't extend to website analytics or similar internet tracking technologies. But the other troubling ruling went the opposite way and said that website cookies might qualify as pen registers or trap and trace devices. These rulings create uncertainty for businesses operating in California and raise many questions about best practices. This Insight will dive into the three cases and provide businesses with a game plan to manage this turbulent time.

What Courts Have Decided?

Schallert v. Palo Alto Networks (Los Angeles County Superior Court)

- Facts:

Related People

Usama Kahf, CIPP/US
Partner

949.798.2118

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

- The plaintiff alleged that software embedded on the defendant's website functioned as a trap-and-trace device under CIPA 637.2(a) by capturing electronic identifiers of website visitors.

- Key Holdings:
  - The court focused on statutory interpretation, emphasizing that the CIPA trap-and-trace framework repeatedly refers to telephone lines, including provisions requiring a court order to identify the specific telephone line to which the device will be attached.
  - Based on this structure, the court concluded that the statute's trap-and-trace provisions were intended to regulate telephone surveillance, not internet communications.
  - The court also observed that no binding California authority has held that CIPA's trap-and-trace provisions apply to websites, and it found the federal cases cited by the plaintiff unpersuasive.

Blalock v. EquipmentShare.com Inc. (Orange County Superior Court)

- Facts:
  - The plaintiff similarly alleged that website technology violated California's trap-and-trace law (Penal Code § 638.51).

- Key Holdings:
  - The court emphasized that the legislative history indicates the trap-and-trace provisions were enacted primarily to allow law enforcement to obtain emergency orders for telephone surveillance devices, not internet monitoring tools.
  - Although the statute broadly defines devices that capture routing or signaling information, the court found that the overall statutory scheme was directed at telephone communications.
  - The court further analyzed that the statute was enacted in 2015, when internet communications and communicating through computers was not a new technology. If the Legislature had intended to regulate

858.597.9632

Service Focus

Litigation and Trials

Privacy and Cyber

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

website tracking technologies or other internet communications, it could have explicitly included them but did not.

Barajas v. La Mesa RV Center, Inc. (Los Angeles County Superior Court)

- Facts:
  - The plaintiff alleged that X Corp's tracking software development kit was installed on defendant's website to identify website visitors without user consent, which is a violation of California Trap and Trace Law Penal Code § 638.51.
- Key Holdings:
  - The court held that the legislature enacted CIPA to broadly protect privacy, reflecting a strong policy against intrusive surveillance. Nothing in the statute limits this definition to telephones, meaning the statute may potentially apply to internet communications and websites.
  - The court rejected the argument that the California Consumer Privacy Act (CCPA) replaces or conflicts with CIPA. The CCPA explicitly states that it supplements existing laws, so both statutes can operate concurrently.
  - The court distinguished between metadata and content of communication.
    - The court concluded that technical identifiers (metadata), such as browser characteristics, installed fonts, screen dimensions, system settings and device specifications and routing data, are not the contents of communication.
    - The court contrasted this case with another involving TikTok tracking software, where the technology allegedly collected biographical information (e.g., name, date of birth, and address), which the court found to constitute the content of a communication.

Practical Implications for Businesses

The three recent California state court decisions reflect diverging judicial approaches to whether CIPA's trap-and-

trace provisions apply to modern website technologies. While two courts rejected the application of CIPA to website tracking, another court suggested that the statute could potentially reach certain internet-based data collection practices.

Federal courts have sometimes adopted a broader view of privacy statutes, with most federal courts holding that website cookies and pixels can qualify as pen registers or trap and trace devices for purposes of a motion to dismiss. This split between state and federal courts indicates that future courts could adopt either interpretation, leaving continued litigation risk for businesses.

Both *Schallert* and *Blalock* emphasized that internet communications were already widespread when the Legislature enacted the relevant provisions in 2015. Those courts reasoned that if lawmakers intended to regulate website tracking technologies, they could have said so explicitly. By contrast, the court in *Barajas* emphasized CIPA's broad privacy purpose and declined to limit the statute to telephone communications.

The *Barajas* court further held that the CCPA did not displace or replace CIPA. Instead, the statutes operate in parallel, meaning that businesses that fully comply with CCPA requirements may still face claims under CIPA. For businesses that have been trying to comply with the CCPA since it took effect in 2020, this holding by the *Barajas* court reflects a lack of understanding of how the CCPA regulates data sharing through website tracking technology. The CCPA expressly permits such disclosure of data, so long as consumers are provided with an effective **opt-out** mechanism.

Countless resources were spent by the state and private parties in the CCPA rulemaking process, which establishes exactly what businesses have to do to lawfully deploy third-party cookies on their websites. And yet a general law (CIPA) that says nothing about cookies and pixels is being interpreted by plaintiffs' attorneys and some courts to prohibit businesses from doing exactly what the CCPA permits and regulates, finding that CIPA requires **opt-in** consent **before** a business can share any data with third parties through website cookies.

The *Barajas* court seems to posit that an opt-out and an opt-in framework can live concurrently. Perhaps telling is that

the *Barajas* court decided to ignore numerous decisions by state court judges on this issue while finding as "persuasive" the federal district court decisions interpreting California law.

Key Case Alert: *Variety Media LLC v. Superior Court* is currently pending before the California Court of Appeal and is expected to address whether CIPA § 638.51 extends to commonly used website tracking technologies. This will be the first appellate authority on this issue, but it may take a year for a decision to be issued. Until appellate courts provide clearer guidance, companies should assume that claims related to web analytics, SDKs, pixels, and other tracking tools will continue to be litigated.

Key Takeaways for Businesses

These conflicting decisions create uncertainty for businesses, but you can glean some important guidance to help minimize your risk if you operate websites or use analytics tools.

1. Privacy Compliance Remains Important

Although some courts have effectively abrogated the CCPA's opt-out framework, compliance should remain a priority. Are you audit ready? This should be the question for 2026 and beyond. Even if you decide to turn off all third-party cookies on your website until after a consumer's opt-in consent, there are many CCPA requirements that continue to apply, including ensuring that consumers who do opt-in to cookies have an easy and effective process for changing their mind and opting out. Maintain strong privacy disclosure and consent practices as plaintiffs continue to test alternative privacy theories under CIPA and other statutes. Work with your FP Privacy and Cyber counsel to make sure your policies and practices are in good shape.

2. Implement Consent Mechanisms Where Appropriate

Consider using cookie banners or consent management tools that allow users to understand and control the use of tracking technologies. While not always legally required in every context, such tools can help mitigate risk and demonstrate good-faith privacy practices.

3. Maintain Clear Privacy Disclosures

Ensure that website privacy policies and cookie disclosures accurately describe the categories of data collected through website technologies and the purposes for which the data is used. Transparent disclosures can reduce litigation risk and strengthen defenses if claims arise.

4. Monitor Litigation Trends in Website Privacy Cases

Website privacy litigation under CIPA and related statutes continues to evolve rapidly. Companies should monitor developments in California courts, particularly as appellate courts may eventually address these issues. For a broader view of digital wiretapping litigation trends nationwide, you can consult the Fisher Phillips Digital Wiretapping Litigation Map, which tracks related cases across all 50 states.

5. Consider Early Defense Strategies

If a complaint is filed alleging that website technologies constitute a trap-and-trace device, these recent rulings suggest that early motions, such as demurrers or motions to dismiss, may be an effective strategy before discovery.

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. 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.