Insights, News & Events

CALIFORNIA FEDERAL COURT'S DENIAL OF CLASS CERTIFICATION MAY RESHAPE WEBSITE TRACKING LITIGATION: 5 STEPS FOR BUSINESSES

Insights
Jun 23, 2026

California Federal Court's Denial of Class Certification May Reshape Website Tracking Litigation: 5 Steps for Businesses

In one of the most significant class action rulings in website tracking litigation to date, a California federal court just denied class certification in a long-running dispute and suggested that obtaining such certification may prove substantially more difficult for plaintiffs than surviving a motion to dismiss. The June 16 decision in *Ingraham v. Capital One Financial Corp*. from the U.S. District Court for the Northern District of California could offer your business a roadmap for defeating similar website wiretapping class actions. What do you need to know about the case and what are the five steps you should consider taking?

Why is This Decision Important?

While courts have spent the last several years addressing motions to dismiss in privacy and wiretapping class actions involving website and mobile app use of cookies, pixels, analytics tools, and other online tracking technologies, relatively few courts have confronted the question of whether these cases can be certified as class actions.

The Allegations

Plaintiffs alleged that Capital One's credit card application and preapproval website used tracking technologies that transmitted applicants' personal and financial information to

Related People

Usama Kahf, CIPP/US
Partner

949.798.2118

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

third parties without consent. They asserted claims under federal and California privacy laws, including violations of the Electronic Communications Privacy Act (ECPA), the California Invasion of Privacy Act (CIPA), and the California Consumer Privacy Act (CCPA), as well as common law claims for negligence and unjust enrichment.

Plaintiffs sought certification of proposed classes targeting two categories of tracking technologies used on Capital One's credit-card application and pre-approval website:

- **Server-to-Server Technology Classes**: A nationwide class and California subclass consisting of users whose information allegedly was collected or transmitted through server-to-server data-sharing technologies.
- **Tracking Technology Classes**: A nationwide class and California subclass consisting of users whose information allegedly was collected or transmitted through browser-based tracking technologies.

The Legal Standard

To certify the class of website visitors, plaintiffs needed to offer a reliable method for proving:

- data transmission of each class member's data;
- that each class member did not consent (even implicitly) to such transfer of data; and
- that each class member suffered an injury because their sensitive data was disclosed.

The Court Identified 3 Obstacles to Class Certification

What makes the decision particularly significant is that the court did not rely on a single defect to deny class certification. Instead, it identified three separate predominance problems, each of which independently defeated certification.

1. Individualized Questions Regarding Data Transmission Defeated Predominance

The court found that plaintiffs could not establish through common proof that the same information was transmitted for all putative class members. According to the court, the evidence demonstrated significant variation in the operation

858.597.9632

Service Focus

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

of the challenged tracking technologies and the information allegedly disclosed.

The court emphasized that:

- Different tracking technologies collected different data.
- Browser settings and user behavior affected what was transmitted.
- Even named plaintiffs' transmissions were disputed.
- Determining what information was shared would require examining each person's application and interactions individually.

Because liability depended on what information was transmitted from a particular user under particular circumstances, the court concluded that individualized issues predominated over common questions.

2. Individualized Consent Issues Continue to Defeat Predominance

Although plaintiffs argued that Capital One relied on uniform privacy disclosures, the court found that the consent inquiry would require individualized analysis.

The court noted that:

- Users encountered different disclosures.
- California residents received additional privacy notices.
- Consent depends on what disclosures a user saw and understood.
- Courts treat consent under ECPA and CIPA as a highly fact-specific inquiry.

The court concluded that determining consent would require individualized examinations of each user's experience and understanding.

3. Standing Deficiencies Defeated Predominance

The court found that Article III standing presented another predominance problem. In a prior ruling, one named plaintiff had standing because she showed that private information was disclosed, while another plaintiff had not demonstrated

the same privacy injury. The court reasoned that it would need to conduct that same individualized analysis for every class member:

- What data was shared?
- How was it shared?
- For what purpose?
- Did the person suffer a cognizable privacy injury?

Because plaintiffs failed to identify a class-wide methodology for proving injury and standing, the court concluded that individualized standing issues provided an additional and independent ground for denying certification.

Where Does *Ingraham* Fit in the Emerging Class Certification Landscape?

This decision is the latest in a growing line of privacy cases in which courts have declined to certify classes challenging the use of website tracking technologies. Although each case arose from different factual backgrounds, the decisions collectively highlight a recurring theme: individualized issues often overwhelm common questions in online privacy litigation.

Recent examples include:

- **May 2025**: A California federal court denied class certification in a proposed CIPA action alleging that multiple online retailers unlawfully collected website users' browsing information and used that data for targeted advertising. The court concluded that individualized issues relating to user interactions and consent prevented certification. You can read more here.
- **June 2025**: The Northern District of California denied class certification in *Calhoun v. Google LLC*, a privacy lawsuit alleging that Google collected Chrome users' browsing activity without adequate consent when users browsed in non-synced mode. The court held that individualized questions regarding users' knowledge of and consent to Google's practices predominated over common issues. You can read more here.
- **March 2026**: The Northern District of California denied class certification, holding that individualized statute-of-

limitations issues and standing deficiencies predominated over common questions in claims alleging a technology company unlawfully collected tax-filing website users' data through tracking means. You can read more here.

Impact on Businesses

The Capital One decision may provide businesses with a significant new roadmap for defeating class certification in website tracking litigation. While many companies have struggled to obtain dismissal of CIPA, ECPA, and related privacy claims at the pleading stage, this ruling highlights the substantial hurdles plaintiffs may face in certifying broad classes based on alleged website tracking practices.

5 Practical Takeaways for Businesses

Businesses should consider the following practices, which may help reduce litigation risk and strengthen defenses if litigation arises:

1. Regularly Audit Your Website Tracking Technologies

Businesses should conduct periodic audits of pixels, analytics tools, session replay technologies, APIs, and other third-party tracking tools deployed on their websites and applications. These audits should assess what information is collected, how it is transmitted, with whom it is shared, and whether those practices align with the organization's privacy disclosures, consent mechanisms, and legal obligations. It is also prudent to conduct this type of audit under the attorney-client privilege and attorney work product protections, whether through inhouse or outside counsel.

2. Closely Monitor Third-Party Vendor Implementations

Regularly evaluate how third-party vendors collect, process, and use information transmitted through tracking technologies, including updates to products, integrations, and data-sharing practices. Because vendor functionality can change over time, ongoing monitoring is critical to identify privacy risks, maintain compliance, and ensure that disclosures and consent mechanisms accurately reflect actual data flows.

3. Assessing Website Consent and Disclosure Mechanisms

Businesses should regularly review their consent flows, cookie banners, privacy notices, and other disclosure

mechanisms to ensure that users receive clear and meaningful notice regarding the collection, use, and sharing of information through tracking technologies. Particular attention should be paid to disclosures relating to third-party analytics, advertising technologies, and data-sharing practices, as well as compliance with California-specific privacy requirements.

4. Paying Attention to Sensitive Data Being Collected and Shared

Businesses should carefully evaluate whether website tracking technologies may collect, transmit, or disclose information that users reasonably expect to remain confidential. This includes personally identifiable information (PII), protected health information (PHI), financial information, application data, and other sensitive categories of data. This is particularly important for businesses in highly regulated sectors, where the collection and disclosure of sensitive data may increase both regulatory scrutiny and litigation risk.

5. Preserving Documentations for Daily Practice

Businesses should maintain and preserve records relating to privacy disclosures, consent mechanisms, vendor relationships, data-sharing practices, and tracking technology configurations. Documentation can serve as critical evidence in future litigation, particularly where businesses seek to demonstrate variations in user experiences, disclosures, consent, or data transmissions.

Conclusion

If you have questions about your online agreements or want a review of your website terms, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Team. You can also explore additional resources on our Digital Wiretapping Litigation page, including our interactive Digital Wiretapping Litigation Map. Fisher Phillips will continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox.