Federal Judge Denies CIPA Lawsuit's Class Certification: 5 Key Takeaways for Businesses

Insights
6.10.25

In a significant decision for privacy class action litigation, a federal judge in California recently denied the certification of a proposed class action involving claims under the state's invasion of privacy law. The May 29 ruling marks a noteworthy development in the ongoing legal battles under the California Invasion of Privacy Act (CIPA) over online data tracking and consumer privacy rights and provides valuable guidance for businesses facing these claims. Here is a quick summary of the decision and five key takeaways you can apply right away.

Background

The lawsuit centers on claims that AddShoppers, a marketing tech company, collects website users' online browsing data without their consent and uses it for targeted advertising for the benefit of a variety of online retailers.

- A group of plaintiffs, including Abby Lineberry and Miguel Cordero, pursued a CIPA claim against Lineshoppers and several retailers alleging that they received promotional emails based on retail products they reviewed despite never having provided their personal information.
- They alleged that AddShoppers' software constitutes a machine, instrument, contrivance or other device used to intercept and access their communications and those of other putative class members while those communications were in transit and without proper consent.
- They sought injunctive relief, non-monetary relief in which a court orders a defendant to stop specific conduct, as well as statutory damages of $5,000 per violation.

Why the Court Denied Class Certification

To be certified as a class action, a class must meet the four prerequisites outlined in Rule 23(a) of the Federal Rules of Civil Procedure: numerosity, commonality, typicality, and adequacy of representation. Judge Vince Chhabria denied class certification due to several key deficiencies:

Lack of Article III Standing

While AddShoppers tracked Lineberry and sent marketing emails, Cordero failed to show that his detailed browsing data was collected. The court found that his testimony lacked credibility and was

contradicted by records produced in discovery, leading to dismissal of his claims and removal of the retailer from the case.

Lack of Typicality and Adequacy

Both Lineberry and Cordero were found to be unfit class representatives.

- Cordero could not prove that he was tracked beyond a single website visit. Even if he were tracked, the sparse evidence and his lack of credibility created high risk that a jury could rule against him on grounds not applicable to the class.
- The court found that Lineberry was an atypical class member which made her inadequate to represent the class. The court found she relied on certain assumptions based on the evidence produced in discovery which showed her data was linked to other users. Her testimony was unpersuasive, the court concluded, and demonstrated that she could not recollect visiting the website or placing any items in her shopping cart. She also deleted key browsing history, raising concerns of spoliation and weakening her adequacy as a class representative.

Class Definition Issues

The plaintiffs narrowed the class to only website users of two retailers (instead of all Californians tracked by AddShoppers), which exacerbated the typicality problem. Even under a broader injunctive relief class, the same credibility and data preservation issues raised doubts about their adequacy and typicality of their claims.

The Court's Conclusion

The court denied class certification because neither Lineberry nor Cordero satisfied the foundational requirements of having claims that are typical of the proposed class and being an adequate representative of the proposed class, and both would face unique defenses not shared by the absent class members. These issues created a substantial risk that the jury could rule against them on individualized grounds, undermining the integrity of any class-wide adjudication.

Where Does This Fit Into the Puzzle?

This is the third key privacy class certification decision in the last six months, each providing another lesson for businesses.

- November 2024: In a first-of-its-kind decision, a California federal court granted class certification in a wiretapping claim brought against a website operator that used third-party technology to track users' activity. It signaled a willingness by courts to accept an expansion CIPA's scope to a user's interactions with a website. You can read more here.

- May 2025: Another California federal court certified a class action involving allegations that a health-tracking app improperly shared sensitive health information with third parties without user consent. You can read more here.

5 Key Takeaways for Businesses

This decision has significant implications for businesses facing privacy-related class action litigation. Here are five key takeaways:

1. Increased Scrutiny of Third-Party Tracking Practices

- Vendors that use tracking pixels to collect user data will face continued legal challenges, especially under California privacy laws like CIPA.
- Even though class certification was denied here, the court confirmed that tracking users without proper consent remains potentially actionable. Better-prepared plaintiffs may succeed in future cases.

Takeaway: Businesses using tracking tools should audit and document user consent mechanisms (e.g., cookie banners) to ensure they are clear, enforceable, and legally compliant, as well as that those mechanisms function properly as they are supposed to.

2. Liability Risks Extend to Brand Partners

- This case underscores that brands using third-party tracking services can be drawn into litigation, not just the vendors themselves.
- Businesses should ensure their websites and third-party vendors comply with state consumer privacy laws.

Takeaway: You should vet third-party vendors carefully and implement privacy-by-design principles in your websites and marketing strategies.

3. Data Minimization and Record Integrity Matter

- One major weakness in plaintiffs' case was the difficulty proving that their data had been collected or linked accurately.
- For third-party vendors, the merging of multiple user identities and weak recordkeeping undermined the defense and could hurt credibility in future cases.

Takeaway: You should make sure your vendors improve their data accuracy, user ID management, and transparency in how identities are linked, especially if those systems are later scrutinized in court.

4. Future Class Actions Could Still Succeed

- This denial of class certification was not on the merits of the privacy claims, but on the unsuitability of the named plaintiffs.
- A plaintiff with clearer evidence, stronger credibility, and preserved browsing data could succeed where this case failed.

Takeaway: The threat of class action exposure remains real, and businesses should treat this denial as a temporary reprieve, not a shield against liability.

5. Evidence Preservation Cuts Both Ways

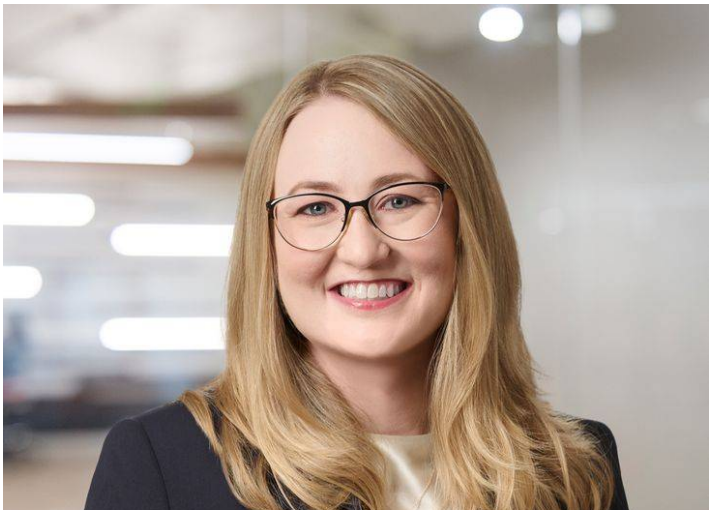
- Plaintiffs' failure to preserve key data (browsing history, cookies, device data) weakened their case.
- On the other hand, defendants must preserve their records carefully and be ready to defend how data was collected and associated with users.

Takeaway: You should implement strong robust data retention and discovery protocols. Well-kept records can support defenses against class certification and challenge class-wide claims.

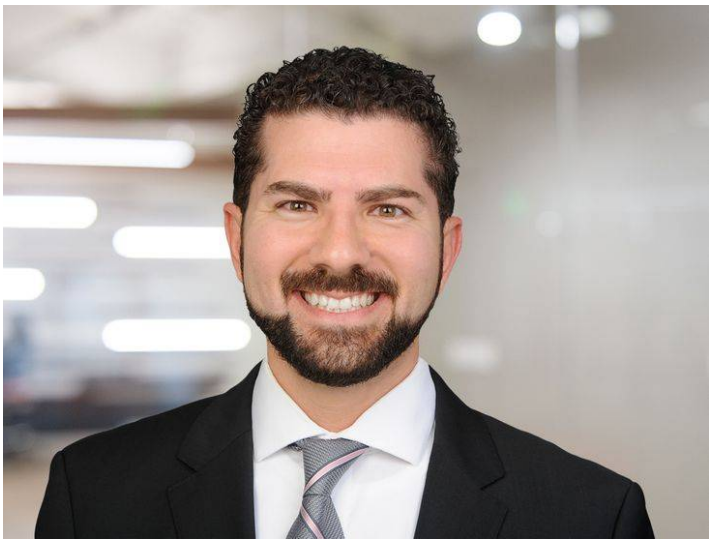
Conclusion

Fisher Phillips will continue to monitor developments in this area. We will provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You should also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate these developments. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Consumer Privacy Team.

Related People



Catherine M. Contino
Associate
610.230.6103
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

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

Service Focus

Privacy and Cyber

Litigation and Trials

Digital Wiretapping Litigation

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills