PUBLICATION

Green Light for CIPA: New Federal Court Ruling Fuels Digital Tracking Class Actions

Authors: David J. Oberly, Matthew George White
January 08, 2026

Businesses across all industries continue to face an onslaught of class action lawsuits asserting novel liability theories under the California Invasion of Privacy Act (CIPA) in connection with the use of cookies, pixels, and similar online tracking and analytics tools, making this a critical concern for any company operating a website. The most recent (and ongoing) wave of CIPA class action litigation contends that digital tracking technologies violate CIPA § 638.51's prohibition on the use of pen registers and trap and trace devices. In addition to background on CIPA and a review of relevant cases, this alert provides key next steps for companies with websites to ensure strict compliance with CIPA's statutory requirements and manage outsized legal risk and liability exposure.

In a recent decision that could reshape the CIPA litigation landscape, *Camplisson v. Adidas Am., Inc.*, 2025 WL 3228949 (S.D. Cal. Nov. 18, 2025), a California federal court rejected several recent decisions dismissing substantively identical CIPA pen register/trap and trace claims. The court held that allegations of Adidas installing tracking pixels on website visitors' browsers that recorded their personally identifiable information (PII) were sufficient, *without more*, to plausibly allege use of a pen register device and therefore to avoid dismissal at the pleading stage.

Following *Camplisson*, businesses are likely to see yet another substantial uptick in the already high volume of CIPA pre-suit demand letters and class action lawsuits, which have continued to plague website owners and operators for several years now. More than that, the decision highlights the significant uncertainty that persists with many of the core issues at the heart of CIPA disputes, while underscoring the need for companies to work proactively with privacy counsel.

Background of CIPA

Enacted in 1967 in response to concerns over eavesdropping and telephone surveillance, CIPA makes it illegal to intercept communications or aid and abet third parties in doing so. In addition, under Penal Code § 638.51 (CIPA § 638.51), CIPA prohibits the use of pen registers and trap and trace devices without a court order or user consent. The law provides for the recovery of statutory damages of $5,000 per violation, even in the absence of any actual injury or harm, as well as attorney's fees in certain instances.

Historically, pen registers and trap and trace devices were used by law enforcement while conducting telephone surveillance, with pen registers capturing the phone numbers of outgoing calls and trap and trace devices doing the same for incoming calls. CIPA defines pen register as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." The critical distinction between pen registers and other devices is that the former is designed to capture information *about* a communication, but not the *content* of the communication itself.

Camplisson v. Adidas Am., Inc.

In *Camplisson*, website visitors brought a putative class action against Adidas, alleging it violated CIPA § 638.51 through its website's use of two "tracking pixels," the TikTok Pixel and Microsoft Bing, installed on the

visitors' web browsers without their consent. According to the plaintiffs, the trackers purportedly collected IP addresses, browser information, unique identifiers, and other PII and addressing information. The plaintiffs also alleged the trackers used so-called "device fingerprinting," a process that associates information collected through the trackers with other PII to facilitate specific device activity tracking.

Adidas moved to dismiss, arguing (among other things) the trackers did not meet the statutory definition of a pen register, thus precluding the plaintiffs' CIPA § 638.51 claim as a matter of law, because:

1. The trackers only captured specific outgoing information, as opposed to all outgoing communications, from a given device; and
2. The information collected through fingerprinting was substantive, rather than mere dialing, routing, addressing, and signaling information.

The court rejected both arguments. Relying on CIPA's purportedly "intentionally broad language," it found that limiting pen registers to a process that collects all information would "take away from CIPA's purpose of protecting privacy, making it underinclusive." Additionally, according to the court, "most cases in this and other districts have also recognized that website-based trackers *can* plausibly constitute a pen register." Turning to the dispute before it, the court held the plaintiffs' allegations that the trackers recorded their PII, including the information contained in an IP address, were sufficient to plausibly allege use of a pen register and, in turn, avoid dismissal at the pleading stage.

Adidas also argued that the plaintiffs' consent barred their CIPA claims as a matter of law. The court disagreed, finding the website did not:

3. Make Adidas's online terms and conditions sufficiently conspicuous, as website visitors were required to find the details of the terms and Adidas's privacy policy by scrolling down to the footer of its site; or
4. Offer a pop-up window or similar method for visitors to affirmatively demonstrate their assent to Adidas's online terms.

Accordingly, the court held the plaintiffs were not put on notice of the terms and privacy policy outlining Adidas's use of the trackers and, thus, did not consent to the use of pen registers on their web browsers.

Analysis & Takeaways

The seminal CIPA pen register/trap and trace decisions, which opened the floodgates to the current wave of class action filings, are *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023), and *Moody v. C2 Educ. Sys., Inc.*, 742 F. Supp. 3d 1072 (C.D. Cal. 2024). In *Greenley*, the court latched onto CIPA's supposedly "expansive" and "vague" definition of pen register to reach the conclusion that software which identifies consumers, gathers data, and correlates that data through unique fingerprinting *could* constitute a pen register. Shortly thereafter, in *Moody* the court declined to "foreclose the possibility that software may qualify as a pen register or trap and trace device under California law, at least at the motion to dismiss stage."

The plaintiff's bar used these two decisions as a springboard to launch their newest campaign of class action filings for purported violations of CIPA § 638.51. In the early stages of these cases, defendants had considerable difficulty in achieving dismissals at the pleading stage. However, last year multiple courts issued defendant-favorable rulings dismissing CIPA § 638.51 class actions, including *Price v. Headspace, Inc.*, 2025 WL 1237977 (Cal. Sup. Ct. Apr. 1, 2025), *Kishnani v. Royal Caribbean Cruises Ltd.*, 2025 WL 1745726 (N.D. Cal. June 24, 2025), *Mitchener v. Talkspace Network LLC*, 2025 WL 1822801 (C.D. Cal. June 27, 2025), and *Mitchener v. CuriosityStream, Inc.*, 2025 WL 227413 (N.D. Cal. Aug. 6, 2025), all of which held the TikTok Pixel definitionally does *not* fall under the ambit of CIPA § 638.51. More importantly, these opinions called this

particular CIPA liability theory into question altogether, indicating a potential shift in the trajectory of pen register/trap and trace disputes.

That sliver of hope may be short-lived if additional courts follow the reasoning of *Camplisson*, which squarely rejected *Headspace*, *Royal Caribbean*, *Talkspace*, and *CuriosityStream*. Importantly, *Camplisson* illustrates the significant uncertainty that persists as to the precise scope and contours of CIPA pen register/trap and trace claims. Looking ahead, courts will likely continue to issue conflicting decisions on CIPA's applicability and scope, with businesses remaining subject to substantial legal risk and liability exposure tied to the use of digital tracking tools for the foreseeable future.

What to Do Now: Strategic Compliance and Risk Mitigation Measures

While the CIPA legal landscape remains in flux, it is imperative that all companies that have a website work with experienced privacy counsel to evaluate their current practices and implement risk mitigation strategies as part of their comprehensive privacy compliance programs. Doing so ensures compliance with CIPA's statutory requirements and helps manage the considerable legal risk and associated potential liability arising from the high volume of privacy- and technology-related class action filings focused on cookies, pixels, and other digital tracking tools – which will only increase as time progresses.

As an initial roadmap, companies should prioritize the following action items.

5. **Affirmative, Meaningful Consent**. Regardless of liability theory, consent has, and will continue to serve, as the strongest defense to CIPA class action claims. Accordingly, effective, dependable methods and mechanisms must be in place for securing affirmative, meaningful consent from website visitors. Clickwraps, which require visitors to take a clear, affirmative action – such as clicking a button or ticking a box – after being presented with an online agreement or privacy disclosure to signify their assent, should be used, as courts regularly uphold their validity. Consent mechanisms should be tested prior to initial deployment to confirm no cookies or similar technologies "drop" or "fire" until consent has been affirmatively manifested.

6. **Privacy Disclosures**. Privacy policies, notices, and other external-facing disclosures must clearly and conspicuously disclose all tracking technologies in use on any digital property. Disclosures should also provide detailed descriptions of all other tools that may collect, use, or share PII, such as through session replay software or the deployment of video content. Online terms and similar agreements may need to include arbitration and class action waiver provisions. All disclosures must be accurate and reflect actual data practices.

7. **Digital Audits**. Regularly assess and evaluate all digital tracking tools and how they collect and process PII. In particular, closely evaluate whether PII is shared with third parties, as this has become an increasingly significant target of plaintiffs' attorneys and privacy regulators alike. At the same time, audit all tracking tools deployed by third parties to ensure they are compliant with applicable law and contractual obligations.

8. **Vendor Agreements**. Ensure that vendor agreements where PII is implicated by way of digital tracking tools contain language: (a) requiring vendor compliance with applicable law governing the use of digital tools and PII; (b) limiting vendor data use to what is necessary for performance under the agreement; (c) barring any vendor sharing or disclosure of PII for any reason without prior express consent; and (d) requiring vendor indemnification for any claims, losses, expenses, and fees (including attorney's fees) arising from any actual *or alleged* legal noncompliance or contractual breach relating to the handling of PII.

9. **Demand Letter Response Playbooks**. Be prepared with demand letter response playbooks containing documentation that conclusively establishes legal and regulatory compliance, as well as pre-scripted negotiation strategy guidance. Where feasible, consider maintaining digital audit analyses and reports that are generated by the same tools used by plaintiffs' attorneys.

The Final Word

In today's digital world, companies with even a small digital footprint face mounting legal risks and liability exposure stemming from the extremely common (and often unknown) use of cookies, pixels, and other digital tracking tools. Implementing strategic compliance and risk mitigation measures as part of comprehensive compliance programs can directly address and mitigate the threats posed by the high volume of CIPA and similar privacy class action filings, which will only continue to increase for the foreseeable future.

As we begin 2026, now is the perfect time to consult with experienced privacy counsel, who can review and audit current compliance practices and assist in remediating any gaps to minimize the risk of being targeted with CIPA or other wiretapping class action claims. Robust, comprehensive compliance measures, such as those discussed above, can also arm companies with formidable defenses in the event they find themselves on the receiving end of a tenuous CIPA demand letter or class action complaint.

For more information or assistance, please contact David Oberly, Matt White, AIGP, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, or another member of Baker Donelson's Data Protection, Privacy and Cybersecurity, Digital Marketing, AdTech, and Consumer Privacy Compliance, or Privacy Litigation Teams.