# Thanks to CIPA Lawsuits, California May Already Be an Opt-In Jurisdiction for Web Tracking — Even Though the CCPA Says Otherwise

May 15, 2026

By: James D. Snyder, Esq.
Joshua B. Heiman, Esq., CIPP/US
**Klinedinst PC**

**Which technologies are targeted.** Session replay tools, advertising pixels, chat widgets, AI chatbots and search functionality — the standard infrastructure most businesses treat as routine.

**What to do about it.** Six concrete compliance steps — from blocking scripts, pre-consent, to locking down vendor contracts — with real-world scenarios showing how each one works in practice. We will also explain why your existing CCPA program leaves gaps that CIPA exploits.

**The dark pattern trap.** Fixing your CIPA problem incorrectly can create a new CCPA problem. Your consent banner must satisfy both laws simultaneously.

**The legislative outlook.** California lawmakers have tried to fix this — SB 690 passed the California Senate unanimously — but the bill has stalled. Do not wait for future reform.

**Why CCPA Compliance Alone Leaves You Exposed**

CCPA, as amended by the California Privacy Rights Act (CPRA), is California's primary data privacy law. It requires transparency about data collection and gives consumers the right to opt out of the sale or sharing of their personal information.[1] Critically, CCPA lets businesses collect data by default — tracking begins the moment a page loads, and consumers can opt out later. This is the model most companies have built their compliance programs around.

*Consider a concrete example.* An online pet pharmacy like 1800PetMeds.com embeds the Meta Pixel and tools from companies like Attentive and Zeta in its website code. Under CCPA, this is lawful — the pharmacy can collect browsing history, cart additions and search queries for specific medications as long as it provides a "Do Not Sell or Share" link, explains to consumers their rights under CCPA and honors opt-out requests. Affirmative consent is *not* required. Most businesses would assume this is enough. It is not.

The problem is that a second California privacy law — CIPA — imposes a fundamentally different standard. A wave of lawsuits now use CIPA to attack common tracking technologies, often ones your IT team deployed without legal review. And the financial stakes are severe: **$5,000 per violation**, with each website visit potentially counting as a separate violation.

Courts are deeply divided on whether CIPA even applies to websites — which means your exposure depends in significant part on which court hears the case. In a single ten-day span in April 2026, four judges reached opposite conclusions on nearly identical claims: one allowed a class action against CNN to proceed; another dismissed a matching case against USA Today; and two Los Angeles judges issued conflicting rulings against the same defendant.[2] Until appellate courts, or the California legislature, resolve this uncertainty, every business with California web traffic operates in a legal gray zone.

**What Is CIPA and Why Does it Apply to Your Website**

CIPA was enacted in 1967 to prevent telephone wiretapping. Its core rule is simple: in California you cannot intercept or record a communication ***without the consent of all parties***.[3] Violators face criminal penalties and — more relevant for businesses — a private right to sue, where anyone whose communications are intercepted can recover **$5,000 per violation** or three times their actual damages, whichever is greater.[4] For decades, this law applied mainly to phone calls. The "***this call may be recorded"*** announcement you hear on customer service lines exists because of CIPA.

Around 2020, plaintiffs' attorneys recognized that CIPA's broad language could potentially reach modern website technologies. Their core argument is as follows: when a visitor types a search query, enters a chat message or browses your site while tracking scripts are running, that activity is a "communication." If a third-party tool — a session replay service, analytics pixel or chat widget — captures that communication in real time, without prior consent, it is an illegal wiretap under CIPA.

CIPA litigation—not the statute itself—has effectively pushed California toward a functional opt-in regime in this context.[2][3]

Not all courts have accepted this theory, but enough have to create serious litigation risks. In one of the first major rulings, a federal court held that session replay software on Lululemon's website — which captured keystrokes, clicks, browsing history, shipping information and IP addresses — could constitute third-party eavesdropping or interception under CIPA.[5]

The facts mirror what happens on most commercial websites. Lululemon had embedded session replay software from Quantum Metric — marketed as letting companies "watch [a user's] journey as if [the company] was standing over their shoulder" — that captured keystrokes, clicks, pages viewed, shipping and billing information, and IP addresses, which then transmitted everything to Quantum Metric's servers. Lululemon's privacy policy disclosed this, but in 7.5-point, non-contrasting font, buried at the bottom of the page. Further, no one asked the plaintiff, visiting Lululemon's website, to agree. The court allowed the CIPA claim to proceed.

CIPA litigation accelerated sharply in 2022, when the Ninth Circuit ruled, in an unpublished memorandum, that CIPA claims against website operators could proceed.[6] The decision is not binding precedent, but rather an unpublished disposition, citable only under Ninth Circuit Rule 36-3, but it opened the floodgates. Subsequent courts have confirmed, in varying degrees, that session replay technology, analytics pixels and similar tools can constitute illegal "interceptions" under CIPA — and have increasingly focused on whether users provided clear, advance consent ***before*** any interception occurs. Since that ruling, plaintiffs' firms have aggressively and systematically targeted thousands of businesses across every industry.

**The Financial Exposure: Why CIPA Claims Are So Dangerous**

CIPA claims are much more dangerous than CCPA violations to your business. Under CCPA, consumers generally ***cannot sue*** you for tracking violations — only for ***data breaches,*** caused by inadequate security practices.[7] For ordinary tracking issues, enforcement falls to regulators, who may impose fines of up to $2,500 per violation (or $7,500 for intentional violations).[8] That is manageable. CIPA is not. CIPA gives ***every affected consumer*** the right to sue your business directly — no regulator needed — and recover **$5,000 per violation** or three times actual damages.[4] Each website visit arguably can be a separate violation. In a class action, the numbers compound to existential levels.

This gap has proven especially significant in healthcare. In *Maghoney v. Dotdash Meredith Inc.*, a plaintiff alleged that VeryWellHealth.com's advertising platform intercepted his searches for information about sexually transmitted infections — but the court dismissed the suit, finding the plaintiff failed to plausibly allege a concrete privacy injury.[10] By contrast, in *Cobbs v. Petmed Express, Inc.* — a federal court applying California law — the court allowed CIPA claims to proceed where plaintiffs alleged the Meta Pixel captured veterinary prescription searches and routed that data to Meta for targeted advertising.[11] Even within the same subject matter, outcomes are unpredictable.

The scale of litigation is staggering. According to Fisher Phillips' Digital Wiretapping Litigation Map, more than **4,300 CIPA-related lawsuits** have been publicly filed since 2022, roughly 75% in California.[12] Thousands more demand letters and arbitration claims remain outside the public record. Many follow a template: plaintiffs' firms identify targets based on visible tracking scripts, send demand letters and file near-identical complaints across hundreds of defendants.

The practical effect is that CIPA has become, in the view of many practitioners, a de facto web privacy enforcement mechanism in California — one that may impose stricter requirements than CCPA itself; namely an "Opt-In" consent requirement.

## The Core Problem: When Consent Is Required

Everything comes down to ***timing*** and the legal standard courts use to decide whether your website visitors actually agreed. Under CCPA, tracking begins by default; consumers are tracked until they opt out. Under CIPA, ***liability turns on whether valid consent was obtained before any interception occurs***. The Ninth Circuit's consent test comes from *Berman v. Freedom Financial Network, LLC*: a user "manifests assent" only when she "intend[s] the conduct and know[s], or ha[s] reason to know, the other party may infer [her] assent from the conduct."[13] In plain terms, passive browsing (such as scrolling or continued use) is generally not enough — the visitor must take a deliberate action (a click, a checkbox) while understanding that the action signals agreement to tracking. If your analytics pixel, session replay tool, or chat widget activates ***before*** the user takes that deliberate step, courts may find that consent was not obtained before an alleged interception, creating CIPA risk — even if your CCPA compliance is flawless.[11] This means a fully CCPA-compliant website can still face massive CIPA liability if its tracking technologies load before the user consents — or if no consent mechanism exists at all.

Two recent cases show how this plays out. Six Flags' website offered a "Deny Non-Essential" cookies button — but even after users clicked it, third-party cookies allegedly continued tracking their browsing. The court allowed the CIPA claim to proceed.[14] Further, Motorola's website had a "Reject All non-essential cookies" option that, according to the plaintiff, simply did not work — scripts from Google, TikTok and Amazon kept firing. The court refused to dismiss, calling Motorola's defense an "inherently factual contention" it could not resolve at the motion to dismiss stage.[15] The takeaway: if your consent controls do not actually stop tracking when a user says no, you could have a CIPA problem.

## Which Technologies Put You at Risk

CIPA litigation has targeted the tracking technologies most businesses treat as standard infrastructure:

**Session replay tools** (Hotjar, FullStory, LogRocket) record keystrokes, mouse movements, and page interactions. In some cases, courts have treated these as real-time interception of communications. In the Lululemon case, the court said session replay software was "more akin to 'an eavesdropper standing outside the door'" than a passive recording device.[16]

**Live chat and AI support widgets** transmit user messages to third-party platforms. The legal risk depends on what your vendor does with the data. When the vendor acts purely as your tool — processing data only on your behalf — courts have generally dismissed CIPA claims.[17] But when the vendor retains data for its own purposes — for example, training AI models, building audience profiles — courts have allowed claims to proceed.[18] The difference turns on your vendor contract.

AI chatbots present a growing frontier of risk. As more companies deploy AI-powered chatbots for customer service, applicant screening, and HR queries, the question of whether user inputs qualify as protected communications under CIPA is increasingly being litigated. Legal

commentators have argued that chatbot inputs — particularly those involving health, financial, or employment information — likely qualify as substantive communications under CIPA's broad statutory language, not mere technical data, and courts have begun analyzing analogous forms of digital communication under similar theories.[19] No appellate court has squarely addressed the issue, but if your business has deployed an AI chatbot, this is an emerging risk area your business should evaluate.

**Advertising and analytics pixels** (Meta Pixel, TikTok Pixel, Google Analytics) — small pieces of code embedded on web pages — capture user behavior and transmit it to third-party servers. At least one court found that CIPA's statutory language was broad enough to plausibly encompass such tracking software.[20] If your marketing team uses any major advertising pixel, your business is potentially within CIPA's reach.

**Search functionality** that transmits user queries to third parties via tracking pixels has become a particular litigation target. When a visitor types a search term on your website and that query is simultaneously sent to an advertising platform, plaintiffs allege this constitutes interception of a private communication. At least one federal court found such allegations sufficient to proceed past the pleading stage.[21]

The online pharmacy cases illustrate the worst-case scenario. In *Cobbs v. Petmed Express* — a Florida federal court applying California law — plaintiffs alleged the Meta Pixel tracked specific medications customers searched for and sent that data to Meta's servers, where it was paired with Facebook profiles for targeted advertising.[11] The court found that the pharmacy's generic privacy policy was not enough to establish consent at the pleading stage. If your website handles sensitive information — health data, financial queries, personal searches — the litigation risk is especially acute.

**Why Your CCPA Compliance Program Will Not Protect You**

Many businesses assume that a well-run CCPA compliance program protects them from data privacy litigation. It does not — at least not from CIPA claims. CCPA's disclosure requirements (privacy policies and "Do Not Sell or Share" links) are necessary but insufficient for CIPA purposes. A privacy policy buried in a footer link, without a mechanism requiring the user to affirmatively agree, before tracking begins, very likely does not establish the consent under CIPA. Several courts have rejected the argument that simply visiting a website implies consent to tracking.[22] If you do business in California, you should evaluate whether a CIPA-specific compliance strategy — not just a CCPA checkbox — is warranted.

*Gianne v. Accor Management US Inc.* (the Fairmont Hotels case) illustrates the problem. The hotel chain displayed a cookie banner stating: "By continuing your browsing, you are agreeing to the use of cookies," with a gray overlay dimming the page. But a plaintiff alleged she bypassed the banner by simply scrolling down — reaching the reservation page without interacting with it. The court found the overlay provided reasonably conspicuous notice but nevertheless allowed the CIPA claim to proceed, concluding that issues regarding user assent could not be resolved at the pleading stage.[23]

Even a relatively robust cookie banner may still fail if users can bypass it.

**What Your Business Should Do Now**

Given the current litigation landscape, many privacy practitioners recommend treating California as a de facto **opt-in** jurisdiction for website tracking — regardless of what CCPA requires. Here are the specific steps your business should evaluate:

**Block All Tracking Until Users Consent**

Configure your consent management platform such that no analytics pixels, session replay tools, advertising trackers or chat widgets fire until the user affirmatively clicks "Accept." Loading scripts before the consent banner renders — or allowing them to continue after the user declines — creates CIPA exposure.

*Mini-scenario:* A bakery chain launches an online ordering site with Meta Pixel and Google Analytics firing the instant a browser loads the homepage — before the cookie banner appears. A potential consumer visits the site, confirms pre-consent script loading using browser developer tools and files a CIPA complaint. The bakery faces potential $5,000-per-visit exposure for every California visitor who arrived before clicking "Accept." Had the consent platform held all scripts until consent was received, the claim likely would not have been viable.

*Mini-scenario:* After receiving a demand letter, the bakery adds a "Reject All" button, but fails to update the tag manager. Scripts keep firing after visitors click "Reject." This is exactly what allegedly happened to Motorola, as described above. The lesson is straightforward: test your consent mechanism regularly with an independent auditor.

**Do Not Rely on Browsewrap Terms**

"Browsewrap" refers to terms stating something like "by continuing to browse, you agree to our terms." Courts have generally declined to enforce these absent clear and conspicuous notice and unambiguous user assent. As explained above, the *Berman* standard requires a deliberate action coupled with awareness that the action signals agreement — and passive browsing satisfies neither element.[13] You need an affirmative action — a click, a checkbox or a similar mechanism — that clearly demonstrates the user has agreed. In the Lululemon case, the court found that a privacy policy accessible only via a hyperlink in 7.5-point, non-contrasting font was "insufficient to give rise to constructive notice" — even when the hyperlink was in "close proximity . . . to relevant buttons users must click on."

*Mini-scenario:* A similar issue arose in the Fairmont Hotels case described above. The hotel's cookie banner included a gray overlay, but a guest bypassed it by scrolling. The court allowed the CIPA claim to proceed despite finding the notice was "reasonably conspicuous." If users can reach your content without clicking a consent button, browsewrap is unlikely to provide a reliable defense.

**Ensure That Your Privacy Policy Matches What Your Site Actually Does**

Conduct a technical audit of every tracking tool on your site. Your privacy policy must accurately list each vendor and describe the data it collects. Generic disclosures about "tracking tools" and "third parties" are unlikely to establish meaningful user consent where the actual data collection is far more specific.

*Mini-scenario:* An online pharmacy's privacy policy says it uses "tracking tools including cookies" and shares information "with third parties." In reality, the Meta Pixel captures specific prescription medications customers search for and transmits that data to Meta for targeted advertising. When sued, the pharmacy points to its privacy policy. The court disagrees, finding that generic language about "tracking tools" did not clearly disclose the sharing of sensitive prescription data with advertising platforms. Similar allegations have been raised in cases involving PetMed Express and HealthWarehouse.com. The fix: name each vendor and describe the data each collects.

**Lock Down Your Vendor Contracts**

If your chat widget, session replay tool or analytics provider retains independent rights to user data — for model training, audience building or advertising — the "third-party interception" theory gains significantly more traction against your business. Negotiate contractual limitations on vendor data use and specify that each tool operates purely as your agent.

The distinction matters. In *Graham v. Noom,* a court found the chat provider was merely a tool — "like the tape recorder" — processing data only on the defendant's behalf and dismissed the CIPA claim.[17] In *Saleh v. Nike*, the opposite result occurred: where the monitoring company was alleged to retain and use data independently, the court treated it as a potential third-party eavesdropper and allowed the claim to proceed.[18]The difference turns on whether the vendor operated as the website's agent or exercised independent control over the data.

*Mini-scenario:* A fitness app uses a chat widget whose contract allows the vendor to retain conversation data and use it to "improve its services" — including training AI models. A plaintiff sues, and the court applies reasoning similar to *Saleh*: independent commercial use of the data may support treating the vendor as a third-party eavesdropper rather than a passive tool.[18] Had the contract prohibited the vendor from retaining data beyond the contracted service, the *Graham* "tape recorder" defense would have been more likely to apply.[17]

**Have Proof Users Consented**

Even if you cannot prove a specific plaintiff consented, evidence of consistent consent practices can make or break your defense. Retain timestamped records of when users granted or denied consent and which version of your consent notice they saw.

*Mini-scenario:* A SaaS company is sued by a visitor from six months ago. The consent banner worked at the time, but the company kept no records. The plaintiff claims she never consented and

the company has no evidence to refute her claim. Compare *Lakes v. Ubisoft*, where the court dismissed all claims with prejudice — and denied leave to amend as futile — after finding that the defendant implemented and documented a layered consent flow, including a cookie banner, account-creation checkbox, and repeated presentation of its privacy policy.[24] That case is currently on appeal to the Ninth Circuit (No. 25-2857). The lesson: retain timestamped logs of consent interactions.

**Consider Different Consent Flows for California Visitors**

CIPA's stricter requirements are most directly relevant to California visitors, though the statute's precise jurisdictional reach remains subject to debate. Some businesses implement geo-targeting to present an opt-in banner to California users while maintaining simpler opt-out practices elsewhere. This approach is designed to limit the operational impact while addressing the highest-risk jurisdiction.

*Mini-scenario:* A national retailer, after its third CIPA demand letter in a month, implements geo-targeting: California visitors see an opt-in banner blocking all scripts until they click "Accept;" other visitors see a standard CCPA opt-out link. The geo-targeting costs roughly $15,000 — a fraction of the potential $50,000+ cost of defending a single demand letter.

*Mini-scenario:* Alternatively, a healthcare information website deploys the European Union's GDPR-style opt-in consent globally, eliminating jurisdictional complexity at the cost of a roughly 30% reduction in analytics data. The company determines that reduced litigation risk outweighs the marketing loss.

**The Legislative Outlook: Will the Rules Change?**

California lawmakers have recognized this problem. Senate Bill 690 (SB 690), introduced in 2025, would exempt businesses from CIPA liability for tracking technologies already regulated under CCPA and subject to consumer opt-out rights. The bill passed the California Senate unanimously, before stalling in the Assembly.

If enacted, it would allow CCPA-compliant opt-out mechanisms to satisfy certain CIPA requirements for standard business tracking — potentially providing significant relief to businesses caught between the two laws' conflicting demands.

Since it has lost momentum in the Assembly, do not count on it. SB 690 stalled amid concerns that its exemptions were too broad. It is unlikely to take effect before 2027, and even if passed, it will not apply retroactively. The Reform CIPA Coalition launched in April 2026 to push for the bill's revival, but the timeline remains uncertain.[25]

The strategic implication is straightforward: do not build your compliance strategy around the assumption that legislative reform will arrive in time to help. Plan for the rules as they exist today.

**The Dark Pattern Trap: How Fixing One Problem Can Create Another**

There is an additional risk your business must understand: dark patterns. These are interface designs that manipulate users into unintended choices — a large, colorful "Accept" button next to a tiny "Decline" link, or confusing double negatives. California's Privacy Protection Agency (CPPA) issued regulations and enforcement guidance addressing and restricting these designs.

Here is the trap: consent obtained for CIPA purposes can create dark pattern liability under CCPA if poorly implemented. A banner that makes "Accept" prominent while hiding "Decline" might satisfy CIPA's consent requirement, while potentially violating CCPA's restrictions on dark patterns — exposing your business to regulatory enforcement, including civil penalties of up to $7,500 per violation. The Motorola case is instructive: the company's "Reject All" button allegedly did nothing, and the court refused to dismiss the fraud claim, noting the banner's promises were "outright lies, designed to lull users into a false sense of security." Your consent mechanism must actually work as advertised.

The design requirement is clear: your consent flow must obtain prior, affirmative consent (for CIPA) while maintaining symmetry of choice and avoiding manipulative design (for CCPA). Both laws must be satisfied simultaneously.

*Mini-scenario:* A travel site redesigns its consent banner with a large green "Accept All" button and a small gray "Reject" text link. The banner solves CIPA — but may trigger a CCPA enforcement action alleging the asymmetric design constitutes a dark pattern. The company faces potential civil penalties of up to $7,500 per violation.

*Mini-scenario:* The fix: equally sized "Accept" and "Decline" buttons, side by side, same font and color weight. "Decline" blocks all non-essential scripts immediately; "Accept" triggers scripts only after the click registers. The modest drop in acceptance rates is more than offset by eliminating the dual-front litigation risk.

**What You Should Take Away**

Here is the core of what this article has covered:

**CCPA compliance is necessary but not sufficient.** CCPA's opt-out framework does not address CIPA's requirement for prior, affirmative consent. If your compliance strategy stops at "Do Not Sell or Share" links and privacy policies, you likely have a gap.

**CIPA is being applied to websites.** Courts have extended — or are being asked to extend — this 1967 wiretapping statute to session replay tools, analytics pixels, chat widgets and AI chatbots — the standard tracking infrastructure most businesses deploy without a second thought. Not all courts agree and the question remains unsettled at the appellate level.

**The financial stakes are severe.** At $5,000 per violation, with each visit potentially counting separately, a mid-sized e-commerce website with 100,000 monthly California visitors faces theoretical exposure approaching **$500 million** *per month*. Even at a fraction of that figure, the settlement pressure is immense.

**Consent timing is critical.** If your tracking scripts fire before a user clicks "Accept" — or if your "Reject All" button does not actually stop them — you are exposed regardless of what your privacy policy says.

**No industry is immune.** CIPA claims have hit athletic apparel, theme parks, pharmacies, hotels, technology companies, news outlets, retailers and even nonprofit healthcare providers. If your organization operates a website with tracking technologies accessible to California consumers, you are a realistic potential target — regardless of your business' industry or size.

**Legislative relief is not imminent.** SB 690 passed the California Senate unanimously but has stalled. It is unlikely to take effect before 2027 and would not apply retroactively. Do not build your compliance strategy around the assumption of reform.

**Your consent banner must satisfy two California laws at once.** A banner designed to obtain CIPA consent can create dark pattern liability under CCPA if the design is asymmetric or manipulative. Both "Accept" and "Decline" options must be equally prominent.

Your business' solution is straightforward:

- Implement opt-in consent mechanisms that block tracking until website users affirmatively agree,
- Ensure consent is obtained before any third-party scripts fire,
- Align privacy disclosures with actual technical website practices,
- Document consent decisions with timestamped logs, and
- Ensure vendor contracts limit independent third-party data rights.

Investing in proper consent infrastructure is not a legal nicety — it is a cost-of-doing-business decision. Businesses should act now rather than wish they had.

---

**About Klinedinst PC and the Authors:**

**Klinedinst PC** is a full-service law firm serving businesses, insurers, and individuals across California and the western United States. The firm's Data Privacy and Artificial Intelligence Practice Groups advise clients on AI governance, regulatory compliance, technology transactions, data privacy, intellectual property, and risk management strategies related to emerging technologies.

**James D. Snyder** is the Managing Shareholder of Klinedinst PC's San Diego office and Co-Chair of the firm's Data Privacy and Artificial Intelligence Practice Groups. **Joshua B. Heiman,** CIPP/US, is Co-Chair of the Klinedinst Data Privacy and Artificial Intelligence Practice Groups.

---

your specific circumstances. Privacy law is rapidly evolving, and the application of CIPA to digital technologies in California remains unsettled in many respects. Businesses should consult with legal counsel in California before making compliance decisions based on the information presented in this article.

---

**Notes**

[1] Cal. Civ. Code § 1798.100 et seq.; Cal. Civ. Code § 1798.120(a).

[2] *See*, e.g., *Heiting v. Taro Pharms. USA, Inc.*, 728 F. Supp. 3d 1112 (C.D. Cal. 2024); *In re USA Today Co. Internet Tracking Litigation*, No. 24-cv-5150 (N.D. Cal. Apr. 6, 2026); *D'Antonio v. Cable News Network, Inc.*, No. 1:24-cv-03132 (S.D.N.Y.).

[3] Cal. Penal Code § 631(a).

[4] Cal. Penal Code § 637.2(a).

[5] *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081–83 (C.D. Cal. 2021).

[6] *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022) (mem.).

[7] Cal. Civ. Code § 1798.150(a).

[8] Cal. Civ. Code § 1798.155(a).

[9] [Reserved].

[10] *Maghoney v. Dotdash Meredith, Inc.*, No. 3:24-cv-02394-AJB-BJW, 2026 WL 497402 (S.D. Cal. Feb. 23, 2026).

[11] *Cobbs v. Petmed Express, Inc.*, 2026 U.S. Dist. LEXIS 74228 (S.D. Fla. 2026) (applying California law).

[12] *See,* Fisher Phillips, *Digital Wiretapping Litigation Map*, https://www.fisherphillips.com/en/resources-and-innovation/trackers-and-maps/wiretapping-litigation-map (last visited Apr. 2026).

[13] *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 856–57 (9th Cir. 2022); *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1175–76 (9th Cir. 2014).

[14] *Casillas v. Six Flags Ent. Corp.*, No. 2:25-cv-06824-CBM-PD (C.D. Cal. 2025).

[15] *Gabrielli v. Motorola Mobility LLC*, No. 4:24-cv-09533-JST (N.D. Cal. 2024).

[16] *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082 (C.D. Cal. 2021).

[17] *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021).

[18] *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503 (C.D. Cal. 2021); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022) (mem.).

[19] *See*, e.g., Byars v. Goodyear Tire & Rubber Co., 654 F. Supp. 3d 1020 (C.D. Cal. 2023); *In re Meta Pixel Healthcare Litig.*, No. 3:22-cv-03580-WHO (N.D. Cal.); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022) (mem.).

[20] *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1037–39 (S.D. Cal. 2023).

[21] *Rodriguez v. Autotrader.com, Inc.*, 762 F. Supp. 3d 921 (C.D. Cal. 2025).

[22] *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1083 (C.D. Cal. 2021); *Cobbs v. Petmed Express, Inc.*, 2026 U.S. Dist. LEXIS 74228 (S.D. Fla. 2026).

[23] *Gianne v. Accor Mgmt. US Inc.*, No. 2:25-cv-02425 (C.D. Cal. 2025).

[24] *Lakes v. Ubisoft, Inc.*, No. 24-cv-06943-TLT, 2025 WL 1036639 (N.D. Cal. Apr. 2, 2025).

[25] *See,* Reform CIPA Coalition, https://reformcipa.com/.