Shumaker

DECEMBER 12, 2025 | PUBLICATION

"The California Invasion of Privacy Act Meets the Modern Web: What Businesses Need to Know Now"

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Brian C. Focht

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

When California enacted the California Invasion of Privacy Act ("CIPA") in 1967, lawmakers were concerned about physical wiretaps and hidden listening devices, not pixels, chatbots, or on-site search bars.

Fast-forward to 2025, and CIPA has become one of the most litigated statutes in the digital privacy space. Plaintiffs' firms use its statutory damages (up to $5,000 per violation) to challenge common website practices, from analytics tags and session replay scripts to third-party chat and built-in search tools that quietly send user inputs to vendors.

(Reuters)

This article explains how we got here, the stalled legislative effort to reduce CIPA website lawsuits, and provides a few practical steps businesses can take now to lower their risk.

From Wiretapping Statute to Web-Tracking Weapon

CIPA was enacted "to protect the right of privacy" of Californians from "eavesdropping upon private communications" and related forms of wiretapping. It prohibits, among other things intercepting or recording certain "confidential communications" without consent (e.g., §§ 632, 632.7) and installing or using a "pen register" or "trap and trace" device without a court order or consent (e.g., §§ 638.50–638.51).

- (California Lawyers Association)

CIPA is unusual because it combines criminal provisions with a civil private right of action that awards statutory damages of up to $5,000 per violation. California's more modern consumer privacy laws, the CCPA and CPRA, provide consumers with only a limited private right of action for specific data breaches. For most alleged tracking and disclosure violations, enforcement is left to regulators. This "enforcement gap" has prompted plaintiffs' lawyers to use CIPA as a de facto web privacy law for online tracking, including cookies,

pixels, and similar tools.

How Website CIPA Litigation Got Here (Last 4–5 Years)

Although CIPA has existed for decades, its use against websites is new. The cases being filed and threatened are routinely called frivolous; initiated by opportunists and unethical attorneys.

Such outcry overlooks how we got here.

Leading up to the enactment of the CCPA and CPRA, the internet as we knew it was engaged in a fierce battle between advertisers and consumers. As the internet became more integral, shifting from a computer-based encyclopedia to a ubiquitous, always-listening repository of information, consumers' ability to protect their personal data has nearly vanished. GDPR in Europe and CCPA in California offered a glimmer of hope for reclaiming some privacy. However, as mentioned above, they fall short for many.

CIPA, enacted initially to address increasing capabilities of non-governmental entities to intercept our phone calls, included the necessary remedy: statutory damages. Later-in-time updates added cellular phones, wireless communication, and all-party consent to CIPA's regime.

Still, how did we get from the privacy of cell phone calls to the uses of a website's search bar?.

1. Early cases: chat and call recording

Before the current web-tracking focus, CIPA lawsuits focused primarily on call-center recording (i.e., "this call may be recorded" scenarios) and certain forms of electronic messaging and chats without appropriate disclosures. *See Montemayor v. GC Servs. LP*, 302 F.R.D. 581, 583 (S.D. Cal. 2014) *and Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014).

Those claims laid the groundwork for arguing that web-based communications (not just phone calls) could be "intercepted" or "recorded" under CIPA. The floodgates opened, however, following *Gruber v. Yelp,* 55 Cal. App. 5th 591, 269 Cal. Rptr. 3d 790 (2020), *as modified on denial of reh'g* (Oct. 23, 2020) *and In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020),

2. Chatbots and Session Replay

By 2021, businesses were facing an onslaught of CIPA demands alleging that website chat features and session replay software constituted illegal wiretaps. Plaintiffs' claims advanced two related theories:

- **"Chat box" theory** – Since many websites depend on third-party vendors to provide chat features (including "virtual assistants"), plaintiffs argued that the vendor is a separate, non-consenting "eavesdropper," improperly "listening in" on chats between the user and the website. *See, e.g., Martin v. Sephora USA, Inc.,* No. 1:22-CV-01355-JLT-SAB, 2023 WL 2717636 (E.D. Cal. Mar. 30, 2023), *report and recommendation adopted,* No. 122CV01355JLTSAB, 2023 WL 3061957 (E.D. Cal. Apr. 24, 2023).
- **Session replay and analytics theory** – Session replay tools record mouse movements, keystrokes, scrolls, and page views. Plaintiffs argue that this is the digital equivalent of wiring a line and recording a conversation, especially when a third-party vendor has access to that data. *See, e.g., Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073 (C.D. Cal. 2021)

The Ninth Circuit's 2022 decision in Javier v. Assurance IQ, No. 4:20-cv-02860-JSW, 2022 WL 1744107 (9th Cir. May 31, 2022) supercharged these theories. *Javier* ruled that consent for session-replay recording must be

obtained before tracking begins. Retroactive or implicit consent is not enough.

3. 2023–2025: Pixels, Cookies, and "Pen Registers"

Since 2023, plaintiffs have broadened their theories to encompass essentially the full stack of website tracking and communications tools, including chatbots and virtual agents (live or automated), session replay and keystroke logging tools, marketing pixels (e.g., Meta Pixel), conversion tags, and cross-site advertising IDs, and first-party and third-party cookies and other identifiers. A second area of litigation targets these tools as illegal "pen registers" or "trap and trace" devices under the later-added provisions of CIPA.

CIPA is now described as "one of the most litigated statutes in the digital age," with claims increasingly targeting Google Analytics and similar tools for "intercepting" user communications. Based on limited anecdotal reports from attorneys in this area, thousands of claims – in the form of lawsuits, arbitration demands, and pre-suit settlement demands are being sent to U.S. businesses every month. Even if you're not located in California (or even actively pursuing business there), if you have a website, you're a potential target.

So what are these plaintiffs looking for?

Current CIPA Claims

Plaintiffs rely on several recurring theories to support their claims under CIPA. The fact patterns tend to look familiar:

1. Inadequate or misleading privacy notices

These claims are usually based on one of three things:

- The website does not disclose the use of specific tracking or recording tools at all;
- The privacy notice or cookie policy describes a narrower set of practices than what actually occurs; or
- The business markets itself as privacy-focused, while secretly using tools that share detailed behavioral data with different vendors.

These discrepancies are used to argue that there is no informed consent for the interception or recording involved, and that any "assent" to boilerplate terms is just an illusion.

2. "Leaky" cookie banners and broken consent flows

Another common pattern involves the now-ubiquitous cookie banner. In these cases, a cookie banner appears, often with an "Accept All" and a "More Options" or "Decline" button. However, some of the very cookies that this banner addresses (e.g., analytics, pixels, replay) fire before consent or continue firing even after the user rejects them.

Plaintiffs in these cases argue that there was never valid, prior consent to interception or pen-register-type tracking and that the banner itself is misleading because it suggests that declining will stop the tracking, when in practice, it does not.

3. Chat, contact forms, and built-in search bars

Beyond cookies and pixels, plaintiffs are increasingly focusing on user-initiated communications on the site, including live and AI-powered chats, contact or intake forms, and on-site search bars that accept free-text

queries.

The core theory is that these are communications between the user and the website owner, in which the user has an expectation that they have an expectation of privacy. When a third-party vendor (such as analytics, search, or marketing platforms) receives the contents of these communications in real time, plaintiffs allege that the website owner has aided or assisted a third party in obtaining these communications in violation of CIPA.

Importantly for built-in search boxes, the nature and content of the information being shared has the potential to be personal and sensitive. Users may type names, addresses, account numbers, medical terms, or other personal data in order to get specific information from the website that is pertinent to their personal situation. Many search implementations send the full query string, together with identifiers, to vendor platforms for indexing, search-optimization, or logging. In fact, for the most popular website development platform on the internet – WordPress – connecting to third party analytics might be the only way for a website owner to know what searches its visitors have performed.

Plaintiffs allege that such search functions collect "signaling" or routing information (e.g., IP address, device ID, referrer, geolocation) plus the typed terms and share the data with third-party providers. Importantly, the search bar almost always operates exclusive of any cookie preferences or website privacy tools, and will not block such use.

4. Where We Stand… Legally Speaking

Federal courts in California have issued conflicting decisions on CIPA web-tracking claims. Some decisions (e.g., *Byars v. Goodyear Tire & Rubber Co.*) have read CIPA broadly to cover certain smartphone web chats, and have allowed CIPA claims to proceed against websites using third-party chat tools. Others (e.g., *Byars v. Hot Topic*, *Valenzuela v. Keurig*) have held that certain CIPA claims are limited to telephonic wiretapping or that other claims do not apply to internet communications. There is also an open question as to whether a website user who does not *actually* believe that information will be kept private – and thus does not have an *expectation of privacy* – suffers any injury to allow standing. *See Khamooshi v. Politico LLC*, 786 F. Supp. 3d (N.D. Cal.).

This split creates uncertainty, but it also means success isn't guaranteed for either plaintiffs or defendants. Plaintiffs can often plead around adverse decisions by emphasizing factual differences, vendor behavior, or smartphone use.

SB 690: The Reform That Didn't Happen… Yet

In 2025, California lawmakers made a determined attempt to limit CIPA's application to typical online tracking—but stopped short of enacting reform.

Senate Bill 690, introduced by Senator Anna Caballero, sought to limit "abusive lawsuits" under CIPA related to standard online business tools such as cookies, pixels, chatbots, session replay, and similar technologies.

The goal was to shield businesses from CIPA liability when they use web trackers in ways already addressed under CCPA/CPRA, while preserving CIPA's application for truly abusive or covert interception.

SB 690 passed the California Senate unanimously, although without any retroactive effect. In the Assembly, however, the bill stalled. By the end of the 2025 legislative session, SB 690 had been passed as a two-year bill, effectively delaying it until at least the 2026 session.

The practical takeaway is that there is no statutory safe harbor yet. Until SB 690 (or something similar) passes, businesses should assume that current CIPA interpretations continue to apply to their websites.

What Businesses Can Do Now to Limit Risk

Fortunately, there are specific that businesses can take *today* to reduce CIPA exposure.

1. Know and understand the tracking tools you use

Start with a technical audit:

- Identify all cookies, pixels, tags, scripts, chat tools, session-replay utilities, and search-related integrations on your site(s).
- Determine what data each tool collects, where it sends that data, and whether third-party vendors can use it for their own purposes (e.g., ad targeting, model training).

Where possible, disable scripts that are not clearly necessary and replace general-purpose marketing tools with configurable, privacy-aware versions (e.g., consent modes, IP anonymization, server-side tags). As much as you might love your website analytics tools, determine whether you truly need session replay or full keystroke logging, especially on pages where users may enter sensitive data.

2. Get actual, meaningful consent

From a CIPA perspective, timing and clarity of consent are critical. Make sure that your non-essential tracking doesn't trigger before consent. This applies to cookies, pixels, analytics, replay, or third-party search logging.

Use banners or consent management platforms that require an explicit action (e.g., "Accept," "Reject All," "Customize") and offer meaningful, specific choices (e.g., strictly necessary vs analytics vs advertising). Critically, you need to reflect the user's choices immediately in what scripts actually run.

Avoid browsewrap terms of use that rely on "By continuing to browse, you agree…" language and tools or flows that still allow third-party tools to collect user data regardless what the user selects on the cookie notice. (This one is where the search bar issue is most significant!)

Document your consent logic and retain logs where possible. Even if you can't prove that a plaintiff provided specific consent, evidence of practice can be critical evidence in defending a CIPA claim.

3. Fix privacy notices and cookie disclosures

Make sure your words and deeds match up. Update privacy notices and cookie policies at least annually. Fully describe the categories of data collected, types of tools used (analytics, advertising, session replay, etc.), and classes of recipients.

Pay special attention to search bars, chat features, and forms. Where queries or messages may be processed by third-party vendors, say so plainly and in tight proximity to the tool itself.

Avoid aspirational statements or promises that are inconsistent with how your website actually works. Don't make blanket statements, like "we never sell data to third parties," without legal advice. Courts and regulators have shown little patience for mismatches between stated and actual practices, and those mismatches are also a ready hook for CIPA complaints.

4. Chat, forms, and search tools need to expect misuse

Treat any free-text input, including "harmless" on-site search bars, as potentially sensitive. Configure chat tools and search solutions to mask or suppress personal data before it leaves your environment where feasible (although, be advised that these features are not 100% effective!). Favor architectures in which vendors act purely as service providers/processors, with contractual restrictions on their ability to use or monetize data beyond delivering the service.

Provide clear, up-front disclosures in or near the chat or search interface (e.g., "Chats may be monitored and recorded using a third-party service provider" or "Search queries may be processed by our search vendor to return results and improve our site").

5. Tighten vendor contracts and allocation of risk

Review contracts with any vendors that provide analytics, advertising, session replay, chat, search, or consent management, or otherwise receive web-interaction data.

Key points to address:

- **Role and data-use restrictions**: Clearly define the vendor as a service provider/processor where possible, limit data use to specified purposes, and prohibit resale or independent profiling.
- (California Lawyers Association)
- **Compliance obligations**: Require vendors to maintain reasonable security, honor user consent signals, and support your compliance efforts (including providing configuration options).
- **Indemnification and limitations of liability:** Allocate responsibility for CIPA and other privacy claims appropriately, especially where a vendor's configuration or misuse of data could drive exposure.
- **Audit and information rights**: Preserve the ability to confirm how tools operate in practice.

Conclusion

CIPA may be an old statute, but it has had a major impact on modern digital operations. Plaintiffs' firms have successfully re-cast a wiretapping law into a powerful tool against website operators whose privacy notices, cookie banners, or embedded tools do not line up with their actual data practices.

For businesses, the instruction is clear:

1. Understand how your website really works.
2. Align your words with your deeds by providing transparent, accurate disclosures and obtaining true prior consent.
3. Manage the vendors and agencies who sit in the middle.

Done well, these steps not only reduce litigation risk, but also build the kind of privacy posture that courts, regulators, and consumers increasingly expect.

If you would like more information on managing CIPA exposure, strengthening website compliance, or evaluating your digital tracking practices, please contact Brian Focht.

Whether you are assessing consent flows, updating privacy notices, or implementing vendor and governance safeguards to mitigate litigation risk, Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line provides practical, strategic guidance to help your organization stay compliant and resilient in an evolving digital-privacy landscape.

Shumaker