SpencerFane®

Your Website May Be Creating Hidden Privacy Risk Under California Law

When companies think about data privacy risk, they usually focus on the growing patchwork of modern privacy laws, breach notification obligations, and increasingly complex disclosure requirements. But one of the most active areas of privacy litigation today is being driven by a statute that predates the internet by decades.

The California Invasion of Privacy Act (CIPA) was enacted in 1967 to address wiretapping and other forms of eavesdropping. Today, however, plaintiffs are using that same statute to challenge routine website technologies such as tracking pixels, analytics tools, chat features, session replay tools, and related third-party software. For businesses with an online presence, this trend is becoming increasingly difficult to ignore.

Why CIPA Matters

CIPA has become an attractive tool for plaintiffs for one simple reason: it carries meaningful litigation leverage. The statute provides a private right of action and authorizes damages of $5,000 per violation or three times actual damages, whichever is greater. Unlike the California Consumer Privacy Act as amended by the California Privacy Rights Act, which generally limits private actions to certain data breach scenarios, CIPA gives plaintiffs a direct avenue to assert claims tied to website communications and data collection practices.

That exposure is not limited to California-based companies. Courts have found that CIPA can apply where the website user is located in California, even if the business itself operates elsewhere. As a result, companies across the country may face demand letters or litigation based on how their websites or apps collect and share information during user interactions.

The Expanding Scope of Claims

Recent cases reflect an increasingly broad effort to apply CIPA well beyond traditional wiretapping. Plaintiffs have targeted a range of common website tools, including software development kits, tracking pixels, fingerprinting technologies, cookies, APIs, analytics platforms, and conversation intelligence or chat related software. In multiple cases, courts have allowed those claims to survive early dismissal efforts.

This matters because many of these technologies are now part of the standard digital toolkit. Businesses use them to understand website performance, improve user experience, personalize marketing, support customer communications, and better analyze engagement. Yet as the caselaw develops, ordinary use of these tools does not necessarily insulate a company from scrutiny.

Public filings likely capture only part of the picture. Many businesses appear to be responding to CIPA-related demand letters before litigation is filed, and some disputes may proceed privately through arbitration or confidential settlement. In practice, that means the real scope of CIPA related exposure may be broader than what public dockets alone would suggest.

No Immediate Legislative Relief

California lawmakers have considered narrowing CIPA's reach in the commercial context. During the 2025-26 regular session, legislation was introduced that would have carved out certain personal information processed for business purposes. That proposal has stalled in committee, and its future remains uncertain. For now, businesses should assume that CIPA will remain part of the privacy litigation landscape.

Practical Steps Businesses Should Consider

Whether CIPA applies in a particular situation will depend on the technology involved, how it is implemented, what data it captures, and how the company presents disclosures and obtains consent. But the recent wave of litigation highlights several steps companies should consider now.

- **Conduct a Technology Review:** Many organizations are not working from a current inventory of the tools operating on their websites and applications. Scripts, SDKs, analytics tags, advertising technologies, and embedded third-party tools are often added over time by different teams and vendors. Regular reviews can help companies understand what technologies are in place, whether they remain necessary, and whether their use aligns with current privacy expectations and legal obligations.
- **Evaluate Vendor Relationships:** CIPA risk may extend beyond the website owner. Plaintiffs have brought claims against both businesses and their vendors, and at least one provision of CIPA allows for aiding-and-abetting theories. Companies should therefore examine not only the tools they use, but also how their vendors collect, receive, process, or retain data. Contractual protections, implementation decisions, data-use limitations, and indemnity provisions may all be relevant.
- **Update Website Disclosures:** Privacy policies and terms and conditions should not be treated as one-time drafting exercises. As websites evolve and the privacy landscape continues to shift, those disclosures should be reviewed and updated to ensure they accurately reflect actual data practices. Inconsistencies between public disclosures and operational reality can create unnecessary risk.
- **Revisit Consent Mechanisms:** Recent caselaw continues to reinforce that consent can be one of the most effective defenses to CIPA-related claims. But consent requires more than simply posting a privacy policy or terms and conditions. Courts have focused on whether the user received meaningful notice and then took some affirmative step indicating agreement. That may occur during account registration, purchase flows, or other website interactions where the disclosure is sufficiently clear and conspicuous. By contract, courts have been less receptive where disclosures are vague, buried, or disconnected from any affirmative action by the user. The lesson is straightforward: businesses should not assume that passive disclosures alone will be enough.

The Takeaway

The recent rise in CIPA litigation underscores the importance of treating website privacy compliance as an ongoing business and legal priority, rather than a one-time exercise. Businesses that regularly evaluate their website technologies, contractual arrangements, and user-facing disclosures may be better positioned to

mitigate risk in an increasingly aggressive enforcement and litigation environment. Our technology team here at Spencer Fane regularly advises clients on these issues and can assist with assessing current practices, updating privacy-related documentation, and developing consent and governance strategies tailored to evolving legal requirements.

This blog was drafted by Jack Amaral, an attorney in the Minneapolis, Minnesota office of Spencer Fane. For more information, please visit www.spencerfane.com.

*Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.*