Understanding CIPA: California's Expanding Website Privacy Law

Legal Alert
October 10, 2025

Contact

Claire F. Hawkins

Kenzie Kinsella

Related Services

IP & Technology

Privacy, Cybersecurity & Data Protection

California's Invasion of Privacy Act (CIPA) was enacted in 1967 to prevent unlawful wiretapping. Nearly sixty years later it is being used in a new way: to challenge how websites collect and share user data.

Today, plaintiffs are filing lawsuits that allege certain online tools such as chat features, search boxes, session replay software or tracking technologies like cookies and pixels, allow companies or their vendors to "intercept" or "eavesdrop on" user interactions without consent.

Under CIPA, if only the website and the user are part of the communication, no claim arises (known as the "party exception"). However, when a third party receives or shares that data without clear prior consent, allegations of a violation can arise. These lawsuits are often brought as class actions, and because CIPA allows statutory damages of up to $5,000 per violation, potential exposure can be significant.

CIPA claims are not limited to websites. Plaintiffs have also brought cases involving mobile and cellular communications, reflecting how broadly this law can reach across digital interactions.

What Businesses Should Know

Consent Must Come First

Courts, including the Ninth Circuit in *Javier v. Assurance IQ, LLC*, have confirmed that consent must be obtained before any recording, tracking or interception begins. Consent cannot be implied from later activity or buried within a privacy policy.

"Passive" Tracking Can Still Create Risk

Liability is not limited to active recording. Recent cases show that data captured and shared in real time, especially when used for monetization or analytics, can support claims of unlawful interception or aiding and abetting. While courts in *Torres v. Prudential* and *Gutierrez v. Converse* found no liability where data was accessed only after transmission, other matters such as the ongoing Meta Pixel litigation suggest that simultaneous data capture and third-party sharing may be enough to move a claim forward.

The Legal Landscape Remains Unsettled

The scope of CIPA's "wiretap" provision and the reach of the "party exception" continue to evolve. The Ninth Circuit's decision in *Briskin v. Shopify* made it easier for California plaintiffs to bring CIPA claims based on website interactions, widening potential exposure for both California and out-of-state companies.

Considerations for Website Owners

Review Your Data Tracking Tools

Understand what information is collected, who accesses it and how it is used. Avoid or delay deploying tools such as pixels or session replay on pages that capture keystrokes, searches, chat messages or sensitive information like financial or health data unless prior, explicit consent is in place.

Make Consent and Privacy Disclosures Clear

Your privacy policy and website terms should describe what is tracked, why it is collected and whether third parties are involved. Provide visible opt-in or opt-out options and make sure disclosures match actual practices.

Strengthen Data Controls

Use clear banners or gates to collect express consent before any recording or tracking starts. Limit data retention, mask sensitive fields and ensure contracts with vendors restrict their use of data to processor-only functions, prohibiting data mining, training or resale.

Prefer First Party or Self-Hosted Solutions

Relying on first-party tools reduces risk of third-party interception. Regularly review vendor documentation to confirm that data is not shared or repurposed for marketing, analytics or AI training without authorization.

Customize for California Visitors

Because CIPA applies to California users, consider implementing California-specific experiences. Coordinate with IT to disable or limit chat, pixels or session replay tools for California visitors unless they have opted in. Maintain logs of consent and conduct periodic privacy audits to ensure compliance with emerging case law.

Looking Ahead

CIPA enforcement and litigation are changing quickly as courts apply this decades-old law to modern technologies. While no compliance program can eliminate all risk, businesses that prioritize transparency, consent and vendor oversight will be best positioned to reduce exposure. Working with experienced counsel to review data collection practices and technology partners can help align your approach with the latest interpretations of California privacy law.

The information above involves complex legal considerations and is provided for general informational purposes only. It does not constitute legal advice. For guidance on specific legal matters, please contact your attorney.