masuda funai

News & Types: Client Advisories

From Wiretaps to Websites: Why Your Business Should Care About CIPA

1/7/2026

Practices: Intellectual Property & Technology

As businesses incorporate an increasing range of data-driven tools and digital engagement strategies to maintain a competitive edge, they many find themselves navigating unexpected legal challenges under the California Invasion of Privacy Act ("CIPA"). Increasingly, plaintiffs are relying on CIPA to challenge the use of routine website analytics, software developer kits (SDKs), tracking pixels, and other website analytical and related technologies, exposing businesses to statutory damages and the risk of costly class action lawsuits.

Unlike California's comprehensive data privacy law, the California Consumer Privacy Act (as amended by the California Privacy Rights Act), which regulates the collection, use and disclosure of California residents' personal information and provides only a limited private right of action for certain data breaches, CIPA focuses on the interception of private communications, imposing statutory damages of up to $5,000 per violation or three times the plaintiff's actual damages (whichever is greater).

CIPA is a criminal statute originally enacted in 1967 to address telephone wiretapping, but in recent years has been repurposed by plaintiffs to cover modern digital tools. Such plaintiffs argue that these tools, which collect or monitor information exchanged between a website user's browser and the subject website, constitute an illegal "interception" under the law. Further, courts have held that CIPA applies extraterritorially to business located wholly outside of California where the alleged "interception" involved a website or digital interaction with a user physically located within the state.

Notwithstanding the foregoing, federal courts have begun to scrutinize the recent increase in lawsuits and demand letters more rigorously, with one judge in the Northern District of California describing the current state of CIPA litigation as "untenable." Notably, the Ninth Circuit has provided defendants with several important precedents to combat CIPA claims by holding that (i) data collected by website tracking tools does not constitute the type of private information necessary to establish injury, (ii) CIPA does not extend to routine internet communications or website operators, and (iii) claims brought by "tester" plaintiffs who seek out alleged violations lack standing to bring CIPA claims, establishing critical hurdles for CIPA litigation.

Within this continually evolving CIPA litigation landscape, businesses using tracking and data-driven technologies on their websites should work closely with counsel to ensure compliance and reduce potential exposure to CIPA claims. As a best practice, businesses should regularly audit their website technologies to ensure alignment with privacy laws and business objectives, coordinate with third-party vendors to address potential liability, and regularly work with counsel to review and update applicable privacy policies and terms of use to ensure that data collection and use practices are accurately disclosed. Additionally, user consent

remains the strongest defense against CIPA claims, and businesses should consider implementing robust consent frameworks, including clear notice and requiring affirmative user action before deploying any data-driven tools implemented by the business. By combining these steps, businesses can position themselves for early dismissal, favorable resolution, or a strong defense against potential claims.

Please contact Jake Bennett at jbennett@masudafunai.com or any member of Masuda Funai's Intellectual Property, and Technology group if you have any questions about the CIPA or privacy compliance more generally.

Follow us on LinkedIn for additional Legal Updates.

Masuda Funai is a full-service law firm with offices in Chicago, Detroit, Los Angeles, and Schaumburg.