



Privacy & Cybersecurity Update

October 2026

California Enacts SB 690, Eliminating Private Pen/Trap Claims Over Website Tracking

On September 30, 2026, California Governor Gavin Newsom signed [Senate Bill \(SB\) 690](#) into law after the California Legislature unanimously passed it on August 28, 2026. The law responds to a surge of litigation targeting businesses for their use of common website tracking technologies. SB 690 eliminates the private right of action under the pen register and trap-and-trace (“pen/trap”) provision of the California Invasion of Privacy Act (CIPA), California Penal Code Section 638.51, for claims arising from conduct on an internet website, online application, or mobile application. Going forward, only the California Attorney General may enforce these claims. SB 690 takes effect January 1, 2027.

SB 690 is narrow. It focuses exclusively on CIPA’s pen/trap provision, so businesses remain exposed to demand letters and lawsuits over their websites under other CIPA provisions, other California laws, and federal statutes.

Background: The Rise of CIPA Section 638.51 Claims

Section 638.51 was added to CIPA in 2015 to create a statewide framework for law enforcement to obtain and use pen/trap devices. Although it largely mirrors the federal pen/trap statute, it contains several requirements unique to California.

In short, Section 638.51 prohibits the use of pen/trap devices without a court order or other authorization. Over the past few years, plaintiffs have sent waves of demand letters and filed lawsuits, many as putative class actions, against businesses of all sizes and locations. These claims allege that common website tracking technologies, such as analytics and advertising cookies and pixels, fall within that

prohibition. Unfortunately for businesses, several California federal and state courts have allowed these types of CIPA Section 638.51 claims to survive early dismissal motions, finding them sufficiently plausible to proceed.

What Does SB 690 Address?

As originally introduced, SB 690 would have created a broad “commercial business purpose” exception to several CIPA provisions that have seen a recent uptick in litigation, including its wiretapping, eavesdropping, and pen register provisions. During the legislative process, however, SB 690 was narrowed so that it now applies only to CIPA Section 638.51.

Specifically, SB 690 eliminates the private right of action for a violation of Section 638.51 that is “alleged to arise from conduct occurring on an internet website, online application, or mobile application.” Only the California Attorney General may bring these types of claims. (Cal. Penal Code § 637.2(d)(1).) SB 690 also applies retroactively to any pending claim in an action commenced within the previous two years. (Cal. Penal Code § 637.2(d)(2).)

What Does SB 690 Not Cover?

SB 690 will do little to stop the broader wave of demand letters and lawsuits targeting analytics and advertising cookies and pixels on commercial websites. In recent months, plaintiffs’ attorneys have expanded their theories, alleging that deploying these technologies without consent may violate a wide range of other laws, including the following:

- CIPA Section 631 (wiretapping)
- CIPA Section 632 (eavesdropping)
- California Comprehensive Computer Data Access and Fraud Act (CDAFA) (computer hacking)
- California Unfair Competition Law (UCL)
- Unjust enrichment
- Common law fraud, deceit and/or misrepresentation
- Negligence
- Intrusion upon seclusion
- Electronic Communications Privacy Act of 1986 (EPCA) (federal wiretapping)

Unfortunately for businesses, SB 690 does not change any of these frameworks or clarify whether they apply to analytics and advertising cookies and pixels.

What's Next?

Businesses that have received a demand letter or a complaint alleging a violation of Section 638.51 should consult counsel to evaluate how SB 690 affects pending claims and available defenses.

Although SB 690 is meaningful reform, it does not protect businesses from other website privacy claims, whether under the California and federal laws listed above or under other states' wiretapping and privacy statutes. Businesses should consider the following measures to reduce their exposure:

- **Inventory tracking technologies.** Assess the first- and third-party cookies, pixels, and tags deployed across websites, mobile applications, and other public-facing digital assets.
- **Validate consent tools.** Confirm that consent management platforms and cookie-banner configurations operate as intended and as represented to users.
- **Update disclosures.** Ensure privacy notices/statements and cookie policies are posted clearly and conspicuously and accurately reflect actual business practices.
- **Strengthen terms of use.** Adopt website "terms of use" or similar contractual clauses that bind end users to rules governing site use, including appropriate dispute resolution provisions.

A full list of recommendations is available on Thompson Hine's [Website and Mobile App Compliance & Litigation](#) web page.

Thompson Hine's [Privacy Litigation](#) team has significant experience defending website privacy and accessibility claims, including class action and single plaintiff lawsuits, and pre-suit demand letters. We have deep experience representing clients against the most prolific litigators in this area in state and federal court as well as arbitration.

We have also advised hundreds of companies on website privacy compliance, cookie management, and risk mitigation. If you have received a website privacy or accessibility demand letter or complaint, or want to proactively manage your organization's risk, contact us at PrivacyLitigation@thompsonhine.com.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Kim Sim Sandell

310.382.1309

Kim.Sandell@ThompsonHine.com

Thomas F. Zych

216.566.5605

Tom.Zych@ThompsonHine.com

Kimberly Pack

312.998.4262

Kimberly.Pack@ThompsonHine.com

Certified Information Privacy Professional/United States (CIPP/US)

Certified Information Privacy Manager (CIPM)

Thora Knight, Ph.D.

212.908.3971

Thora.Knight@ThompsonHine.com

Sophie Kreuger

310.382.1327

Sophie.Krueger@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2026 THOMPSON HINE LLP. ALL RIGHTS RESERVED.