



## Privacy & Cybersecurity Update

August 2026

### California Legislature Amends CIPA Pen/Trap Law for Website Claims – What’s Next?

On August 28, 2026, the California Legislature overwhelmingly passed [Senate Bill \(SB\) 690](#), and it will now be presented to California Governor Gavin Newsom for signature. SB 690 is designed to limit the ongoing avalanche of lawsuits and demands targeting businesses for their use of analytical and advertising cookies, pixels, and similar technologies on their public-facing websites. However, SB 690 only applies to a small subset of website-related lawsuits that are brought under the pen register and trap-and-trace (“pen/trap”) provisions of §638.51 of the California Invasion of Privacy Act (CIPA), and therefore businesses are still at risk of receiving demand letters and complaints over their websites based on other areas of California law and federal statutes.

#### Background: The Rise of CIPA § 638.5 Claims

CIPA § 638.51 was enacted in 2015 and created a California-wide framework for law enforcement to obtain and use pen/trap devices. Although CIPA mirrors the federal law regulating pen/trap devices, it contains some unique requirements.

In short, CIPA § 638.51 prohibits the use of pen/trap devices without authorization or a court order. In the last few years, plaintiffs have brought waves of lawsuits and demand letters against businesses (of all sizes), alleging that common website tracking technologies—such as analytics and advertising cookies and pixels—fall within the scope of that prohibition. Unfortunately for businesses, several California federal and state judges have allowed these types of CIPA § 638.51 claims to proceed to litigation on the grounds that these cases could plausibly have merit.

#### What Does SB 690 Address?

As originally drafted, SB 690 would have created a broad “commercial business purpose” exception to several CIPA provisions that have been the subject of a recent uptick in litigation, including CIPA’s wiretapping, eavesdropping, and pen register provisions. However, the legislative amendment process changed the scope and text of SB 690, and the amendment now only applies to CIPA § 638.51.

Specifically, SB 690 removes a private right of action for a violation of CIPA § 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. SB 690 applies retroactively to any pending claim in an action commenced within the previous two years.

#### What Does SB 690 Not Cover?

SB 690 is akin to applying a Band-Aid on a bullet wound, and it will do little to stop the wave of demand letters and lawsuits targeting the use of analytical and advertising cookies and pixels on commercial websites. In the last several months, plaintiffs’ attorneys have expanded their claims against businesses and have alleged that the use of analytical and advertising cookies and pixels without consent could potentially violate a broad range of California requirements, including the following:

- CIPA § 631 (wiretapping statute)
- CIPA § 632 (eavesdropping statute)
- Comprehensive Computer Data and Access Fraud Act (computer hacking statute)

- California Unfair Competition Law (UCL)
- Unjust Enrichment
- Negligence
- Intrusion Upon Seclusion rights
- Invasion of Privacy rights
- Electronic Communications Privacy Act of 1986 (federal wiretapping law)

Unfortunately for businesses, SB 690 does nothing to address these legal frameworks or clarify their inapplicability to the use of analytical and advertising cookies and pixels.

### What's Next?

Even if SB 690 is enacted into law, businesses could still be subject to frivolous website privacy-related claims. Therefore, they should consider undertaking the following measures to better protect themselves.

- Assess the first- and third-party cookies, pixels, and tags deployed across websites, mobile applications, and public-facing assets, for inventory and diligence purposes.
- Confirm that consent management platforms and cookie-banner configurations operate as intended and as represented to users.
- Ensure appropriate privacy notices/statements and cookie policies are posted clearly and conspicuously and reflect actual business practices.
- Draft "terms of use" or similar contractual clauses that bind website end-users to rules governing how they may (and may not) use a website, including appropriate dispute resolution clauses.

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

### FOR MORE INFORMATION

For more information, please contact:

**Steven G. Stransky**

216.566.5646

202.263.4126

[Steve.Stransky@ThompsonHine.com](mailto: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](mailto:Kim.Sandell@ThompsonHine.com)

**Thomas F. Zych**

216.566.5605

[Tom.Zych@ThompsonHine.com](mailto:Tom.Zych@ThompsonHine.com)

**Kimberly Pack**

312.998.4262

[Kimberly.Pack@ThompsonHine.com](mailto: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](mailto:Thora.Knight@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.