Privacy Bill Must Be Amended To Protect Small Businesses

By **Steven Stransky and Kim Sandell** (August 5, 2025)

On June 3, the California Senate passed S.B. 690, which amends certain provisions of the California Invasion of Privacy Act that regulate surveillance activities, such as wiretapping, eavesdropping and the use of pen registers and trap-and-trace devices.[1]

Steven Stransky

Specifically, S.B. 690 seeks to ensure that a company's use of legally compliant website advertising and tracking technologies are exempt from CIPA, and stop the avalanche of abusive lawsuits against companies for their uses of these online technologies.

However, S.B. 690 does not adequately protect small businesses. In fact, if enacted by the California Legislature in its current form, there is a risk that S.B. 690 could expose small businesses as the primary targets in future CIPA lawsuits.

Kim Sandell

Fortunately, there is still time to address this issue and update S.B. 690 to ensure that it fully protects all companies — including small businesses — from frivolous CIPA litigation.

Background: California Privacy and Surveillance Laws

There are two key legal frameworks underlying S.B. 690: (1) California's consumer privacy laws and regulations, and (2) CIPA.

The California Consumer Privacy Act regulates the manner in which a covered business may collect and process a consumer's personal information. The California Privacy Rights Act amended, added to and reenacted the CCPA.

The CPRA specifically addresses how a covered business may deploy website advertising and tracking technologies for cross-contextual behavioral advertising and sell a consumer's personal information. Generally, the law requires covered businesses to provide consumers with the ability to opt out from such digital advertising and sales — this is often referred to as a consumer's opt-out rights.

The CPRA has a limited private right of action and the California Privacy Protection Agency is chiefly responsible for enforcing its data protection rules.

On the other hand, CIPA primarily regulates the use of wiretapping, eavesdropping and similar technologies. It also enumerates the procedures under which certain California state officials may submit a judicial application for approval to use a pen or trap-and-trace device. CIPA was originally enacted in the 1960s and has been amended several times to account for advances in various surveillance technologies.

CIPA also includes a private right of action and a statutory damages framework for noncompliance. This is a key reason plaintiffs have relied on CIPA — and not the CPRA — to bring an unprecedented amount of website privacy-related lawsuits targeting business for their use of website advertising and tracking technologies.

The Surge in Frivolous CIPA Claims

It is common for organizations to deploy website advertising and tracking technologies for cross-contextual behavioral advertising. This approach helps to better ensure that customers receive advertisements that are relevant and targeted to their interests and limits the amount of resources a company has to spend on identifying new leads.

However, plaintiffs lawyers have seen these digital advertising activities as a litigation opportunity and there has been a surge in class actions alleging that the use of advertising cookies and pixels violate CIPA's opt-in provisions governing wiretapping, eavesdropping and pen register or trap-and-trace provisions.[2]

In particular, as noted by the U.S. District Court for the Central District of California in its 2023 decision in Byars v. Hot Topic Inc., CIPA litigators have developed a stable of "serial litigants" that simply "copy and paste a complaint over and over again" while targeting new companies as potential CIPA violators.[3]

These legal claims have resulted in contradictory judicial rulings, and created uncertainty on whether, and how, a company should comply with the CPRA's opt-out framework and CIPA's opt-in framework governing website advertising and tracking technologies. S.B. 690 is intended to address this litigation crisis.[4]

New CIPA Exemptions

S.B. 690 seeks to end these CIPA-related website privacy claims by exempting certain activities from the scope of CIPA itself. Specifically, S.B. 690 amends CIPA's provisions governing wiretaps, eavesdropping devices and pen register or trap-and-trace devices by expressly stating that they do not apply to activities undertaken for a "commercial business purpose."

In turn, the term "commercial business purpose" is defined as the processing of personal information that satisfies either of the following criteria: (1) it is performed to further a "business purpose" as so defined by the CPRA, or (2) it is subject to a consumer's opt-out rights under the CPRA.

Thus, if S.B. 690 is enacted, then CIPA would not apply to the use of website advertising and tracking technologies when they are conducted for a business purpose under the CPRA (e.g., auditing of ad impressions, website security) or when conducted in accordance with the CPRA's opt-out framework for cross-contextual behavioral advertising and the sale of data, among other areas.

But therein lies the problem for small businesses: The exemptions within S.B. 690 are limited by, and only apply to, activities performed in accordance with the CPRA. However, the CPRA does not apply to all organizations and often does not include small businesses within its scope of applicability.

Rather, the CPRA primarily applies to a subset of companies that collect large volumes of personal information or generate significant profits each year and many small business entities, like mom-and-pop shops, are simply not subject to the CPRA.

As of 2025, for-profit businesses are subject to the CPRA if they have a gross annual revenue of at least $26.625 million; buy, sell or share the personal information of 100,000 or more California residents or households; or, derive at least 50% of their annual revenue from selling California residents' personal information.[5]

Accordingly, for the same reasons that a small business may not be subject to — or even have to comply with — the CPRA, a California judge could rule that it cannot invoke the CPRA exemptions within S.B. 690 to avoid a CIPA-based website privacy claim.

In other words, a judge could analyze S.B. 690 and hold that a mom-and-pop shop cannot rely on the CPRA exemptions therein because the small business is not considered — as a matter of law — a covered business within the plain meaning of the CPRA. And such an interpretation could have devastating consequences on small businesses.

It could potentially result in CIPA litigators focusing their lawsuits on small businesses that are not subject to the CPRA, and that are not hampered with the business purpose framework within the law or otherwise legally required to deploy opt-out rights on their websites.

The Solution to Better Protect Small Businesses

S.B. 690 is an excellent start to curbing frivolous CIPA litigation.[6] However, S.B. 690 should be amended in two ways to better ensure that all companies — including small businesses — are not targeted with frivolous CIPA litigation related to website advertising and tracking technologies.

First, the term "commercial business purpose" should be amended to clarify that any company may invoke the two CPRA exemptions set forth therein (i.e., the business purpose and opt out rights exemptions) regardless of whether they are a covered business for purposes of the CPRA. This will help ensure that any company — of any size — will be able to leverage the new exemptions enacted under S.B. 690.

Second, the California Legislature should consider removing the private right of action under CIPA for claims related to website advertising and tracking technologies. This can be accomplished by adding a new Section (e) to Section 637.2 of the California Penal Code stating that, notwithstanding any other provision within CIPA, an individual may not, in any capacity, bring or continue to proceed with an action, under the law against a legal entity on the basis or otherwise related to whether the legal entity installed, used, deployed or transmitted certain types of advertising or tracking technologies on the legal entity's website or similar online applications.

The removal of a private right of action in this very limited context is important to help deter frivolous litigation in the first instance by removing the law's statutory recovery provisions. It also has the ancillary benefit of bolstering the authority of the California Privacy Agency, which was created to implement and enforce the CPRA's requirements, including those related to website advertising and tracking technologies.

By deterring CIPA litigation in federal and state courts, the California Privacy Agency will not have to contend with potentially competing and contradictory judicial rulings, and it will be in better position to articulate clear regulatory standards.

Steven G. Stransky is a partner and co-chair of the privacy and cybersecurity practice at Thompson Hine LLP.

Kim Sandell is senior counsel at the firm.

[1] LegiScan, California Senate Bill 690, available at https://legiscan.com/CA/bill/SB690/2025 (last visited July 20, 2025).

[2] Steven G. Stransky, et al., "No Cause of Action: California's Pen/Trap Law Inapplicable to Web Ad Cookies and Pixels," Washington Legal Foundation Working Paper (Mar. 2024).

[3] Byars v. Hot Topic Inc., 656 F. Supp. 3d 1051, 1059-60 (C.D. Cal. 2023).

[4] According to Senator Anna M. Caballero, the primary sponsor of SB 690, the bill "[s]tops the abusive lawsuits against California businesses and nonprofits" under CIPA for engaging in "standard online business activities that are already regulated" by the CCPA/CPRA. Senator Anna M. Caballero, "Senator Anna M. Caballero Unveils Bold Legislative Package for 2025" (Apr. 8, 2025), available at https://sd14.senate.ca.gov/news/press-release/senator-anna-m-caballero-unveils-bold-legislative-package-2025 (last visited July 20, 2025).

[5] Cal. Civ. Code §1798.140(d)(1). Interestingly, the CCPA/CPRA provides that an organization that does not satisfy the applicability thresholds of a covered "business" may still be considered a "business" for purposes of the law if it "voluntarily certifies" to the CA Privacy Agency "that it is in compliance with, and agrees to be bound by," the CCPA/CPRA. Id. at §1798.140(d)(4).

[6] Steven G. Stransky, et al, "California Has A Duty To Curtail Frivolous CIPA Suits," Law360 (June 13, 2024).