SENATE THIRD READING
SB 690 (Caballero)
As Amended July 2, 2026
Majority vote

SUMMARY

Eliminates the private right of action in the California Invasion of Privacy Act (CIPA) where the cause of action is against an internet website, online application, or mobile application for violation of the pen register statute, as specified; and states this bill applies retroactively to any pending claim against an internet website, online or mobile application based on the pen register statute commenced within two years before January 1, 2027

COMMENTS

According to the Author

"Recently, a handful of trial lawyers have sent thousands of demand letters and sued over 1,800 businesses in California using a 1967 criminal wiretapping statute called the California Invasion of Privacy Act, which requires a court order before recording phone calls.

"This small group of trial lawyers is alleging that typical online business activities, like web analytics or online advertising, constitute "wiretapping" or an illegal "pen register" under the wiretapping statute. They argue that businesses must get consumer consent – or "opt-in" consent – before a business can, for example, assess which pages are getting the most views, save an online shopping cart, or show an ad. Without that consent, trial lawyers are suing businesses for $5,000 of statutory damages – no proof of injury required - for every visit to their website under the wiretapping statute's private right of action.

"Meanwhile, the California Consumer Privacy Act (CCPA) is the strongest privacy law in the nation and California businesses have invested significant revenue – by the state's own estimates, over $55 billion in initial compliance costs alone - to comply with CCPA. In 2018, the Legislature unanimously decided that consumers benefit most when these types of online business activities should be regulated by the CCPA, which requires "opt-out" consent. The first Executive Director of the California Privacy Protection Agency, Ashkan Soltani – also former Obama-era Federal Trade Commission (FTC) Chief Technologist – explained why in a 2019 Senate Judiciary Committee hearing, stating:

'…by moving to an opt-in regime where consumers have to opt-in and consent to the use of their information, not only are they not going to be able to understand and consent for immediate benefits…they're also going to experience opt-in fatigue when they're just going to opt-in to whatever the service is, like free coffee, in order to get that benefit today at the risk of anything that happens tomorrow.'

"Then, in 2020, California voters reaffirmed their support of CCPA via ballot measure and strengthened its privacy protections. The ballot measure also created the California Privacy

Protection Agency, which has drafted over 150 pages of regulations on how a business must implement this extensive privacy regime."

"The CCPA *is* a floor, not a ceiling – and more privacy protections have been added to the CCPA every year. SB 690 would not change that. For example, in 2023, Assemblymember Wendy Carrillo, passed AB 1194, Chapter 567, Statutes of 2023, a bill that added additional protections in the CCPA for reproductive health data. That same year, Assemblymember Jesse Gabriel passed AB 947, Chapters 551, Statutes of 2023, which explicitly added immigration and citizenship protections to the statute. Even more bills have been proposed this year.

"Assemblymember Chris Ward introduced AB 1355 to add further protections for geolocation data. Although his legislation was not successful this year, Assemblymember Ward intends to continue to pursue this issue. Importantly, AB 566 (Lowenthal), sponsored by the Privacy Agency, continues to move through the legislature this year with the goal of further strengthening CCPA's opt-out regime by requiring internet browsers to provide consumers with the ability to opt-out at the browser level – which would automatically opt them out of the sale/sharing of their data for every website a consumer visits in a browser.

"Yet, California businesses are now being sued *because of* their compliance with CCPA's opt-out regime. These abusive lawsuits do nothing to help consumer privacy. They use the same "test plaintiffs" repeatedly – 60, 70, 80, or even 100+ times. The test plaintiff simply visits a website, looks to see if there are any cookies on the website, and if there is no corresponding opt-in consent mechanism, they send off a demand letter based on CIPA's $5000 per violation (read: per website visitor) and ask for, typically, between $20,000-$50,000 from a business (or non-profit).

"Smaller businesses typically cannot afford the cost to litigate and settle to make cases go away. As a result, many have struggled financially.

"For larger businesses with many viewers on their website, the liability is staggering. In the Senate Public Safety Committee, the President of the LA Times testified the Times has been sued for <u>billions</u> and called the lawsuit an "extinction level threat" to publishers. Even for those businesses who pay a trial lawyer to settle a case, another law firm can sue them the next day. This is why a legislative solution is necessary.

"SB 690 seeks to stop these abusive lawsuits by clarifying that CIPA, the 50-year-old criminal eavesdropping statute, does not apply to modern, online business activities that are already intentionally, purposefully, and extensively regulated by the CCPA.

"SB 690 intends to keep CIPA's intended protections in place, while ensuring that these lawsuits cannot continue to be based on a legal theory that creates liability for nearly every website on the internet in California, especially when CCPA was specifically designed to govern business website activity. Putting aside the unfairness to businesses, our state has been very clear as to how it wants to regulate online business activity - and these lawsuits have caused significant confusion for business compliance.

"Notably, the Attorney General has never brought a claim against a business under CIPA for online business activity. Instead, the AG as well as California Privacy Protection Agency have brought claims against businesses for not complying with the many, detailed requirements of the CCPA's opt-out regime. These state enforcement authorities are also shutting down data brokers and punishing businesses who are engaging in online tracking without complying with the CCPA's many notification requirements and consumer rights.

"Notably, the pen register and trap and trace provision of CIPA, which is the center of many of these lawsuits, was added to CIPA in 2015 with AB 929 (Chau), Chapter 204, Statutes of 2015. The legislative history of this provision makes it clear it was not intended to apply to online activity. At the time, former Assemblymember Ed Chau stated, "This bill is intended to authorize state and local law enforcement to seek emergency orders for pen registers/trap and trace devices, [which] are used by law enforcement for telephone surveillance to record incoming and outgoing phone numbers from a tapped line." He further explained, "[a] pen/trap order is only for the capture of incoming and outgoing phone numbers."

"To the extent opponents of SB 690 believe privacy protections in California are not strong enough, despite having the strongest law in the nation, reform belongs in the CCPA – not via an endless avalanche of CIPA lawsuits. The CCPA already includes a mechanism for regulatory updates via the California Privacy Protection Agency. Suing under CIPA for behavior explicitly regulated (or permitted) by CCPA short-circuits legislative intent.

"Opponents to SB 690 often cite to a few prominent cases against large technology companies as the reason the flood of CIPA lawsuits should be allowed to continue unabated. However, CIPA lawsuits against "Big Tech" companies account for about 1% of these lawsuits. About 40% of these lawsuits are against retailers. If opponents to SB 690 believe that certain aspects of cookie tracking, cross-contextual behavioral advertising, or pixel use allowed California's omnibus privacy law are too permissive, the fix is not to shoehorn these modern issues into an old eavesdropping criminal statute – it is to reform the CCPA through clear and democratically accountable updates.

"With respect to strengthening the regulatory guardrails for the data broker industry, which are often mentioned by opponents to SB 690, the Legislature and the regulatory enforcement authorities are on the case. In 2019, the Legislature amended CCPA by adding requirements that data brokers register with the state so that consumers wishing to exercise their deletion rights or to opt out of the sale and sharing of their data from data brokers would have a one-stop-shop to effectuate their CPPA rights. In 2023, the Legislature passed the DELETE Act with SB 362 (Becker), Chapter 709, Statutes of 2023, which created a new right for consumers with respect to data brokers. SB 362 requires that after a data broker receives a "deletion request" from a consumer, in addition to deleting all current data, every 45 days the data broker must delete any new data it has received regarding that consumer, and the data broker is prohibited from selling or sharing any new information it acquires for that consumer.

"This year, Senator Becker has introduced SB 361, another bill strengthening consumer protections with respect to data brokers that is moving through the Legislature. SB 361 expands the type of information data brokers must disclose that they collect, which will then be displayed on the data broker registry.

"Meanwhile, the California Privacy Protection Agency, now led by Executive Director, Tom Kemp, who was the chief sponsor of the DELETE Act, continues to crack down on data brokers – in some cases by shutting entire companies down - by enforcing the CCPA and the statutes intended to regulate this industry – *not* a wiretapping statute passed in 1967, with no legislative history stating that it is intended to apply to online activities.

"SB 690 will stop abusive shake down lawsuits for standard online business activities against California businesses and nonprofits filed under the CIPA enacted in 1967, long before the internet was even developed. Online business activity is regulated by the CCPA, and is California's omnibus privacy law which is the guiding statute for online privacy protections including data protections. Despite the enactment of the CCPA, vexatious litigation using the CIPA prey on small business owners and non-profits who cannot afford to defend themselves even though they are in compliance with existing law. SB 690 will clarify that online businesses that comply with the CCPA opt-out requirements cannot be punished under the CIPA.

"Finally, most of these CIPA lawsuits are settled without admission of wrongdoing. A private settlement does not create stronger protections for consumers or clearer rules for businesses. It just ends one case. The only beneficiaries of CIPA lawsuit settlements are the handful of trial lawyers pursuing these cases and the organizations that benefit from funding from the plaintiffs' bar."

Arguments in Support
According to the *Reform CIPA Coalition*:

The California Invasion of Privacy Act (CIPA) was written in 1967 to stop illegal telephone wiretapping, but since around 2022, a small group of predatory attorneys have exploited this law to sue businesses and organizations for using common website analytics tools. Over 3,500 of these frivolous lawsuits have been filed in California courts just over the past three years, alongside thousands of demand letters.

While SB 690 is a meaningful step toward curbing these predatory lawsuits, it does little to eliminate this type of litigation overall. As amended, SB 690 only affects the pen register component of the pen register and trap and trace claim (§ 638.51), leaving the law's other provisions open to exploitation. An analysis of the Fisher Phillips' Wiretapping Litigation Map, estimates that the current version of SB 690 would fully relieve only 27% of organizations now facing CIPA litigation while partially relieving another 12%, leaving 61% of businesses and organizations unprotected. That gap carries significant fiscal consequences. This wave of litigation draws on public resources at scale, with many cases filed against small businesses, nonprofits, healthcare clinics, and even local government agencies. However, due to the immense legal costs to fight these baseless claims in court, many defendants are forced to settle — all while doing nothing to strengthen consumer privacy. A June 2026 study conducted by Oxford Economics estimates the average CIPA demand letter at roughly $30,000 to resolve. The statewide cost of demand letters alone rests well above $1 billion, and as many as 100,000 California businesses and organizations have received one.

Arguments in Opposition
According to the *Electronic Frontier Foundation (EFF)*:

We sincerely appreciate how the bill's most recent amendments reduce consumer harm as compared to the language as originally filed. A broad exemption from the law for a "commercial business purpose" would have essentially removed businesses from the law entirely. However, as an organization that advocates for private rights of actions to promote corporate accountability, we must remain opposed to the bill. It is a cornerstone of EFF's legislative advocacy that ordinary technology users should have the power to decide for themselves whether to bring a lawsuit to enforce their statutory privacy rights.

It is one of the most effective ways to change corporate behavior. CIPA was originally intended to protect personal privacy against the threat of surveillance of private communications. S.B. 690, even as amended, harms privacy by making it impossible for ordinary persons to sue companies engaged in unlawful metadata surveillance.

This rollback is particularly troubling as the federal government and other law enforcement agencies are looking for data from businesses or data brokers to target people based on their political beliefs, religious affiliations, or health decisions. People should be able to continue to sue for these violations, which can endanger their privacy and physical safety. Removing mechanisms to hold companies accountable for this sort of secret sharing is a step in the wrong direction.

Furthermore, the bill still contains a retroactivity provision that purports to eliminate "any pending claim in an action commenced within two years before the operative date" of the bill. Even if the companies being sued actually violated the law by recording sensitive location and other information, this provision means that the customers they harmed will not be made whole. Weakening CIPA's private right of action—and therefore reducing individual power and ability to enforce their privacy rights—remains wholly inappropriate.

FISCAL COMMENTS

According to the Assembly Appropriations Committee:

1) Costs of up to approximately $1.5 million (General Fund) to the Department of Justice (DOJ), reflecting six positions and $150,000 in external expert costs beginning January 1, 2027. Within the Public Rights Division, the Consumer Protection Section would add two deputy attorneys general, two legal secretaries, and one senior legal analyst, along with the external expert costs, to investigate and enforce violations for which this bill makes the Attorney General (AG) the exclusive enforcement authority. The Public Inquiry Unit within the Directorate Division would add one analyst to intake, process, and route related complaints and inquiries. DOJ reports the department could not absorb these costs within existing budgeted resources. Notably, the bill authorizes the AG to bring these actions but requires no enforcement activity of any kind. The volume and pace of enforcement, and therefore the resources needed to support enforcement, would remain within the AG's discretion.

2) Potential reduction in trial court workload and associated cost pressures (Trial Court Trust Fund (TCTF)) of an unknown, but potentially significant amount. According to the bill's sponsor, approximately 4,000 lawsuits alleging CIPA violations have been filed against California businesses, the bulk of which assert pen register claims based on website tracking software. By eliminating the private right of action for these claims and applying that change retroactively to pending claims commenced within two years before the bill's operative date, this bill would remove a substantial volume of pending and future civil litigation from the trial courts. Although courts are not funded on the basis of workload, reduced pressure on the TCTF may reduce demand for increased General Fund support of the courts.

VOTES

SENATE FLOOR: 35-0-5

YES: Allen, Alvarado-Gil, Archuleta, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Choi, Dahle, Durazo, Gonzalez, Grayson, Grove, Jones, Laird, Limón, McGuire, McNerney, Menjivar, Niello, Ochoa Bogh, Padilla, Pérez, Richardson, Rubio, Seyarto, Smallwood-Cuevas, Stern, Strickland, Umberg, Valladares, Weber Pierson, Wiener
ABS, ABST OR NV: Cervantes, Cortese, Hurtado, Reyes, Wahab

ASM PUBLIC SAFETY: 9-0-0
YES: Schultz, Alanis, Mark González, Haney, Harabedian, Lackey, Nguyen, Ramos, Sharp-Collins

ASM PRIVACY AND CONSUMER PROTECTION: 14-0-1
YES: Bauer-Kahan, Macedo, Bryan, DeMaio, Hoover, Irwin, Lowenthal, Ortega, Patterson, Pellerin, Petrie-Norris, Ward, Bennett, Wilson
ABS, ABST OR NV: McKinnor

UPDATED

VERSION: July 2, 2026

CONSULTANT: Kimberly Horiuchi / PUB. S. / (916) 319-3744 FN: 0003508