May 28, 2025

The Honorable Anna Caballero
State Capitol, Room 412
Sacramento, CA 95814

RE: S.B. 690 (Caballero) – *Oppose*

Dear Senator Caballero,

Consumer Reports[1] respectfully opposes S.B. 690, legislation that would create a series of broad new exemptions under the California Invasion of Privacy Act (CIPA) to allow any business to tap, secretly record, or intercept the private communications of individuals for any commercial business purpose. These exemptions contradict the fundamental purpose of CIPA to prevent spying on individuals and would put Californians' most intimate and private conversations at risk of being misused, leaked, or otherwise shared with bad actors.

S.B. 690 Would Grant Businesses Unacceptably Wide Latitude to Wiretap and Surveil Consumers

According to proponents,[2] the intent of this legislation is to reduce the amount of lawsuits filed against businesses under CIPA that have leaned on the theory that a variety of internet tracking technologies (e.g. cookies, pixels, tags, and beacons) constitute illegal wiretapping, or pen-register or trap and trace devices, especially when businesses don't obtain affirmative consent before employing them.

However, in attempting to eradicate any current and future cases brought under that theory, S.B. 690 seeks to amend CIPA to exempt *any* type of wiretapping, eavesdropping, and interception of communication when carried out for *any* "commercial business purpose."[3] Under the bill, commercial business purposes are defined as processing of personal information in a manner that is consistent with, but not necessarily for, either furthering a "business purpose" as defined under Section 1798.140 of CCPA, or that is subject to a consumer's opt-out rights under CCPA.[4]

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.
[2] See, e.g., Senate Public Safety Committee Analysis, (pgs. 6-7) https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202520260SB690#
[3] Section 1(b)(4), Section 2(e)(5), Section 3(b)(4), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB690
[4] Section 5(e)

These allowances are extremely broad in scope and would create loopholes that would open the door for surveillance far beyond what is currently allowed by law.

For instance, authorized business purposes under Section 1798.140 of CCPA include the use of personal information for first-party "advertising or marketing services" or "internal research." That means that under this legislation, a phone company would be able to secretly listen in on an individual's phone conversations for the purposes of serving them targeted advertisements. A social media company could quietly create a backdoor to allow employees to read encrypted messages between users to help them tweak their algorithm to keep people on their platform. Or a smart TV or home speaker could surreptitiously listen to all the conversations in your home to help train their next AI system. While experts have long disputed the widespread notion that people's phones are "listening to them" (companies collect so much data through regular commercial transactions that they already know more about you than your closest friends and family),[5] S.B. 690 would take the dubious step of blessing that behavior under state law.

Furthermore, under S.B. 690 companies that wish to wiretap or record the private conversations of individuals for the purposes of *selling* that information or using it for cross-context targeted advertising (neither of which are authorized business purposes) can do so as long as they provide consumers an opportunity to opt out. This would represent another major blow to any remaining notion of privacy online and in the physical world. Our every phone call, text message, or even utterance in a public place could be secretly recorded, added to an all-encompassing profile about us, and then sold to the highest bidder for marketing or other purposes. And if the underlying concept behind that proposal isn't alarming enough, the supposed guardrail of providing the consumer an opportunity to opt out is nonsensical. How are consumers supposed to opt out of wiretapping that *by definition* is occurring without their knowledge?

Mass Collection of Individuals' Private Communications Creates Unacceptable Risk

Even if companies don't use the contents of individuals' private communications for unwanted internal or commercial purposes, the mass collection of this data for *any* purpose is incredibly dangerous on its own. If our private communications are lost to cybercriminals in a data breach, collected by data brokers, or otherwise obtained by bad actors, they can easily be weaponized against individuals in ways that directly threaten their physical safety, health, or bodily autonomy.

As an example of how easily our sensitive data can be leaked, California's health insurance website, Covered California, was recently revealed to have shared web visitors' confidential information, such as whether they are pregnant, transgender, or victims of domestic abuse to social media companies like LinkedIn, claiming an accidental website misconfiguration.[6] Unfortunately, once our private information is propagated to third-parties, there is very little we

[5] See, e.g., Shira Ovide, Washington Post, "Is your phone listening to you? Yeah, but probably not to target ads," (January 7, 2025), https://www.washingtonpost.com/technology/2025/01/07/phone-listening-target-ads-iphone-siri/
[6] Tomas Apodaca and Colin Lecher, CalMatters, How the state sent Californians' personal health data to LinkedIn, (April 28, 2025), https://calmatters.org/health/2025/04/covered-california-linkedin-tracker/

can do to claw it back. At a time where agencies of the federal government are actively hunting down individuals based on information collected from businesses about their political beliefs, religious affiliations, or health decisions, we cannot risk sharing even more sensitive information with them. The legislature should be doing all it can to prevent the additional outward flow of personal data, not enabling even more collection.

Conclusion

Irrespective of its stated intent, S.B. 690 gives the greenlight to dystopian corporate surveillance practices, which will endanger the privacy and safety of all Californians, with very little guardrails to prevent abuse. Allowing businesses to secretly wiretap, record, or intercept the communications of individuals for their own businesses purposes fundamentally contravenes the purpose of CIPA, as well as the California constitution, which recognizes individuals' inalienable right to privacy. For the above reasons, we must oppose S.B. 690 and urge the Legislature to reject it.

Sincerely,

Matt Schwartz
Policy Analyst
Consumer Reports