



COST DRIVER

June 11, 2026

TO: Members, Senate Privacy, Digital Technologies, and Consumer Protection Committee

SUBJECT: **AB 2564 (WARD) SURVEILLANCE PRICING
OPPOSE/COST DRIVER – AS AMENDED APRIL 16, 2026
SCHEDULED FOR HEARING - JUNE 15, 2026**

The California Chamber of Commerce and the undersigned respectfully **OPPOSE AB 2564 (Ward)** as amended on April 16, 2026, as a **COST DRIVER**, because it will outlaw a vast range of existing, consumer-friendly discounts and force businesses to fit their discounts into limited, permissible categories or face lawsuits. In addition, **AB 2564** creates new disclosure standards, different from California's existing law on data collection and usage, the California Consumer Privacy Act (CCPA), as well as the CCPA's implementing regulations. Moreover, **AB 2564** uses undefined and ambiguous terms, meaning it will be difficult for employers to ascertain whether they are in compliance with its language without litigation. Because **AB 2564** is enforced via legal action by private citizens or by state and local prosecutors, we expect these vagaries to add considerable litigation costs for businesses who are simply trying to offer long-standing discounts to consumers.

To be clear: we do not support any targeted price increases based on protected characteristics. Moreover, *none of our members utilize any such targeted price increases*. However, we are very concerned that **AB 2564** will place civil penalties and litigation on non-problematic and widely-accepted practices (such as membership rewards programs or local discounts) because of its overbroad language, while banning permissible uses of data under the CCPA.

Throughout the 2025 legislative session, we offered amendments to protect existing discounts and practices related to this bill's precursor, **AB 446 (Ward – 2025)**, while still prohibiting businesses from using the personal identifiable information of a consumer to raise the price of goods for an individual or group of consumers. Similarly, this year, we have offered amendments to exempt discounts from the bill (similar to Maryland's recently-passed law on this topic) but they have been refused.

Context: AB 2564 Outlaws Offering Different Prices—including Discounted Prices—Based on Any Sort of Data.

AB 2564 prohibits “surveillance pricing,” which it loosely defines as “offering or setting a customized price¹ for a good or service for a specific consumer or group of consumers, based, in whole or in part, on personally identifiable information collected through electronic surveillance technology...” (emphasis added)

Notably, “electronic surveillance technology” is not actually defined in **AB 2564**. Instead, the bill only provides a list of examples that are “included,” but no description that would help a covered entity determine if the bill applied to the consumer information in their possession. A metaphor helps illustrate the problem

¹ “Customized price” is undefined in **AB 2564**.

with definitions that only say what they “include.” Imagine trying to define what is a “pet” - but the only definition is “Pets includes dogs or cats.” Such a definition provides no helpful guidance for anything not listed, such as bird or fish. Are those “pets?” Without a descriptive definition, it is impossible to know. Under **AB 2564**, the term “electronic surveillance technology” has the same problem – the definition does not describe what makes something an electronic surveillance technology. Instead, it only provides examples. Without a descriptive definition, employers will be left guessing what technologies are or are not covered by the bill.

This undefined term “electronic surveillance technology” is then relied upon in the bill’s central definition (“surveillance pricing,” see above quotation), meaning that the central concept of the bill remains functionally undefined.

Importantly, **AB 2564**’s definition of surveillance pricing prohibits not just cost increases, but also any discounts offered to consumers based on any personal data.² To enforce its provisions, **AB 2564** then relies on litigation (by individuals, the attorney general, or local prosecutors).

1) AB 2564 Outlaws Consumer-Friendly Discounts – and Will Hurt Affordability Across California by Creating Litigation Risks for Businesses That Offer Discounts.

AB 2564 creates the following three-step process:

- Step (1) - Any difference³ in price (including discounts) is presumptively banned as “surveillance pricing” (Section 7200(e)(2) / 7202(a));
- Step (2) – Companies must prove that their discount meets one of four⁴ listed exceptions in order to be offered (Section 7202(b)(1) / 7202(b)(2)(A)(i-iii)); and
- Step (3) – For the three allowable types of discounts, businesses must then prove that their discount meets the additional requirements of subsections 7202(bb)(2)(B)(i) and (ii).

We are greatly concerned that California businesses will be sued because of **AB 2564**’s presumptive outlawing of all discounts, limited exceptions, and ability for private or local prosecutorial enforcement. Forcing companies to litigate their ability to offer discounts seems unlikely to improve affordability in California and will certainly chill companies’ willingness to offer discounts to their customers. Applying **AB 2564**’s process illustrates this reality.

Step 1 outlaws all changes to price based on personal information, meaning that any business attempting to offer targeted discounts (such as for local residents or former subscribers) will always start on the defensive in any lawsuit pursuant to **AB 2564**. In simple terms – any discounts they offer in a targeted sense will be presumptively a violation of law and expose them to significant penalties. As noted above, **AB 2564** does not actually contain a definition of what constitutes “electronic surveillance technology” in any functional way. As a result, we read **AB 2564** as applying to all consumer data.

Then, under Step 2, employers will need to consider whether their present discounts fit into the listed permissible exceptions. If not, they would need to potentially eliminate those discounts. And even if they believe that their discounts could qualify - the company still has to weigh the costs and risks of litigation to defend their discounts. We expect this to cause many businesses to: (a) stop offering discounts which do not easily fit **AB 2564**’s vague terms; (b) choose to cancel even potentially compliant discounts because the cost of potential litigation and shakedown demand letters is too great.

These litigation risks are particularly significant when the applicable language is vague, and therefore impossible for employers to ensure compliance with. For example: the first purported exemption for discounts in **AB 2564** contains two clauses that combine to render the exemption functionally useless. First,

² Our coalition offered repeated amendments last year to clarify that the bill should prohibit only price increases based on personal data, but they were not accepted.

³ The bill prohibits any “customized” prices that are “based ... on [personal] information collected through electronic surveillance technology.” Though “customized” is also undefined, it would presumably include both price increases or price decreases.

⁴ The first exception – 7202(b)(1) – “difference in price based solely on costs” – is not traditionally considered a “discount” at all, and is not at issue. Functionally, the other three exceptions are the only relevant language to analyze (7202(b)(2)(A)(i-iii)), as they will now govern all discounts in California.

it contains three different standards for disclosure of discounts ... in one sentence.⁵ Second, though it attempts to allow for discounts based on “eligibility criteria,” it then provides that such criteria must be of such a nature that “any consumer could potentially meet [them].” In reality, criteria for a discount may not be something which every customer might qualify for. These drafting vagaries make **AB 2564**’s first so-called “discount exemption” functionally unusable for employers.

Step 3’s requirements then function to make it even harder for retailers to offer discounts and avoid liability in California. Pursuant to Step 3, retailers must be able to prove that every eligibility criteria for every discount, and every discount is clearly and conspicuously disclosed on their website. The scale of this task is critical to understand: retailers across California may have thousands of discounts for their rewards members at a single store, and those may differ regionally based on availability of goods, freshness of goods, and other factors.⁶ In simple terms – if the strawberries are getting old, and a new batch has arrived, a grocer may wish to implement a quick discount at one store for members in order to clear those shelves. But under **AB 2564**, if the grocer fails to update the price of strawberries at that one store for that one-day deal, they will be in violation of **AB 2564**.

Now, consider the number of products in a single aisle of a grocery store ... and apply the same process ... for thousands of retail locations across California. And remember – if a retailer fails to keep every discount “clearly and conspicuously disclosed” – then they are subject to penalties of \$12,500 per transaction.⁷ The simple math of risk to reward here – selling a few more strawberries before they spoil vs a fine of \$12,500 per transaction – will push retailers to avoid such beneficial discounts to avoid the risk of massive liability.

To the extent the author intends to prevent targeting of individuals or groups based on personal information with price increases – we completely understand and agree that such targeted price increases should be (and usually already are) illegal – but **AB 2564** goes far beyond that noble goal. As noted above, we have offered amends to clarify that the bill is intended to prevent businesses from targeting individual consumers with higher prices, but they were not adopted in last year’s **AB 446** or integrated into **AB 2564**.

2) AB 2564 Contradicts California’s Landmark Privacy Law – the California Consumer Privacy Act – by Creating New Consent and Disclosure Requirements, as Well as New Limitations on Data Usage.

The California Consumer Privacy Act⁸ is the definitive statute related to consumers’ privacy and their personal data – whether that data is collected online, in brick-and-mortar stores, by technological means, on paper, or by powers of observation. It is a broad, technology-neutral, industry-neutral, and comprehensive consumer data protection law, which was also voter-approved via Proposition 24 in 2020. Substantively, the CCPA governs how a covered business may collect data related to a customer’s behavior (such as buying certain products) and utilize that data. The CCPA also already addresses permissible and impermissible business uses of consumer data for activities such as targeted advertising, loyalty and rewards programs, and the like. In fact, the CCPA places limits on the selling or sharing of customers’ data, allowing customers to opt-out of allowing a business to sell or share such data.⁹ In fact, as strengthened

⁵ Specifically, subsection 7202(b)(2)(A)(i) requires any discount price be “based on publicly disclosed eligibility criteria...” and then adds three different disclosure requirements in the following sentence: “The terms and criteria for receiving the discounted price shall be (1) conveyed (sic) clearly and conspicuously disclosed (2) in clear and prominent terms (3) in such a manner that an ordinary consumer would notice and understand them.” (numerals and underline added for emphasis)

⁶ In addition, we believe this difficulty is even more substantial for small retailers – who do not have the staff to actively update their website on a regular basis – and would therefore face even greater hurdles in offering discounts under **AB 2564**.

⁷ Section 7204(a)(1)(A).

⁸ See Cal. Civil Code Section 1798 *et seq.*

⁹ See Cal. Civil Code Section 1798.140(e) (defining “Business purpose” use of data and identifying specific uses of data as acceptable).

by voters through Proposition 24, the CCPA also grants consumers the right to further limit the use and disclosure of their sensitive personal information — including precise geolocation data.¹⁰

Despite the CCPA's coverage of such programs, **AB 2564** requires different opt-in consent from the CCPA's provisions that govern all existing loyalty programs. The CCPA provides that "a business may enter into a financial incentive program only if the consumer gives the business prior opt-in consent ... [the agreement to opt-in must] clearly describes the material terms of the [program], and which may be revoked by the consumer at any time."¹¹ In other words: the CCPA already squarely addresses the consent necessary for a loyalty program – and we are unaware of any justification from **AB 2564**'s proponents as to why this consent standard has proved insufficient.¹² Still, despite lacking any apparent justification for the change, **AB 2564** puts contradictory language¹³ into law without amending the terms of the CCPA.

3) Concerns Over Use of Third-Party Data Triggering Liability.

We also have concerns over **AB 2564** creating liability for businesses that purchase data but are unaware that it was collected using electronic surveillance technology,¹⁴ and still face liability. The proposed language contains no mental state or intent requirement for a violation – and defines surveillance pricing broadly, to also include "personally identifiable information collected through electronic surveillance technology that is gathered, purchased, or otherwise acquired from a third party." As we read this language, it seems to provide that a retailer purchasing data (to confirm eligibility for a discount) from a third party would be potentially liable if the third party gathered the data using electronic surveillance technology, regardless of whether the purchaser was aware of that fact. In simple terms: this seems to create pass-through liability that could catch even good-faith actors who believe they purchased non-covered data.

Conclusion

While we appreciate and support the intention of this bill — to ensure California consumers are treated fairly and without discrimination — we are very concerned by its infringement upon the CCPA, and the collateral damage that its broad language will have for California retailers as they attempt to compete and offer discounts for consumers. We look forward to working with the author – as we did on last year's **AB 446** – but, for these reasons, we must **OPPOSE AB 2564 (Ward)** as a **COST DRIVER**.

Sincerely,



Robert Moutrie
Vice President for Policy Advocacy
on behalf of

Association of National Advertisers, Jonathan Arambel
Building Owners and Managers Association of California, Skyler Wonnacott
California Business Properties Association, Skyler Wonnacott
California Chamber of Commerce, Robert Moutrie
California Fuels + Convenience Alliance, Alessandra Magnasco

¹⁰ Specifically, consumers may limit a business's use of such sensitive personal information to uses necessary to perform the services or provide the goods reasonably expected by an average consumer requesting them, or to certain limited "business purposes," such as ensuring security or short-term transient uses, including non-personalized advertising shown as part of a consumer's current transaction with a business. (See Civ. Code Sec. 1798.121.)

¹¹ See Cal. Civil Code Section 1798.125(b)(3).

¹² To the contrary, all publicly provided justifications for **AB 2564** - such as the bill's initial legislative findings, which were removed after our prior letter questioned their accuracy - have focused on allegations of secretive pricing targeting individuals ... and not criticized consent standards for loyalty programs in any way.

¹³ To be specific: **AB 2564** includes standards of disclosure in 7202(b)(2)(B)(i) that are applicable to any allowed forms of discounts, including the incentive programs that are specifically covered under the CCPA.

¹⁴ As noted above, though the definition that **AB 2564** creates for electronic surveillance technology is incredibly broad and are uncertain if any data is actually excluded from the definition at present – the issue of pass-through liability remains critical in case the definition is tightened in future amendments.

California Grocers Association, Rachael O'Brien
California Restaurant Association, Marlon Lara
California Retailers Association, Ryan Allain
Civil Justice Association of California, Annalee Augustine
Greater Conejo Valley Chamber of Commerce, Josh Gray
Greater San Fernando Valley Chamber of Commerce, Nancy Hoffman Vanyek
Internet.Works, Austin Heyworth
NAIOP California, Skyler Wonnacott
Orange County Business Council, Amanda Walsh
TechNet, Jose Torres
USTELECOM, The Broadband Association, Yolanda Benson

cc: Legislative Affairs, Office of the Governor
Charles Loudon, Office of Assemblymember Ward
Christian Kurpiewski, Chief Consultant, Senate Privacy, Digital Technologies, and Consumer
Protection Committee
Emilye Reeb, Consultant, Senate Republican Caucus