Date of Hearing: April 14, 2026

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
AB 2564 (Ward) – As Amended March 23, 2026

As Proposed to be Amended

SUBJECT: SURVEILLANCE PRICING

KEY ISSUE: SHOULD CALIFORNIA PROHIBIT BUSINESSES FROM USING SURVEILLANCE-DERIVED DATA TO VARY PRICES BETWEEN CONSUMERS FOR THE SAME GOOD OR SERVICE, SUBJECT TO NARROWLY DEFINED EXCEPTIONS, IN ORDER TO PREVENT OPAQUE AND DISCRIMINATORY PRICING PRACTICES?

SYNOPSIS

This bill prohibits the practice of "surveillance pricing," whereby a business offers or sets a customized price for a good or service for a specific consumer or group of consumers based on personal or aggregate data collected through electronic surveillance technology. The bill targets a growing pricing model that uses data such as location, browser history, device usage, or behavioral profiling to infer a consumer's willingness or ability to pay and adjust prices accordingly—often without the consumer's knowledge. In response to this practice, last year the author introduced AB 446 (Ward, 2025), which prohibited "surveillance pricing" and authorized a private right of action to enforce against a violation. AB 446 passed out of this Committee before being significantly amended in the Senate. This year, the author has introduced AB 2564 which is substantially similar to AB 446. Of particular relevance to this Committee, the bill differs from the previous version in that it authorizes enforcement by a public prosecutor only. As currently in print, the bill incorporates enforcement by a public prosecutor using outdated language. The author is proposing amendments to streamline and update the enforcement language, incorporated into the SUMMARY and discussed in the analysis.

This bill is sponsored by Consumer Reports, TechEquity, and Consumer Watchdog. It enjoys broad support from consumer protection advocates, labor unions, and various other nonprofit organizations. It is opposed by business and industry advocates, including the California Chamber of Commerce, who contend that the bill is overbroad and may result in retailers being unable to provide discount programs generally.

This bill was previously heard by the Committee on Privacy and Consumer Protection where it was approved on a vote of 10-4.

SUMMARY: Prohibits retailers from engaging in surveillance pricing. Specifically, **this bill**:

1) Defines all of the following for purposes of the bill:

    a) "Discounted price" means a price that is verifiably lower than the widely available and publicly disclosed bona fide market price;

    b) "Electronic surveillance technology" includes the use of technological methods, systems, or tools, including, but not limited to, sensors, cameras, device tracking, or biometric

monitoring, that are capable of gathering personally identifiable information about a consumer's behavior, characteristics, location, or other personal attributes, whether in physical or digital environments;

c) "Personally identifiable information" has the same meaning as "personal information" as defined in paragraph (1) of subdivision (v) of section 1798.140 of the Civil Code and any regulations promulgated thereunder;

d) "Retailer" has the same meaning as that term is defined in Section 6015 of the Revenue and Taxation Code.

e) "Surveillance pricing" means offering or setting a customized price for a good for a specific consumer or group of consumers, based, in whole or in part, on personally identifiable information collected through electronic surveillance technology, including personally identifiable information collected through electronic surveillance technology that is gathered, purchased, or otherwise acquired from a third party. "Surveillance pricing" does not include a discounted price offered to a consumer terminating or taking steps to terminate a service or membership with a person, but does include offering random variations in prices to different customers using a website, mobile application, or comparable online technology.

2) Prohibits a retailer from engaging in surveillance pricing, except as specified.

3) Specifies that a retailer does not engage in surveillance pricing if either of the following apply:

a) The difference in price is based solely on costs associated with providing the good to different consumers;

b) The retailer offers a discounted price that complies with the requirements in c), below, and any of the following apply:

i) A discounted price is offered based on publicly disclosed eligibility criteria that any consumer could potentially meet, including, but not limited to, signing up for a mailing list, providing personal information registering for promotional communications, or participating in a promotional event. The terms and criteria for receiving the discounted price shall be conveyed and clearly and conspicuously disclosed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand them;

ii) A discounted price is offered to members of a broadly defined group, including, but not limited to, teachers, active or retired military, senior citizens, students, or residents of a certain area based on publicly disclosed eligibility criteria;

iii) A discounted price is offered through a loyalty, membership, or rewards program that consumers affirmatively purchase or enroll in.

c) Requires the current eligibility criteria, available discounts, and any conditions for receiving or earning the discounted price to be clearly and conspicuously disclosed on the

company's internet website, and requires the discounted price to be uniformly offered or made available to all consumers who meet the disclosed eligibility criteria.

4) Authorizes the Attorney General, a city attorney, or a county counsel to bring a civil claim against a retailer who violates this bill's provisions for the following civil penalties, with each violation with respect to an individual consumer or transaction involved constituting a distinct violation:

   a) A civil penalty not to exceed $12,500;

   b) For a retailer that intentionally violates the bill, a civil penalty no greater than three times the amount of the penalty assessed, above, and all revenues earned from the violation.

   c) Reasonable attorney's fees and costs.

5) Authorizes a consumer to bring an action for injunctive relief as necessary to enforce this bill and to remedy any violations of its provisions and recover reasonable attorney's fees and costs.

6) Makes any waiver of this part against public policy and void and unenforceable.

7) Includes a savings clause.

EXISTING LAW:

1) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (California Constitution Article 1 Section 1.)

2) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. Places attendant obligations on businesses to respect those rights. (Civil Code Section 1798.100 *et seq*.)

3) Defines the following terms under the CCPA:

   a) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes such information as:

      i) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.

      ii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

      iii) Biometric information.

iv) Internet activity information, including browsing history and search history.

v) Geolocation data.

vi) Audio, electronic, visual, thermal, olfactory, or similar information.

vii) Professional or employment-related information. (Civil Code Section 1798.140 (v).)

b) "Sensitive personal information" means personal information that reveals a person's:

i) Social security, driver's license, state identification card, or passport number.

ii) Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials.

iii) Precise geolocation.

iv) Racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

v) Email, mail and text messages.

vi) Genetic data.

vii) Information collected and analyzed relating to health.

viii) Information concerning sex life or sexual orientation. (Civil Code Section 1798.140 (ae).)

4) Establishes the California Privacy Protection Agency (Privacy Agency) and vests it with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. (Civil Code Section 1798.199.10.)

5) Establishes the Unfair Practices Act (UPA), which is intended to safeguard the public against the creation or perpetuation of monopolies and to foster and encourage competition by prohibiting unfair, dishonest, deceptive, destructive, fraudulent, and discriminatory practices by which fair and honest competition is destroyed or prevented. (Business and Professions Code Section (BPC) 17000 *et seq*.)

6) Provides that the secret payment of allowances of rebates, refunds, commissions, or unearned discounts, whether in the form of money or otherwise, or secretly extending to certain purchasers special services or privileges not extended to all purchasers upon like terms and conditions, to the injury of a competitor and where such payment or allowance tends to destroy competition, is unlawful. (BPC Section 17045.)

7) Establishes a general prohibition on unfair competition, known as the Unfair Competition Law (UCL), which covers any unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue, or misleading advertising, and any act prohibited under the False Advertising Law. (BPC Section 17200.)

8) Defines "retailer" to include every seller who makes any retail sale or sales of tangible personal property, and of making retail sales at auction of tangible personal property owned by the person or others; every person engaged in the business of making sales for storage, use, or other consumption or in the business of making sales at auction for tangible personal property owned by the person or others for storage, use, or other consumption; any person conducting a race meeting under the specified provisions of the Business and Professions Code, with respect to horses which are claimed during such meeting. (Revenue and Taxation Code Section 60158.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: Over the past decade, advances in artificial intelligence, machine learning, and data collection technologies have given rise to a new and largely unregulated pricing model known as surveillance pricing—a form of individualized price discrimination in which businesses use real-time consumer data to set different prices for the same good or service based on a consumer's perceived willingness or ability to pay. This data may include the consumer's location, device type, browsing history, financial characteristics, or behavioral profile. The price is then algorithmically adjusted to maximize the seller's profit from that individual consumer.

While California law provides some of the strongest privacy protections in the nation through the California Consumer Privacy Act (CCPA), existing law does not restrict businesses from using lawfully collected consumer data to change their internal pricing. The CCPA was designed to increase transparency and give consumers control over their data—but it does not prohibit a business from using that data to charge a consumer more, as long as that practice is disclosed or purportedly tied to the "value provided" by the data. In practice, this creates a loophole that permits forms of digital economic discrimination. This measure seeks to address that problem. According to the author:

> With the rise of artificial intelligence and data collection, businesses increasingly use personal data to set prices, often leading to unfair and discriminatory pricing practices. This legislation aims to establish safeguards that ensure transparency, fairness, and consumer protections in pricing algorithms. AB 2564 will prohibit the practice of surveillance pricing by making it unlawful for businesses to use personal data when charging different prices for the same product, or service whether online or during in-store checkout.

The problem & legal background. Surveillance pricing—the practice of using real-time consumer data to adjust the price of goods or services for specific individuals—has emerged as a pervasive and largely unregulated feature of the digital economy. Enabled by advances in artificial intelligence, biometric surveillance, and algorithmic profiling, this pricing model allows businesses to extract maximum profit from each consumer based not on market conditions or product costs, but on a predictive assessment of the consumer's personal habits, financial capacity, or perceived willingness to pay.

Surveillance pricing is distinct from traditional dynamic pricing, in which prices change uniformly for all consumers based on time, demand, or inventory. Instead, surveillance pricing relies on individualized inputs such as browsing history, ZIP code, geolocation, device type, demographic data, purchase patterns, and even biometric characteristics. These data points—collected through cookies, mobile apps, facial recognition, or sensor-equipped shelves—are

analyzed to generate behavioral profiles and assign different prices to different consumers for the same product or service.

Real-world examples illustrate the risks. In 2022, the County of San Diego settled a $5 million lawsuit against Target Corporation for using consumers' location data to increase online prices when a customer physically entered a store's parking lot—without clear disclosure. (Associated Press, *Target pays $5 million to settle California pricing lawsuit*, Dec. 6, 2022, *available at* https://apnews.com/article/technology-business-lawsuits-california-target-corp-35db1e4f1ea1d43ef7a1f7f2b4630c41.) In January 2025, the Federal Trade Commission (FTC) released findings from its surveillance pricing inquiry, revealing that over 250 businesses had adopted systems capable of using personal data to algorithmically tailor prices. (FTC Press Release, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices*, Jan. 29, 2025 *available at* https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.) Former FTC Chair Lina Khan noted that retailers routinely rely on "a person's location and demographics, down to their mouse movements on a webpage," to determine individualized prices. (*Id.*) Investigative reporting from *SF Gate* further confirmed that major hotel booking websites offered Bay Area consumers rates up to $500 higher than identical listings shown to users in less affluent cities—despite identical booking parameters. (SF Gate, *Hotel sites quietly raising prices based on your location*, January 12, 2025, *available at* https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.)

While companies claim that such models improve pricing efficiency, critics argue that surveillance pricing redistributes consumer surplus entirely to the seller—leaving buyers with diminished bargaining power and no visibility into the pricing algorithm. The result is a non-transparent and inequitable digital marketplace in which consumers may unknowingly pay more based on private inferences drawn from their data profiles.

Despite California's strong consumer privacy framework under the CCPA and the California Privacy Rights Act of 2020, existing law does not prohibit surveillance pricing. The CCPA provides consumers with rights to opt out of the sale or sharing of their personal information (Civil Code Section 1798.120) and mandates notice at collection (Civil Code Section 1798.100). However, it also permits businesses to charge different prices to consumers based on the "value provided to the business by the consumer's data" (Civil Code Section 1798.125 (b)), a provision that may inadvertently authorize surveillance pricing as long as the practice is disclosed. The absence of substantive legal limits on these practices leaves consumers with little recourse. Surveillance pricing often operates invisibly, making it difficult for consumers to detect that they are being charged more than others. There is no obligation for companies to disclose individualized pricing, no way for consumers to compare prices offered to others, and no regulatory mechanism to prevent price discrimination based on income, race, geography, or inferred behavior.

In the absence of legislative intervention, surveillance pricing risks becoming the industry default—deepening inequality, normalizing digital redlining, and undermining consumer trust in fair market practices.

Last year, the Legislature considered AB 446 (Ward, 2025), which was substantially similar to the current measure when presented to this Committee. When heard by this Committee, AB 446

prohibited any person from engaging in surveillance pricing, which was defined as "offering or setting a customized price for a good or service for a specific consumer or group of consumers, based, in whole or in part, on covered information collected through electronic surveillance technology." In other words, the bill prohibited businesses from determining the price of a good or service based, in whole or in part, by the consumer's personal data gathered by electronic surveillance technology. The bill also included four exemptions to the prohibition: when the difference in price is based solely on costs associated with providing the good or service to different consumers; when a discounted price is offered based on publicly disclosed eligibility criteria such as signing up for a mailing list; when the discounted price is offered to members of a broadly defined group such as teachers or veterans; and when the discount is offered through loyalty or membership rewards programs that require affirmative enrollment.

Of particular relevance to this Committee, AB 446 made a person who impermissibly engaged in surveillance pricing liable in a civil claim brought by a consumer for a civil penalty of up to $12,500 per violation for each consumer and transaction. The bill also made a person who intentionally violated its provisions liable for a civil penalty up to three times the underlying civil penalty and disgorgement, and attorneys fees and costs, and injunctive or declaratory relief. AB 446 was substantially amended in the Senate, and in its final form only applied to grocery establishments and only authorized enforcement by public prosecutors, before the author shelved it on the Senate floor.

This bill picks up where AB 446 left off when it was before the Assembly. While substantially similar to that measure, it varies slightly in that it explicitly prohibits *retailers* from engaging in surveillance pricing. It is possible that this change does not make a substantial difference in practice, as the only entities (or persons) authorizing a price, whether lower or higher, would be retailers of one form or another. Like AB 446, this bill also specifies that a retailer does not engage in surveillance pricing if either the price distinction is based only on the cost difference to provide the good to difference consumers or the different price is essentially a rewards program or mailing list discount, or discount for a broadly defined group of people, such as veterans or teachers, and meets specified requirements.

Additionally, where AB 446 authorized a private right of action against a business that engaged in surveillance pricing, AB 2564 primarily authorizes public prosecutors to bring claims against retailers who engage in surveillance pricing. A successful claim entitles the public prosecutor to a civil penalty of $12,500 per violation, with each violation with respect to an individual consumer or transaction constituting a distinct violation. In other words, if a single consumer buys five products from a single retailer, if that retailer modifies the price of each of those products using the consumer's information, that single transaction could give rise to five distinct violations. Additionally, the bill authorizes a court to award treble damages and disgorgement against a retailer that intentionally violates the bill's requirements.

Acknowledging that private individuals may be best positioned to raise an alarm and stop future harms of this nature, the bill also authorizes private individuals to bring a claim. However, AB 2564 strikes a balance between acknowledging consumers' firsthand knowledge of potential violations against the feasibility of expansive litigation by only authorizing private individuals to seek injunctive relief and a recovery of attorney's fees and costs.

As currently in print, this bill authorizes the Attorney General, any district attorney, any city attorney of a city having a population in excess of 750,000, any city attorney of a city and

county, or, with the consent of the district attorney, a city prosecutor in any city having a full-time city prosecutor, to bring file suit. This language reflects outdated language that is no longer commonly used by this Committee to authorize public prosecutor enforcement. To align this provision with current practice and to generally streamline the provision but achieve the same effect, the author proposes the following amendment:

> **7204.** ~~(a) Except as provided under subdivision (b), actions pursuant to this part may only be brought by the Attorney General, by any district attorney, by any city attorney of a city having a population in excess of 750,000, by a county counsel of any county within which a city has a population in excess of 750,000, by any city attorney of any city and county, or, with the consent of the district attorney, by a city prosecutor in any city having a full-time city prosecutor, in any court of competent jurisdiction.~~ ***A retailer who violates this part shall be liable for the following penalties, upon a civil action brought by the Attorney General, a city attorney, or a county counsel, with each violation with respect to an individual consumer or transaction constituting a separate and distinct violation:***
>
> ~~(1) In addition to any other remedy at law, a retailer that violates this part shall be liable for the following civil penalties, which shall be assessed and recovered in a civil action brought pursuant to this subdivision:~~
>
> (A) A civil penalty not to exceed twelve thousand five hundred dollars ($12,500) ~~for each violation, with each violation of this part constituting a separate violation with respect to each consumer or transaction involved.~~

Opposition. As with its predecessor, AB 2564 has significant opposition from the business sector, including the Chamber of Commerce and TechNet. As a threshold issue, they contend the language is overbroad and insufficiently defined. In particular they point out that while the bill prohibits surveillance pricing, which is then defined by determining a price based, in whole or in part, on a consumer's information collected through "electronic surveillance technology," "electronic surveillance technology" is not itself defined but is instead explained by a list of technologies that constitute electronic surveillance technology. This is a common statutory drafting practice to indicate the types of circumstances of particular relevance to the bill in question where the environment itself may be changing – such as technology.

Additionally, the coalition raises concerns that the bill contradicts the California Consumer Privacy Act "by creating new consent and disclosure requirements, as well as new limitations on data usage." As a threshold matter, this bill does not modify the CCPA. As explained in the analysis for this bill from the Assembly Committee on Privacy and Consumer Protection, even if the disclosure requirement in AB 446 overlaps with privacy-related concepts, the CCPA operates as a regulatory floor—not a ceiling. Section 25(a) of Proposition 24 expressly grants the Legislature the authority to amend the CCPA by a majority vote, provided that the amendments are consistent with and further the purpose and intent of the CCPA. In this regard, Section 3 of the Proposition provides "it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional right privacy." Since the passage of Proposition 24, the Legislature has amended the CCPA to expand privacy protections in several bills.

Enforcement concerns. The opponents broadly contend that the bill "will hurt affordability across California by creating litigation risks for businesses that offer discounts. […] 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." In other words, the Chamber of Commerce and coalition members seem to believe that authorizing public prosecutors to bring claims against businesses that engage in *any* form of discount programs will force businesses to either stop offering the discounts all together or cancel "even potentially compliance discounts because the cost of potential litigation and shakedown demand letters is too great." The Chamber provides an example that a grocery store seeking to sell strawberries before they spoil by selling them at a lower price may opt not to do so because the risk of litigation and a potential penalty of up to $12,500 per transaction is too great.

To be sure, if selling strawberries on the verge of spoiling triggered a penalty of $12,500, it would be reasonable to conclude that such massive liability could lead to grocers simply tossing those strawberries instead. However, a grocer who opts to decrease the cost of strawberries that may be about to spoil would not be engaging in surveillance pricing because the decision is not based on a potential shopper's data but rather the age of the strawberries. A grocer in this scenario would likely make the decision regardless of who may shop at the store that day. Thus, the grocer would have a strong argument that this "discount" does not fall under the bill's scope. Moreover, while the risk of litigation under AB 446, including the potential risk for unviable claims such as the strawberry scenario, may have been higher due to that version's authorization of a private right of action, it seems the author has opted to take a narrower approach by only authorizing enforcement by public prosecutors. Public prosecutors, who both bring and defend claims involving their city or local government, are already overworked with limited resources. It seems more likely that a public prosecutor would only bring a claim to enforce against an egregious violation that they are fairly certain they can prevail on.

ARGUMENTS IN SUPPORT: This bill is sponsored by Consumer Reports, TechEquity, and Consumer Watchdog. It enjoys broad support from consumer protection advocates, labor unions, and various other nonprofit organizations. In support of the measure, the sponsors submit:

> Surveillance pricing, also sometimes referred to as "personalized" pricing, is when a company uses personal data that they've gathered about a consumer—like data about their online search history, or inferences about family structure, health conditions, or income—to set the price of a product or the discount offered to a consumer.
>
> If enacted, this bill would make California a leader on affordability. It prohibits surveillance pricing, while protecting transparently offered, non-discriminatory discounts. It builds on California's data privacy and consumer protection statutes, while addressing a gap in the current law. Right now, nothing prohibits businesses from collecting or buying data about individual Californians, and then using that data against them to profile them and charge them a higher price than their neighbor. This bill would address that problem; we encourage an 'aye' vote.
>
> Not long ago, before the rise of online shopping and mass data collection, consumers could shop anonymously, confident that the price tag they saw on the shelf wasn't influenced by the store's knowledge of their family, shopping habits, online browsing, ability to pay, or any particular situation that could increase their urgency to purchase. That is no longer the case.
>
> Companies can gather data on consumers' purchase histories, speed of click through, history of clicks, search history, 'likes' on social media, geolocation, IP address, device type, and more, to create a detailed portrait of a consumer. They can use artificial intelligence to make

detailed inferences about consumers based on this data. These profiles, combined with technology that enables companies to display different prices to different consumers online—or send discounts on an individualized basis—means that companies have all the tools they need to implement surveillance pricing. Companies can understand when a consumer might be desperate enough to tolerate a higher price or when a loyal customer will keep coming back even in the absence of discounts.

Surveillance pricing can be difficult to detect, because consumers rarely have a view into what information a company has about them, or what the prices they see are based on. Still, enterprising journalists have discovered examples.

● An investigative journalist writing for SFGate looked at the prices offered for a hotel room in Manhattan for a specific date, and varied his operating system, browser, cookies, and location (his computer's IP address). He found that when he changed his IP address from a Bay Area location to locations in Phoenix and Kansas City, the prices dropped by more than $200 per night in one instance, and more than $511 in another instance.

● ProPublica found that test-prep company Princeton Review was offering different prices for its tutoring services depending on a customer's zipcode. The result, they found, was that Asian customers were nearly twice as likely to receive a higher price.

● The Wall Street Journal reported that Orbitz, the travel aggregation company, determined that Mac users spent more per night on hotels than Windows users, and began steering Mac users towards pricier hotels.

● A Minnesota local news site discovered that Target changed the prices displayed on its app for certain products based on whether the customer—and their device—was physically inside a Target store. When the reporters looked at the Target app while inside a store, they found that a Graco car seat was $72 more expensive than when they had been sitting on the far side of the Target parking lot, and a Dyson vacuum was $148 more expensive.

***ARGUMENTS IN OPPOSITION**:* This bill is opposed by business and industry advocates, including the California Chamber of Commerce. They submit:

The California Chamber of Commerce and the undersigned respectfully OPPOSE AB 2564 (Ward) as amended on March 23, 2026, as a COST DRIVER, because it will outlaw a vast range of existing, consumer-friendly discounts and conflicts with 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. We look forward to continuing such discussions this year related to this new vehicle but remain concerned that conflicting and vague language in this bill will lead to litigation and lawsuits for non-problematic discounts.

[…]

1) 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,* 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 purchased 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.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Reports (co-sponsor)
Consumer Watchdog (co-sponsor)
Tech Equity (co-sponsor)
Alliance of Californians for Community Empowerment (ACCE) Action
American Federation of Musicians, Local 7
American Federation of State, County and Municipal Employees, AFL-CIO
California Federation of Labor Unions
California Federation of Teachers
California Food and Farming Network
California Low-income Consumer Coalition
California Nurses Association
California School Employees Association
California Work and Family Coalition
Center for AI and Digital Policy
Center for Democracy and Technology
Center on Policy Initiatives
Consumer Attorneys of California
Consumer Federation of America
Consumer Federation of California

Courage California
Economic Security California Action
Electronic Privacy Information Center (EPIC)
End Child Poverty California Powered by Grace
Equal Rights Advocates
Friends Committee on Legislation of California
Indivisible Ca: Statestrong
Institute for Local Self-reliance
Justice2jobs Coalition
Kapor Center Advocacy
LA Defensa
LAANE (Los Angeles Alliance for a New Economy)
LGBT Tech
Oakland Privacy
Privacy Rights Clearinghouse
Public Law Center
Secure Justice
SEIU California
Sister Warriors Freedom Coalition
Smart - Transportation Division
Tech Oversight California
UDW/AFSCME Local 3930
Ultraviolet Action
Western Center on Law and Poverty

Opposition

Association of National Advertisers
Building Owners and Managers Association of California
California Business Properties Association
California Chamber of Commerce
California Fuels and Convenience Alliance
California Grocers Association
California Retailers Association
Chamber of Progress
Civil Justice Association of California (CJAC)
Connected Commerce Council
Greater Conejo Valley Chamber of Commerce
Greater San Fernando Valley Chamber of Commerce
Internet.works
Naiop California
Orange County Business Council
Technet
Ustelecom - the Broadband Association

Analysis Prepared by: Manuela Boucher-de la Cadena / JUD. / (916) 319-2334