SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

AB 2564 (Ward)
Version: April 16, 2026
Hearing Date: June 15, 2026
Fiscal: Yes
Urgency: No
CK

SUBJECT

Surveillance pricing

DIGEST

This bill prohibits "surveillance pricing," as defined, except as provided.

EXECUTIVE SUMMARY

Companies regularly and systematically collect, analyze, share, and sell the personal information of consumers. While this data collection can provide consumers various benefits, public fears about the widespread, unregulated amassing of personal information have only grown since privacy was made a part of California's Constitution. One particularly troubling area of this systematic data collection is utilization of this information to engage in differential pricing for consumers based on various elements of that information.

This bill prohibits this practice of "surveillance pricing," defined as 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. The bill provides exceptions for the offering of discounted pricing, such as through loyalty programs, where certain conditions are met, such as ensuring transparency about the basis for such discounts. Violations are subject to civil penalties.

This bill is sponsored by Consumer Reports, TechEquity, and the California Federation of Labor Unions. It is supported by a wide array of labor, advocacy, and low-income services groups, including the Western Center on Law and Poverty, Equal Rights Advocates, and LGBT Tech. It is opposed by various industry groups, including TechNet and Chamber of Progress. Should the bill pass out of this Committee, it will next be heard in the Senate Judiciary Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) 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. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

2) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

3) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
    a) the categories of personal information it has collected about that consumer;
    b) the categories of sources from which the personal information is collected;
    c) the business or commercial purpose for collecting, selling, or sharing personal information;
    d) the categories of third parties with whom the business shares personal information; and
    e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)

4) Provides that these provisions do not restrict a business's ability to collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information. (Civ. Code § 1798.145(a)(6).)

5) Defines "personal information" as 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. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and "sensitive personal information." It does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v).)

6) 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. (Bus. & Prof. Code § 17000 et seq.)

7) 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. (Bus. & Prof. Code § 17045.)

8) 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. (Bus. & Prof. Code § 17200.)

This bill:

1) Prohibits "surveillance pricing," defined as 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) Defines other relevant terms, including:
    a) "Electronic surveillance technology" includes the use of technological methods, systems, or tools, including 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.
    b) "Personally identifiable information" has the same meaning as "personal information" in the CCPA.

3) Provides that a person 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 following:
        i. The current eligibility criteria, available discounts, and any conditions for receiving or earning the discounted price are clearly and conspicuously disclosed on the company's website.

ii. The discounted price is uniformly offered or made available to all consumers who meet the disclosed eligibility criteria.
iii. One of the following apply:
    1. A discounted price is offered based on publicly disclosed eligibility criteria that any consumer could potentially meet, including 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 clearly and conspicuously disclosed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand them.
    2. A discounted price is offered to members of a broadly defined group, including teachers, active or retired military, senior citizens, students, or residents of a certain area, based on publicly disclosed eligibility criteria.
    3. A discounted price is offered through a loyalty, membership, or rewards program that consumers affirmatively purchase or enroll in.

4) Provides that a retailer in violation hereof is liable for the following penalties in 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:
    a) A civil penalty not to exceed $12,500, except that intentional violations are subject to a civil penalty no greater than three times the amount of the penalty assessed and all revenues earned from the violation.
    b) Reasonable attorney's fees and costs.
    c) Injunctive or declaratory relief.

5) Authorizes a consumer to bring an action only for injunctive relief as necessary to enforce this part and to remedy any violation, and reasonable attorney's fees and costs.

6) Makes any waiver void and unenforceable.

7) Clarifies that the rights, remedies, and penalties are cumulative to any others.

8) Finds and declares that it furthers the purposes of the CPRA.

COMMENTS

1. Surveillance pricing

Surveillance pricing is a practice where companies collect extensive personal data about consumers to implement individualized pricing strategies. Instead of charging everyone the same price, businesses utilize collected data, often using algorithms to analyze personal information, and set different prices for different customers based on their perceived willingness or ability to pay.

Companies gather data through multiple channels, including purchase history, browsing behavior, location tracking, demographic information, social media activity, and even biometric data. This information gets fed into sophisticated algorithms that create detailed consumer profiles. These profiles predict how much each individual might be willing to pay for a product or service, enabling companies to charge personalized prices that maximize revenue extraction from each customer.

The practice extends beyond simple demographic targeting. Companies can factor in real-time data like current location, the device a consumer is using, shopping patterns, and even a consumer's emotional state inferred from online behavior.

The mass collection of consumer data as an asset is not new, but has rapidly expanded beyond just targeted advertising. This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist, Shoshana Zuboff:

> As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the "normal" economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care, and more. . . .
>
> An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.[1]

[1] Zuboff, Shoshana, *You Are the Object of a Secret Extraction Operation* (November 12, 2021) The New York Times, https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html. All internet citations are current as of June 11, 2026.

Surveillance pricing creates several significant problems for consumers. Most fundamentally, it enables price discrimination that can be both unfair and exploitative. People may pay vastly different amounts for identical goods or services based on algorithmic assessments of their personal circumstances rather than the actual value of what they are purchasing.

This system particularly harms vulnerable populations. Consumers with limited mobility, those in underserved areas with fewer alternatives, or people facing urgent needs may be charged premium prices precisely when they have the least ability to shop around. The elderly, disabled individuals, and those with chronic health conditions often face higher prices for essential goods and services.

The practice also creates market inefficiencies and reduces genuine price competition. When companies can extract maximum revenue through personalized pricing rather than competing on value, it reduces incentives for innovation and quality improvements. Consumers lose the benefit of competitive markets driving prices down.

Perhaps most concerning is how opaque these practices are. Companies rarely disclose when and how they are using surveillance pricing, let alone explain what data they are collecting or how their algorithms work. Consumers typically have no way to know whether they are receiving a fair price or being charged a premium based on their personal profile.

This lack of transparency extends to the data collection itself. Many consumers are unaware of the extent to which their online and offline activities are being monitored and monetized. Companies often collect data through data brokers, making it nearly impossible for individuals to understand what information exists about them or how it is being used to determine prices.

The algorithmic nature of these systems adds another layer of opacity. Even when companies acknowledge using personalized pricing, they typically claim their algorithms are proprietary trade secrets. This makes it extremely difficult for consumers, regulators, or researchers to understand how pricing decisions are made or to identify discriminatory practices. A study from George Washington University found that Uber and Lyft charged, on average, higher prices for pickups and drop-offs in predominantly non-white neighborhoods or neighborhoods with lower incomes.[2] One investigation accused Uber of charging varying amounts for identical rides based on how much battery power is remaining on the device arranging the transportation.[3] In any event, the opacity of the pricing model makes it impossible to determine whether

---

[2] Akshat Pandey and Aylin Caliskan, *Disparate Impact of Artificial Intelligence Bias in Ridehailing Economy's Price Discrimination Algorithms* (May 3, 2021) arXiv, https://arxiv.org/abs/2006.04599.
[3] VICE Staff, *Uber Accused of Charging People More If Their Phone Battery Is Low* (April 11, 2023) VICE, https://www.vice.com/en/article/uber-surge-pricing-phone-battery/.

there are legitimate bases for the disparities or whether unlawful discrimination is being carried out.

The practice has prompted the Federal Trade Commission (FTC) to conduct a market study:

> "Initial staff findings show that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage," said FTC Chair Lina M. Khan. "The FTC should continue to investigate surveillance pricing practices because Americans deserve to know how their private data is being used to set the prices they pay and whether firms are charging different people different prices for the same good or service."
> . . .
> The staff perspective found that some [] respondents can determine individualized and different pricing and discounts based on granular consumer data, like a cosmetics company targeting promotions to specific skin types and skin tones. The perspective also found that the intermediaries the FTC examined can show higher priced products based on consumers' search and purchase activity. As one hypothetical outlined, a consumer who is profiled as a new parent may intentionally be shown higher priced baby thermometers on the first page of their search results.
>
> The FTC staff found that the intermediaries worked with at least 250 clients that sell goods or services ranging from grocery stores to apparel retailers. The FTC found that widespread adoption of this practice may fundamentally upend how consumers buy products and how companies compete.[4]

Recently, an investigation led to Target agreeing to pay $5 million in civil penalties and to change its pricing practices:

> The lawsuit and judgement come after a KARE 11 investigation uncovered certain prices in the Target app switching when customers walked into the store.
>
> "We learned of your news story that showed changes on the app depending on the location," said Steve Spinella, deputy district attorney

[4] Press Release, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (January 17, 2025) FTC, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

> for San Diego County. "We conducted our own independent investigation to see if this was also occurring in California."
>
> Spinella joined six other county prosecutors in California and recently sued Target, accusing the chain of charging customers higher prices than advertised.
>
> According to the civil complaint, prosecutors found prices posted for various items on Target.com or the Target app that then switched when a customer entered the perimeter of the store without "clearly and conspicuously disclosing the sales channel."[5]

2. Prohibiting surveillance pricing

This bill prohibits surveillance pricing. 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 bill defines "surveillance pricing" as 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. This does not include situations where the difference in price is based solely on costs associated with providing the good to different consumers.

The Electronic Frontier Foundation highlights the concerns with surveillance pricing practices:

> This practice is harmful in many ways. First, surveillance pricing invades our privacy. Vendors offer us a price only after scrutinizing our personal data about what we've clicked online and where we've travelled offline. Moreover, surveillance pricing incentivizes all businesses to harvest as

[5] Chris Hrapsky, *Target settles lawsuit alleging false advertising, overpricing; fined $5M* (April 27, 2022) KARE 11 News, https://www.kare11.com/article/news/local/kare11-extras/target-settles-ca-lawsuit-alleging-false-advertising-overpricing-fined-5m/89-ba4a5441-c38e-4c9f-b524-b0d13414042f.

> much of our personal data as possible. Some businesses will use it for their own surveillance pricing. Other businesses, which might not themselves use it this way, will sell it to data brokers, which in turn will sell it to others for use in surveillance pricing.
>
> Second, surveillance pricing can disparately burden people of color and other vulnerable groups. For example, surveillance pricing led to Asian people being offered a higher price for test prep services, older people being offered a higher price for dating services, and people living in non-white neighborhoods being offered a higher price for a ride home.
>
> Third, surveillance pricing is opaque. Many people don't even know when they've been subjected to it. Those that do often cannot determine the unknown reasons for the price they're offered. As a result, consumer advocates will be less able to publish meaningful price comparisons to help consumers make choices. And regulators will be less able to identify unlawful pricing practices.[6]

Concerns have been raised that outright banning this practice could negatively impact various programs that are beloved by consumers, many of which provide real benefits. In response, the bill has a broad carveout for situations where surveillance pricing is used to offer consumers such discounts.

Discounted prices can be provided based on surveillance pricing when sufficient transparency and fairness are ensured. First, the eligibility criteria, available discounts, and any conditions for receiving or earning the discounted price must be clearly and conspicuously disclosed on the company's website and uniformly offered or made available to all consumers who meet the disclosed eligibility criteria. This ensures both transparency and equity. Second, the discounted price must meet one of the following criteria:

- Offered based on publicly disclosed eligibility criteria that any consumer could potentially meet, including signing up for a mailing list, providing personal information registering for promotional communications, or participating in a promotional event. The terms and criteria must be conveyed clearly and

---

[6] *See* Julia Angwin, et al., *The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review* (September 1, 2015) ProPublica, The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review — ProPublica; *New Research: Tinder's Opaque, Unfair Pricing Algorithm Can Charge Users Up to Five-Times More For Same Service* (February 8, 2022) Mozilla Foundation, https://www.mozillafoundation.org/en/blog/new-research-tinders-opaque-unfair-pricing-algorithm-can-charge-users-up-to-five-times-more-for-same-service/; Kyle Wiggers, *Researchers find racial discrimination in 'dynamic pricing' algorithms used by Uber, Lyft, and others* (June 12, 2020) Venture Beat, https://venturebeat.com/technology/researchers-find-racial-discrimination-in-dynamic-pricing-algorithms-used-by-uber-lyft-and-others.

conspicuously disclosed in clear and prominent terms so that an ordinary consumer would notice and understand them.
- Offered to members of a broadly defined group, including teachers, active or retired military, senior citizens, students, or residents of a certain area.
- Offered through a loyalty, membership, or rewards program that consumers affirmatively purchase or enroll in.

Violations are subject to civil penalties of up to $12,500 for each violation. Damages are trebled for intentional violations. Consumers are also granted a limited right of action seeking injunctive relief as necessary to enforce the law and to remedy any violation thereof.

3. Other jurisdictions

It should be noted that several other states are also taking action to combat surveillance pricing. Legislation has been introduced and passed through legislatures in four other states.

The New York Legislature has sent Governor Kathy Hochul a bill that would ban surveillance pricing by any entity selling goods or services to consumers in the state. The legislation provides exemptions for bona fide custom discounts connected to loyalty programs, group-based discounts, and discounts based on prior purchase history. The discounts must be offered uniformly to any consumer who meets the eligibility and there are disclosure requirements for the discount exemptions. It also prohibits advertising, promoting, labeling, or publishing a statement, display, image, offer, or announcement using surveillance pricing to a consumer.

Connecticut banned surveillance pricing by retail sellers, entities selling tangible personal property, as part of a larger omnibus bill. It further required disclosure of surveillance pricing for goods and services. It too had exemptions for discounts with some disclosure requirements. It was recently signed into law.

Maryland's version, which was signed by its governor, is a much narrower version. It applies only to certain food retailers and broadly exempts discounts without including many of the transparency requirements included in this bill or elsewhere. Those groups in opposition to this bill argue for a model closer to that found in Maryland.

Colorado's measure prohibited "individualized price setting" and included exemptions for discounts that were publicly disclosed. However, the legislation was much broader than its counterparts in that it applied to individualized *wage* setting as well. The bill was passed by Colorado's legislature but vetoed by Governor Jared Polis.

This increased movement toward regulating this practice is driven in part by polling that suggests consumers find surveillance pricing "fundamentally unfair" and support bans:

> New polling from Groundwork Collaborative and Data for Progress finds that an overwhelming majority of Americans want to ban the use of surveillance pricing – a deceptive tactic used by big corporations that weaponizes consumers' personal data to set prices on everyday goods and services. The poll reveals that over three-quarters (76%) of Americans said they support efforts that bring an end to the algorithmic pricing scheme.
>
> Since the start of 2026, at least 40 bills targeting personalized algorithmic pricing have been introduced in at least 24 states. Legislative momentum accelerated after Groundwork's 2025 investigation with Consumer Reports and More Perfect Union found that Instacart was running pricing experiments on unsuspecting shoppers, a practice Instacart dropped after public backlash.
>
> As high grocery prices drain working families' budgets, the polling released today finds that Americans overwhelmingly believe in one fair price for all consumers – 80% of voters agree that every customer should pay the same price for the same item. Consumers are savvier than corporations give them credit for. The majority of Americans don't buy the industry argument that banning surveillance pricing will bring an end to loyalty programs and discounts. In fact, 72% of voters say they would accept smaller discounts on average if it means all customers are offered the same price.[7]

4. Stakeholder positions

A large coalition of legal services organizations, labor associations, civil rights organizations, and consumer, privacy, and family advocacy groups, including Public Law Center, SEIU California, The Greenlining Institute, and the Center for Democracy and Technology, write in support:

> California consumers face a new and growing threat to fair pricing. Companies now possess the technology to collect vast amounts of consumer data and deploy artificial intelligence to charge each shopper a personalized price — one calibrated not to the market, but to the maximum that an individual can be made to pay. This practice, known as

[7] *Strong Majority of Americans Want Corporations to End Deceptive Surveillance Pricing Schemes* (May 21, 2026) Groundwork Collaborative, https://groundworkcollaborative.org/news/strong-majority-of-americans-want-corporations-to-end-deceptive-surveillance-pricing-schemes/.

> surveillance pricing, exploits detailed consumer profiles built from purchase histories, location data, browsing habits, and more.
>
> Investigations have already uncovered real-world harms. Consumer Reports revealed that Kroger built 60-plus page profiles for individual consumers from loyalty program data to infer willingness to pay. … A SFGate investigation found that the most popular hotel booking sites show prices substantially higher to San Franciscans using their online booking platforms compared with users browsing from less affluent cities, like Phoenix and Kansas City. These are not isolated incidents — they reflect an industry trend. …
>
> While California consumers benefit from some privacy protections under the California Consumer Privacy Act, no existing federal or state law prohibits companies from using the data they collect to charge consumers individually different prices. AB 2564 closes this gap. Without legislative intervention, surveillance pricing will become the industry standard, disproportionately harming lower-income Californians who already face the highest costs of living in the nation and have the fewest alternatives.
>
> AB 2564 protects sensible, transparently offered discounts—including for loyalty programs. The bill's exemptions permit a vast array of discounts, and transparency provisions help ensure that discounts are not secretly discriminatory. The bill does not restrict businesses from offering lower prices — it prevents them from secretly charging higher ones based on personal data profiles.
>
> The right to fair and affordable pricing should not be a privilege for the few but a fundamental protection for all Californians.[8]

Chamber of Progress writes in opposition to the bill, contesting the underlying premise:

> The term "surveillance pricing" suggests that companies are using personal data to charge individual consumers higher prices. We agree that no one should be charged more because of their personal data. But that is not what the evidence shows businesses are doing. What they overwhelmingly use consumer data for is the opposite: offering discounts, coupons, and targeted promotions that help families save money while

[8] *See Consumer Reports Investigation Uncovers Kroger's Widespread Data Collection* (May 21, 2025) Consumer Reports, https://www.consumerreports.org/media-room/press-releases/2025/05/consumer-reports-investigation-uncovers-krogers-widespread-data-collection-of-loyalty-program-members-to-create-secret-shopper-profiles/; Keith A. Spencer, *Hotel booking sites show higher prices to travelers from Bay Area* (February 3, 2025) SFGate, https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.

> enabling businesses to reach the right customers, increase sales, and operate more efficiently.
>
> Consumer markets are intensely competitive. When shoppers can compare prices with a few taps on their phone, using personal data to charge a customer more is a losing strategy. A competitor will simply offer a better price and win the sale. The businesses that use consumer data most actively are the ones competing hardest for customers, and they compete by offering better deals, not higher prices.
>
> In practice, personalized pricing looks like this:
> - *Personalized coupons*. Your grocery store's app sends you a $2-off coupon for the cereal you buy every week, or a deal on diapers because you have a baby at home.
> - *Win-back offers*. You haven't ordered from your favorite restaurant in two months. They send you a 20% off coupon to come back.
> - *Cart abandonment discounts*. You put a pair of shoes in your online cart but don't check out. The retailer emails you a 10% off code to complete the purchase.
> - *New product introductions*. A new snack brand enters your grocery store and the store sends a coupon to customers who already buy similar products, directing the promotion to shoppers most likely to be interested.

A coalition in opposition, led by the California Chamber of Commerce, asserts:

> AB 2564 prohibits "surveillance pricing," which it loosely defines 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 personally identifiable information collected through electronic surveillance technology..."
>
> 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 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.[9]

SUPPORT

California Federation of Labor Unions (co-sponsor)
Consumer Reports (co-sponsor)
TechEquity Action (co-sponsor)
ACLU Cal Action
Alliance of Californians for Community Empowerment (ACCE) Action
American Federation of Musicians, Local 7
Buen Vecino
California Food and Farming Network
California Nurses Association
California School Employees Association
California Work and Family Coalition
Cameo Network
Center for AI and Digital Policy (CAIDP)
Center for Democracy and Technology
Center on Policy Initiatives
CFT- a Union of Educators & Classified Professionals
Consumer Attorneys of California
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Courage California
Economic Security California Action
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
End Child Poverty California Powered by Grace
Equal Rights Advocates
Friends Committee on Legislation of California
Greenlining Institute
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
Nextgen California
Oakland Privacy

[9] The definition in the bill does not include "services."

Parent Voices California
Privacy Defense Alliance
Privacy Rights Clearinghouse
Public Law Center
Secure Justice
SEIU California
Sister Warriors Freedom Coalition
Smart - Transportation Division
Tech Oversight California
Techtonic Justice
UDW/AFSCME Local 3930
Ultraviolet Action
Western Center on Law & Poverty

OPPOSITION

Association of National Advertisers
Building Owners and Managers Association of California
CalBroadband
California Business Properties Association
California Chamber of Commerce
California Fuels and Convenience Alliance
California Grocers Association
California Restaurant Association
California Retailers Association
Chamber of Progress
Civil Justice Association of California (CJAC)
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

RELATED LEGISLATION

SB 259 (Wahab, 2025) establishes the Fair Online Pricing Act, which prohibits a price offered to a consumer through the consumer's online device, as defined, from being generated in whole, or in part, based on any of certain input data, including the presence or absence of any software on the online device or its geolocation data. SB 259 is currently on the Assembly Floor Inactive File.

AB 446 (Ward, 2025) was significantly similar to the current bill. It was amended to apply the prohibition on surveillance pricing only to grocery establishments. AB 446 is currently on the Senate Floor Inactive File.

PRIOR VOTES:

Assembly Floor (Ayes 42, Noes 21)
Assembly Appropriations Committee (Ayes 10, Noes 4)
Assembly Judiciary Committee (Ayes 8, Noes 3)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 4)

****