

SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

AB 446 (Ward)
Version: May 1, 2025
Hearing Date: July 15, 2025
Fiscal: No
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 provides 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 or service for a specific consumer or group of consumers, based on consumers’ personal information collected through electronic surveillance technology. This includes information gathered through sensors, cameras, device tracking, biometric monitoring, or other forms of observation or data collection. The bill provides a series of 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 and other relief to be sought in a civil action.

This bill is sponsored by the United Food and Commercial Workers (UFCW) Western States Council and Consumer Watchdog. 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 the California Federation of Labor Unions. It is opposed by various industry groups, including TechNet and Chamber of Progress.

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' 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 or service for a specific consumer or group of consumers, based, in whole or in part, on covered information collected through electronic surveillance technology. “Surveillance pricing” includes the use of technological methods, systems, or tools, including sensors, cameras, device tracking, biometric monitoring, or other forms of observation or data collection, that are capable of gathering covered information about a consumer’s behavior, characteristics, location, or other personal attributes, whether in physical or digital environments.
- 2) Defines “covered information” as both aggregate consumer information and personally identifiable information, as defined in the CCPA.
- 3) Provides that a person does not engage in surveillance pricing if any of the following apply:
 - a) The difference in price is based solely on costs associated with providing the good or service to different consumers.
 - b) A discounted price is offered based on publicly disclosed eligibility criteria, including, but not limited to, signing up for a mailing list, registering for promotional communications, or participating in a promotional event.
 - c) A discounted price is offered to members of a broadly defined group, including, but not limited to, teachers, veterans, senior citizens, or students, based on publicly disclosed eligibility criteria.
 - d) A discounted price is offered through a loyalty, membership, or rewards program that consumers affirmatively enroll in.
 - e) The person operates as an insurer complying with Section 791.02 of the Insurance Code and the pricing is in connection with that activity, as provided.

- 4) Requires the discounted price offered in b), c), or d) above to comply with the following:
 - a) The eligibility criteria, available discounts, and any conditions for receiving or earning the discount or reward shall be clearly and conspicuously disclosed before any covered information is collected.
 - b) The discount or reward shall be offered uniformly to all consumers who meet the disclosed eligibility criteria.
- 5) Provides that any covered information collected pursuant to the exceptions above shall be used solely for the purpose of offering or administering the applicable discount, cost-based pricing, or loyalty program, and shall not be used for any other purpose, including profiling, targeted advertising, or individualized price setting.
- 6) Subjects a person that violates these provisions, in addition to any other remedy at law, to liability for a civil penalty not to exceed \$12,500 for each violation, with each violation constituting a separate violation with respect to each consumer or transaction involved. Intentional violations are subject to trebling, and a person in violation shall be required to disgorge all revenues earned thereby. A prevailing plaintiff shall be awarded reasonable attorney's fees and costs. A court may also award injunctive or declaratory relief as necessary.
- 7) Provides that a person is not in violation if the refusal to extend credit on specific terms, or the refusal to enter into a transaction with a specific consumer, is based on information contained in a consumer report, as defined.
- 8) Makes any waiver void and unenforceable.
- 9) Clarifies that the rights, remedies, and penalties are cumulative to any others.
- 10) 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

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.

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 July 9, 2025.

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 2021 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 The opacity of the pricing model makes it impossible to determine whether 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.”

...

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>.

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.

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 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."³

2. Prohibiting surveillance pricing

This bill prohibits surveillance pricing. According to the author:

³ 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>.

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 446 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 or service for a specific consumer or group of consumers, based, in whole or in part, on covered information collected through electronic surveillance technology. This includes the use of technological methods, systems, or tools, including, but not limited to, sensors, cameras, device tracking, biometric monitoring, or other forms of observation or data collection, that are capable of gathering covered information about a consumer’s behavior, characteristics, location, or other personal attributes, whether in physical or digital environments. This does not include situations where the difference in price is based solely on costs associated with providing the goods or services to different consumers.

The bill also provides a number of discounting practices that do not fall within this ban. For instance, discounted prices can be provided under certain circumstances and when sufficient transparency and fairness is ensured. This includes offering reduced prices through loyalty, membership, or rewards programs when consumers affirmatively enroll in them. In addition, where the eligibility criteria is publicly disclosed, discounts can be offered to members of broadly defined groups, such as veterans or students, or through mailing lists that consumers sign up for.

To ensure consumers are protected and made aware of the schemes, the eligibility criteria, available discounts, and any conditions for receiving or earning the discount or reward shall be clearly and conspicuously disclosed before any covered information is collected. The discount or reward must be offered uniformly to all consumers who meet the disclosed eligibility criteria.

To protect the privacy of consumers, any covered information collected shall be used solely for the purpose of offering or administering the applicable discount, cost-based pricing, or loyalty program, and shall not be used for any other purpose, including, but not limited to, profiling, targeted advertising, or individualized price setting.

The bill provides carve outs for certain insurance pricing or financial transactions that comply with specified laws.

Violations are subject to civil penalties of up to \$12,500 for each violation. Damages are trebled for intentional violations.

3. Stakeholder positions

UFCW Western States Council, a sponsor of the bill, explains the need for the bill:

Surveillance Pricing Should Be Prohibited Because It Exacerbates Inequality, Especially as Applied To Necessities Like Food.

In October 2024, an explosive news report found that Kroger, one of the largest grocery store chains in the United States,⁴ was exploring the use of facial recognition technology in its stores. Immediately, shoppers and public officials worried that consumers' faces might be used, along with other intimate data, to deliver different prices for different consumers.

Surveillance pricing exacerbates economic inequality. "Higher-income consumers may receive discounts, while those with less disposable income might face higher prices. Surveillance pricing can further entrench these inequalities, like how credit scores impact loan rates or zip codes affect insurance premiums. Marginalized communities, including people of color and low-income individuals, are particularly vulnerable to higher prices due to algorithmic biases[.]"

Consumer Watchdog, the other sponsor of the bill, writes:

Unfortunately, the FTC shelved public comment into surveillance pricing, which makes the work of California legislators that much more important. A.B. 446 aims to address these concerns by prohibiting businesses from setting prices based on personally identifiable information gathered through electronic surveillance. The bill seeks to bar companies from using race, religion, residence, sexuality, political interests, web browsing and purchase history, financial circumstances, and consumer behaviors in setting prices. The bill also outlines civil penalties for violations, ensuring that consumers are protected from such practices.

With prices for essential goods such as groceries up 30 percent since the beginning of the decade, and Kroger's plan to roll out digital price tags and facial recognition technology, the time to act is now.

Plain and simple: Companies shouldn't have to surveil us in order to sell products. Companies are sitting on mountains of personal data – much of it incorrect – that feed this digital auction of exploitation and e-commerce algorithms. By supporting A.B. 446, you can put California on the road to being the first state in the country to address surveillance pricing. AB 446

⁴ <https://therecord.media/kroger-facial-recognition-lawmakers-concerns>.

demonstrates a commitment to consumer rights and privacy, ensuring that all Californians are treated fairly in the marketplace. One product, one price.

A broad coalition of groups, including Economic Security CA Action and the Black Women for Wellness Action Project, write in support:

This bill will prevent companies from exploiting consumers' personal data to maximize profits at a time when average households are struggling with the rising costs of basic necessities. According to the U.S. Labor Department's Bureau of Labor Statistics, current average consumer prices are up 23% since 2019, with some categories even higher, like food, rising about 30% over the same period.

AB 446 will protect consumers' privacy and their right to fair and equitable pricing.

A large coalition of industry associations, including the Association of National Advertisers and the California New Car Dealers Association, write in opposition:

AB 446 conflicts with the approach of the CCPA because it treats "aggregate consumer information" as if it were "personal information," in explicit contradiction of Civil Code 1798.140. As a policy matter, we believe this is incorrect; information that has been deidentified and aggregated is not personal information under the CCPA, nor should it be here. Such data is not a risk of individual profiling or discrimination exactly because it is deidentified or aggregated. That is why, as a matter of public policy, aggregated data and personal data are not treated the same because they neither implicate the same rights for consumers nor pose the same risks in the event of a data leak.

An example helps illustrate how "aggregate consumer information" is used, and how non-problematic it is. Supermarket #1, who is planning on selling pumpkin pie mix in October, is concerned they may have too much pumpkin pie mix on hand in late September, and they have a new shipment coming on October 1. Under present law, they can look at their past aggregate purchase history of all their consumers from last year during October (from which all their customer names and other identifying data has been removed) to see how much pumpkin pie mix was purchased last October (which would qualify as aggregate data under the CCPA and does not require consumer opt-in to utilize) to determine whether they are overstocked and should offer a sale this year. After reviewing their supply, and last year's aggregate sale volume, they can decide whether to offer a quick sale to get rid of soon-to-be-excess

inventory. However, under AB 446, Supermarket #1 could not review last year's sales data because it would qualify as "covered information" and Supermarket #1 had not met the new consent requirements that AB 446 will require for every customer who shopped at their store last year. Without such consent from every shopper, even totally anonymous data such as the date, items, and price of their purchases would necessitate opt-in by consumers. Because AB 446 treats personal data and aggregate data the same, merging them as "covered information," the same onerous (and CCPA-conflicting) disclosure requirements applicable to personal information would apply to aggregate data.

The bill does include within its surveillance pricing definition "covered information," which includes both "personally identifiable information" and "aggregate consumer information." The former borrows its meaning from the CCPA, but as stated, aggregated data is carved out in the CCPA.

In response to the concerns of opposition, the author has agreed to an amendment that removes aggregate consumer information from the definition of "covered information," focusing solely on personally identifiable information.

The opposition coalition also strongly objects to the private right of action in the bill:

[E]mployers will need to consider whether their present discounts fit into the listed permissible exceptions 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 fit AB 446's terms; (b) choose to cancel even potentially compliant discounts because the cost of potential litigation and shakedown demand letters is too great.

In response to these concerns, the author has agreed to an amendment that limits enforcement actions for civil penalties to public prosecutors. Consumers may only bring actions for injunctive relief along with costs and reasonable attorney's fees.

To ensure consumers can still receive discounts, where there is clear transparency about the information being used and meaningful consent, the author has agreed to an amendment that allows offering a discounted price after a consumer directly and knowingly provides specific personally identifiable information for the purpose of obtaining a discount. The nature and purpose of the consumer's disclosure of personal information must be conveyed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand it. To ensure consumers are fully aware of the basis for the differential pricing allowed by the bill, the author's amendment will require that any personally identifiable information provided for the

purpose of receiving a discounted price is not augmented or supplemented by personally identifiable information obtained from a third party or other means.

Additional amendments have also been agreed to that respond to other opposition concerns. This includes extending the exceptions to cover consumer programs that consumers purchase and to allow for discounts to residents of a certain area. In addition, the amendments expand the lending exemption and provide that a person is not in violation if the pricing or specific terms of extending credit, refusal to extend credit on specific terms, or the refusal to enter into a transaction with a specific commercial enterprise, is based on information contained in a commercial credit report, defined under Civil Code Section 1785.42. An amendment requested by the insurance industry is also being taken to clarify that the insurer exception applies to a person that operates as an insurer *as defined by* relevant law.

SUPPORT

Consumer Watchdog (sponsor)
UFCW - Western States Council (sponsor)
American Economic Liberties Project
American Federation of Musicians, Local 7
Black Women for Wellness Action Project
California Civil Liberties Advocacy
California Federation of Labor Unions, AFL-CIO
California Food and Farming Network
California Low-income Consumer Coalition
California National Organization for Women
California Nurses Association
California Safety and Legislative Board, Smart - Transportation Division (SMART - TD)
California School Employees Association
California State Council of Service Employees International Union (SEIU California)
Center on Policy Initiatives
CFT- a Union of Educators & Classified Professionals, AFT, AFL-CIO
Consumer Attorneys of California
Consumer Federation of California
Courage California
Economic Security California Action
Equal Rights Advocates
LAANE (Los Angeles Alliance for a New Economy)
National Consumer Law Center, INC.
Oakland Privacy
Powerswitch Action
Techequity Action
United Domestic Workers/AFSCME Local 3930
Western Center on Law & Poverty

Working Partnerships USA

OPPOSITION

American Property Casualty Insurance Association
Associated Equipment Distributors
Association of National Advertisers
Brea Chamber of Commerce
Building Owners and Managers Association of California
CalBroadband
California Attractions and Parks Association
California Bankers Association
California Business Properties Association
California Chamber of Commerce
California Credit Union League
California Grocers Association
California Hotel & Lodging Association
California New Car Dealers Association
California Retailers Association
California Travel Association
Carlsbad Chamber of Commerce
Chamber of Progress
Chino Valley Chamber of Commerce
Corona Chamber of Commerce
CTIA
Cupertino Chamber of Commerce
Folsom Chamber of Commerce
Greater Conejo Valley Chamber of Commerce
Greater High Desert Chamber of Commerce
Greater San Fernando Valley Chamber of Commerce
LA Cañada Flintridge Chamber of Commerce and Community Association
Lake Elsinore Valley Chamber of Commerce
Long Beach Area Chamber of Commerce
Mission Viejo Chamber of Commerce
Naiop California
National Association of Mutual Insurance Companies
National Federation of Independent Business
Newport Beach Chamber of Commerce
Orange County Business Council
Palm Desert Area Chamber of Commerce
Paso Robles and Templeton Chamber of Commerce
Personal Insurance Federation of California
Rancho Cordova Area Chamber of Commerce
Rancho Mirage Chamber of Commerce

San Juan Capistrano Chamber of Commerce
Santa Ana Chamber of Commerce
Santa Clarita Valley Chamber of Commerce
Simi Valley Chamber of Commerce
Software Information Industry Association
TechNet
The Travel Technology Association
Torrance Area Chamber of Commerce
USTelecom - the Broadband Association

RELATED LEGISLATION

Pending 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 in the Assembly Judiciary Committee.

Prior Legislation: None known.

PRIOR VOTES:

Assembly Floor (Ayes 47, Noes 20)
Assembly Judiciary Committee (Ayes 8, Noes 3)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 3)
