Date of Hearing: March 25, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2564 (Ward) – As Amended March 23, 2026

SUBJECT: Surveillance pricing

SYNOPSIS

Surveillance pricing is the practice of using consumers' personal information – including location, device type, demographics, and credit, browsing, or shopping history – to set the price of a good based on the consumer's perceived willingness to pay. This can lead to different consumers being charged different prices for the same good based on data-driven inferences and personal characteristics. While proponents of this practice claim it enhances price efficiency, critics contend that it is a surreptitious form of economic discrimination that disproportionately impacts lower-income communities that lack adequate options for purchasing essential goods.

This bill, co-sponsored by Consumer Reports and Tech Equity, would impose a blanket ban on personalized price discrimination – "surveillance pricing" – based in whole or in part on the consumer's personally identifying information. The bill defines surveillance pricing in a technology-neutral manner as offering or setting a customized price for a good for a specific consumer or group of consumers based on personally identifiable information collected through electronic surveillance technology. The bill also provides consumers with recourse against businesses that violate this prohibition. The bill is substantially similar to last year's AB 446 (Ward), which passed this Committee on a 10-3 vote and progressed to the Senate floor before being moved to the inactive file.

The bill is supported by numerous consumer rights, privacy, and labor organizations, including the California Nurses Association, Oakland Privacy, California Federation of Labor Unions, and the Electronic Privacy Information Center. The bill is opposed by a variety of business trade associations, including the California Chamber of Commerce, the American Advertising Federation, and Chamber of Progress.

If passed by this Committee, this bill will next be heard by the Judiciary Committee.

EXISTING LAW:

1) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (Cal. Const., art.1, § 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. (Civ. Code § 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. (Civ. Code § 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. (Civ. Code § 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. (Civ. Code § 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. (Bus. & Prof. Code § 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. (Bus. & Prof. Code § 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. (Bus. & Prof. Code § 17200.)

THIS BILL:

1) Prohibits retailers from engaging in surveillance pricing.

2) States that a retailer is not engaging 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 is offering a discounted price based on publicly disclosed eligibility criteria and is uniformly offered or made available to all consumers who meet the criteria. Specifically:

        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.
        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.
        iii. A discounted price is offered through loyalty, membership, or rewards programs that consumers purchase or enroll in.

3) Defines the following terms:

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

    b. "Electronic surveillance technology" means the use of 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" from the California Consumer Privacy Act (CCPA).

    d. "Retailer" means any seller who makes any retail sale of tangible personal property, as defined.

    e. "Surveillance pricing" means offering or setting a customized price for a good for a specific consumer or group of consumers based on personally identifiable information collected through electronic surveillance technology.

        "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.

4) Enables certain public prosecutors to seek a civil penalty of $12,500 for violations, treble damages and disgorgement of revenues earned for intentional violations, and reasonable attorney's fees and costs.

5) Allows a consumer to bring an action solely for injunctive relief as necessary for enforcement.

6) Provides that waivers of the bill are against public policy and are void and unenforceable.

COMMENTS:

1) **Author's statement**. 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.

2) **The Commodification of Personal Data**. Enshrined in the state constitution by a ballot initiative in 1972, the unalienable right to privacy is guaranteed to all Californians and is enforceable against both the public and private sectors. However, for the past 20 years, experts have been warning us about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed.

It has become increasingly clear that not only is our right to privacy significantly eroded, but our private information and activities are now being harvested and sold for a profit. This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist, Shoshana Zuboff. In an opinion piece for *The New York Times*, in 2021, Dr. Zuboff warned:

> 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." *The New York Times* (Nov. 12, 2021) *available at* https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.

The rapid advancement of artificial intelligence over the past five years has significantly accelerated data collection and processing. Artificial intelligence (AI) agents can be deployed to extract data, also known as scraping, from websites. Inevitably, this includes personal information of consumers that data brokers compile and sell to businesses. Even if the data does not include a significant amount of personal information, if it can be attached to an existing dossier on a consumer, AI tools can make sophisticated inferences about the person, including making inferences about very personal, sensitive parts of individuals' lives. These businesses then integrate the acquired data with their own consumer information to create detailed consumer profiles. With AI, these profiles can be updated in real time to personalize user experiences and target advertisements more effectively.[2]

According to the author, it is estimated that 1.7 MB of data is created per second for every person on earth. That equates to about the size of an 850-page book every second. In total, the amount of data created every day around the world, about 2.5 exabytes, is equal to 7500 times the size of The Library of Congress.

3) **The history of establishing sale prices**. For much of history, deals at marketplaces were made via bartering, and consumers and producers alike would try to haggle a deal that would align with the buyer's willingness, or ability, to pay for goods. This system enabled some consumers to cut deals; however, others would be taken advantage of because of the lack of transparency in how much a product costs. The bartering system was upended in mid 1800s when a Wanamaker's department store in Philadelphia began to include price tags on their goods. John Wanamaker believed that customers would trust their retailers more if they could see the prices and therefore make informed decisions about their purchasing options.[3] He incorporated these prices into advertisements, and when customers found them to be accurate, it strengthened their confidence in the retailer. This innovation helped drive the expansion of department stores and set the standard for pricing practices for the next 150 years.

4) **Individualized prices based on consumer dossiers**. Surveillance pricing, also known as individualized pricing, uses AI or other technology for the real-time processing of personal information about a consumer to set a price specific to that consumer. The Federal Trade Commission (FTC) has described surveillance pricing as "an ecosystem designed to use large-scale data collection to help sellers maximize their revenues by customizing the pricing, as well as the selection of products and services, offered to each consumer."[4]

It is important to distinguish surveillance pricing from dynamic pricing, which adjusts prices in response to market demand. For example, Wendy's fast food restaurants appeared to briefly flirt with dynamic pricing with plans to rapidly adjust the cost of their menu items based on demand – increasing the costs at times of peak demand.[5] In contrast, surveillance pricing treats each

---

[2] For more information on surveillance capitalism and the implications, see the background paper of this Committee's March 3, 2026 informational hearing *Somebody's Watching you: Californian's Privacy in the Age of Mass Surveillance*. https://apcp.assembly.ca.gov/hearings/2025-26-informationaloversight-hearings.
[3] PBS, "John Wanamaker" (Mar. 10, 2025), https://www.pbs.org/wgbh/theymadeamerica/whomade/wanamaker_hi.html.
[4] Federal Trade Commission, "Issue Spotlight: The Rise of Surveillance Pricing" (January 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.
[5] "Wendy's denies plans for surge pricing after backlash," BBC News (Feb. 28, 2024).

consumer as their own economy, using algorithms to assess their willingness to pay based on personal information such as browsing history, purchase behavior, and location.

Surveillance Pricing has already impacted consumers. The sponsors of the bill acknowledge that 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." However, they note that a number of journalists have documented examples of practice:

1. 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.

2. 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.

3. 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.

4. 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.

These examples have raised concerns about businesses' ability to analyze a consumer's willingness to pay and adjust prices accordingly without consumer knowledge or consent.

The use of surveillance pricing does not just impact the consumers with higher incomes that the AI tool has determined are willing to pay more because they are able to. Surveillance pricing tools are able to also adjust prices based upon the inferred desperation of the consumer. For example, it is conceivable that a dossier might contain information suggesting that someone is a new parent and is in a 24-hour store late at night that they do not usually frequent that carries diapers. It would not be difficult for the tool to infer that the consumer has a level of desperation and urgency and is therefore willing to pay more for the diapers than someone in a less urgent situation.

The use of AI to set prices also raises concerns regarding biases within the algorithms that may disadvantage different groups. 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.[6] While it is unclear whether these disparities stem from market forces or algorithmic bias because these companies use

---

[6] Akshat Pandey and Aylin Caliskan, "Disparate Impact of Artificial Intelligence Bias in Ridehailing Economy's Price Discrimination Algorithms" *arXiv* (May 3, 2021), https://arxiv.org/abs/2006.04599.

opaque algorithms to set prices, a possible conclusion is that algorithmic price setting could reinforce structural inequities.

Because businesses often operate without transparency, the extent of surveillance pricing remains uncertain. In the summer of 2024, the Federal Trade Commission launched a study to investigate how companies leverage AI, other technologies, and consumer data to set individualized prices. A preliminary report released in January revealed that at least 250 businesses have adopted technologies capable of implementing surveillance pricing. Lina Khan, former FTC Chair, concludes in this report:

> 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. 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.[7]

Surveillance pricing is an example of perfect price discrimination. Under perfect price discrimination, consumer surplus, the difference between what a consumer is willing to pay and the actual price they pay, disappears as each consumer is charged exactly what they are willing to pay.[8] Therefore, all surplus in the market is captured by the producer, which can reduce consumer welfare. The FTC has reported on this phenomenon, finding that businesses that had implemented surveillance pricing had already seen 1-5% increases in revenue.[9] In contrast, traditional competitive pricing exerts downward pressure on prices, increasing consumer surplus and overall consumer welfare, though at the cost of some inefficiency, or deadweight loss, for producers.

Research suggests that surveillance pricing, under highly competitive pressures, could lead to aggressive pricing strategies taken by all firms that result in lower prices.[10] However, this outcome depends on consumer data being used solely for pricing, data is equally available, and the data is not used for other strategic purposes. In less competitive markets, or where one firm has superior access to consumer data, surveillance pricing can instead be used to target specific consumers with personalized discounts, ads, and product recommendations. This strategy fosters customer loyalty, making those consumers less price-sensitive and increasing the cost for competitors to attract them. Competition then softens, which leads to higher costs for consumers. Smaller firms that cannot afford to collect, purchase, or process vast consumer datasets will face increasing disadvantages if surveillance pricing becomes widespread. This imbalance could further entrench market power among large corporations, reducing competition and ultimately harming consumers.

---

[7] Federal Trade Commission, "FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices" (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[8] Organisation for Economic Co-operation and Development "Personalised Pricing in the Digital Era" (Mar. 10, 2025), https://web-archive.oecd.org/temp/2022-02-22/494784-personalised-pricing-in-the-digital-era.htm

[9] Federal Trade Commission, "FTC Surveillance Pricing 6(b) Study: Research Summaries A Staff Perspective" (Jan. 17, 2025), p. 10.

[10] Zhijun Chen, Chongwoo Choe, Noriaki Matsushima, "Competitive Personalized Pricing", *Management science,* vol. 66, No. 9, September 2020, p. 3799

5) **How this bill would affect the price of consumer goods.** The author explains the impact of the bill this way:

> AB 2564 would prohibit the practice of surveillance pricing by making it unlawful for retailers to use personal identifiable information when charging different prices for the same product whether online or during in-store checkout. AB 2564 would include several reasonable exemptions to ensure that consumer friendly discounts and loyalty programs remain unaffected.

Specifically, the bill prohibits the practice of using personal information that is gleaned through the use of surveillance technology and compiled into extensive dossiers on individuals to adjust the price of a good for that individual, regardless of whether the adjustment increases or decreases the price. Instead of individual pricing based on reams of personal data, retailers, as has long been the practice, will need to continue to establish a bona fide price for a product except under certain limited circumstances which allow retailers to offer lower prices through coupons, loyalty programs, or discounts for specific groups of people, such as students, seniors, or veterans. As an example of the practices that will still be allowed, businesses, as Old Navy, Michaels, Ace Hardware and Starbucks do now, can provide rewards to loyalty members that spend a certain amount or purchase a certain number of products. Retailers can also continue sending coupons and special sales to customers who provide their email or sign up for text messages.

In the event a retailer violates the law and uses surveillance pricing, the bill allows public prosecutors from the largest counties and the Attorney General to enforce the bill by seeking a civil penalty of $12,500 for violations, treble damages and disgorgement of revenues earned for intentional violations. In addition, the bill allows a consumer to bring an action solely for injunctive relief and attorney fees if necessary.

6) **Concerns raised by the opposition.** A coalition of business organizations oppose this bill. Primarily they argue that "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." Additional specific concerns from the coalition are set forth in italics and examined below.

The bill 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..."

Though not included in the opposition's quote, the last part of the definition concludes, ". . . collected through electronic surveillance technology that is gathered, purchased, or otherwise acquired from a third party." While the opposition states that surveillance pricing is "loosely defined," the definition in the bill is similar to the descriptions used by the FTC, which describes the practice as businesses "using consumers' detailed personal information—such as their location, demographics, and browsing history—to categorize individuals and set targeted prices

for products or services."[11] In addition, in their FTC Surveillance Pricing Study they describe the practice in the following way:

> Companies that collect or obtain individualized information about their actual or potential customers can potentially use a variety of features to target prices to specific consumers and charge particular groups higher prices or use those features to generate greater profits.[12]

As with many bills that are intended to create permanent statutes, this bill appears to be largely technology-neutral. This approach allows the law to remain relevant and enforceable despite rapidly changing technology.

Notably, "electronic surveillance technology" is not actually defined in AB 2654. 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.

Similar to the previous concern, the definition of "electronic surveillance technology" is technology neutral and in its entirety states:

> "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.

This definition does not appear to be ambiguous or unclear. Regardless of the technology used, businesses are prohibited from using personal information gathered through any type of surveillance technology in order to individually adjust the price of goods.

The bill "Outlaws Consumer-Friendly Discounts – and Will Hurt Affordability Across California by Creating Litigation Risks for Businesses That Offer Discounts." The bill's most recent amendments create the following three-step process:

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

Again, the bill simply bans *individualized* pricing based on *surveillance data*. The opposition correctly notes that the bill lays out several practices, including bona fide reasons for price differentials and discount programs generally available to the public, that do not constitute surveillance pricing:

---

[11] FTC Surveillance Pricing resources. https://www.ftc.gov/news-events/features/surveillance-pricing.
[12] FT*C Surveillance Pricing 6(b) Study: Research Summaries A Staff Perspective* (Jan. 2025). https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf
.

1. The difference in price is based only on the costs associated with providing the item to different customers. An example of this might be a food delivery service that charges different prices based upon the proximity of the customer to the retailer where the food is being picked up.

2. A discounted price that 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.

3. The retailer is offering a discounted price that is offered to members of a broadly defined group such as teachers, active military, students, or seniors.

4. The retailer is offering a discounted price through a loyalty, membership, or rewards program that the customer affirmatively enrolls in.

Thus, pricing differences that are not specific to an individual and based on their surveillance-derived personal information continue to be valid business practices under this bill. As long as any discount includes clear public disclosures and allows anyone who is eligible and/or enrolls in a program to receive the discount, then the company is in compliance with the law and should not face any meaningful prospect of liability under the bill. Therefore, the claim that the bill "outlaws consumer friendly discounts" is at odds with the plain language of the bill.

The bill Contradicts California's Landmark Privacy Law – the California Consumer Privacy Act – by Creating New Consent and Disclosure Requirements, as Well as New Limitations on Data Usage.

The California Consumer Privacy Act is the definitive statute related to consumers' privacy and their personal data – whether that data is collected online, in brick-and-mortar stores, by technological means, on paper, or by powers of observation. It is a broad, technology-neutral, industry-neutral, and comprehensive consumer data protection law, which was also voter-approved via Proposition 24 in 2020.

The CCPA relates primarily to the collection, use, selling, and sharing of Californian's personal information by specific types of businesses. The author has characterized this bill not primarily as a privacy bill but as a consumer protection bill. The distinction being that in this case the concern is the fact that the collected data is used to discriminate against and manipulate certain customers through rapidly changing the prices of goods to allow the business to receive the maximum amount the consumer is willing to pay for a product.

In addition, it is not clear how the bill "contradicts" the CCPA. When the voters approved Proposition 24 in 2020, they established that the CCPA, as amended, was a floor and not a ceiling for privacy protection. Essentially, to protect Californians from any future legislative efforts to weaken statutory protections in the California Privacy Rights Act (CPRA), Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature if

the amendments are consistent with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy.[13]

Given that this bill is further limiting the use of personal information to manipulate and adjust prices, it appears to be in keeping with the CCPA by furthering Californians' privacy rights by curbing the potential misuse of their personal information to set discriminatory prices.

7) **Related legislation.** AB 446 (Ward), a substantially similar bill when it was heard by this Committee (where it passed on a 10-3 vote), was narrowed in the Senate Appropriations Committee to apply only to grocery establishments. Rather than continuing with the bill the author released the following statement:

> This year, I introduced AB 446 to stop companies from charging higher prices based on personal information collected through surveillance technology. Unfortunately, misinformation from the opposition and amendments imposed by the Senate Appropriations Committee have weakened the bill to the point where I am not comfortable advancing it this year. Californians deserve real, meaningful protections—not watered-down half measures—and I refuse to accept anything less. Affordability remains a top priority for me, and I will continue this fight when we reconvene in January.

ARGUMENTS IN SUPPORT: Consumer Reports and TechEquity, co-sponsors of the bill, write in support:

> 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.
>
> [A] recent investigation from Consumer Reports, More Perfect Union and Groundwork Collaborative revealed that Instacart, enabled by the artificial intelligence pricing software Eversight, was running large-scale, hidden price experiments on unsuspecting customers. The team of journalists and researchers analyzed live shopping data from more than 400 Instacart shoppers across four U.S. cities. The findings show many U.S. shoppers who order grocery pickup and delivery through Instacart were unknowingly enrolled in AI-enabled experiments that can charge up to 23% more for the same item ordered from the same store at the same time. Nearly three-quarters of grocery items tested on Instacart showed different prices to different shoppers. Some items carried up to five different price points

[13] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74

simultaneously. For example, people shopping at a Safeway in Washington, D.C., saw a dozen Lucerne eggs listed at five different prices — $3.99, $4.28, $4.59, $4.69, and $4.79. The average price variations observed in the study could cost a household of four about $1,200 per year. Instacart's algorithmic pricing experiments were found to be occurring through the platform at several of the nation's biggest grocery retailers, including Albertsons, Costco, Kroger, Safeway, Sprouts Farmers Market, and Target.

In the wake of the investigation, U.S. Senator Ruben Gallego introduced a bill to prohibit surveillance pricing citing the investigation, at least 12 other members of Congress sent letters to the FTC and to Instacart, the FTC reportedly opened an investigation into Instacart, and Instacart announced it was ending the practice.

In addition, a large coalition of advocacy organizations notes:

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.

ARGUMENTS IN OPPOSITION: Chamber of Progress writes in opposition:

The term "surveillance pricing" suggests that companies are using personal data to charge individual consumers higher prices. **But despite widespread speculation, there is no conclusive evidence that this is actually happening.** In reality, businesses overwhelmingly use consumer data for the opposite purpose: offering discounts, coupons, and targeted promotions that help families save money while 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.

Consumers actively seek out these kinds of deals. A 2024 survey of more than 10,000 consumers found that 91% are willing to share personal data in exchange for value from brands, with discounts, loyalty points, and exclusive access cited as the top motivators. That willingness translates into everyday behavior: 70% of consumers say they value loyalty programs, and about 24% of consumers earning under $40,000 rely on them when choosing where to shop.

The Chamber of Progress continues:

The bill bans any retailer from offering or setting a "customized price" for goods based, in whole or in part, on personally identifiable information collected through electronic surveillance technology. Its definition of PII incorporates the CCPA's expansive definition of "personal information," which includes browsing history, purchase history, IP addresses, and device identifiers.

The bill makes no distinction between using personal data to charge a consumer a higher price and using it to offer a discount. In fact, AB 2564 prohibits any "customized price," capturing both increases and savings. A company that uses browsing history to inflate a price and a grocery store that uses purchase history to send a family a coupon are treated identically.

Eliminating these practices would cost California families real money. Digital coupons alone save the average household $1,465 each year5 Low-income families, especially those with children, are among the most active coupon users, and research published in the Journal of Business Ethics confirms that personalized pricing can direct savings toward the consumers who benefit most from discounts. Banning personalized pricing does not make the market fairer. It makes it less accessible.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Reports (Co-Sponsor)
Tech Equity (Co-Sponsor)
American Federation of Musicians, Local 7
American Federation of State, County and Municipal Employees, Afl-cio
California Federation of Labor Unions
California Food and Farming Network
California Nurses Association
California School Employees Association

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
Kapor Center Advocacy
Laane (los Angeles Alliance for a New Economy)
Lgbt Tech
Oakland Privacy
Privacy Rights Clearinghouse
Public Law Center
Secure Justice
Seiu California
Smart - Transportation Division
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
Naiop California
Orange County Business Council
Technet

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200