Date of Hearing: June 24, 2025
Fiscal: No

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 259 (Wahab) – As Amended June 19, 2025

SENATE VOTE: 30-9

SUBJECT: Fair Online Pricing Act

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 or service based on the consumer's perceived willingness to pay. This can lead to different consumers being charged different prices for the same good or service 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 and services.

This author-sponsored bill tackles this problem by prohibiting prices that are offered to a consumer through the consumer's online device that are generated based on input data related to the device's (1) hardware or hardware state, including battery life; (2) the presence or absence of software, such as apps; or (3) the device's geolocation, unless necessary to reflect the cost of providing the service or as part of real-time dynamic pricing for services such as ride-hailing. The bill also expressly allows for optional coupons, as specified.

The bill is supported by Economic Security California Action and TechEquity Action. It is opposed by a coalition of industry opponents led by California Chamber of Commerce. If passed by this Committee, the bill will next be heard by the Judiciary Committee.

THIS BILL:

1) Defines, among other terms:

    a. "Coupon" as any method by which a consumer receives a discount on the purchase of any item that is funded, produced, sponsored, promoted, or furnished, either directly or indirectly, by a business, including, but not limited to, a paper coupon, a digital coupon, or an instant redeemable coupon.

    b. "Hardware state" as a condition or mode of existence of a system, component, or simulation, including, but not limited to, battery life, number of wireless connections detected, and age of the device, and the content of data, as specified.

    c. "Online device" as a physical object that has built-in resources that allow it to communicate through the internet or a short-range wireless technology and react to interface conditions, including, but not limited to, a laptop computer, a desktop computer, a tablet, a smartphone, or other smart hardware.

2) Prohibits prices that are offered to a consumer through the consumer's online device that are generated based on input data related to the device's hardware or hardware state, the presence or absence of software, or geolocation.

3) Allows for the use of geolocation data to the extent necessary to reflect differences in the costs associated with providing a good or service to different consumers, or to determine a surcharge based on the real-time demand for the product or service in the consumer's vicinity, when the product or service is provided immediately upon request.

4) Excepts from the bill's scope optional coupons that are wholly distinguishable from the price, are available to the general public on the same terms, and that do not incorporate device-specific data as specified above.

5) Provides that the bill does not override duties, obligations, remedies, or penalties under other laws.

EXISTING LAW:

1) Establishes the California Consumer Privacy Act (CCPA). (Civ. Code §§ 1798.100-1798.199.100.)

2) Prohibits a business from selling or sharing the personal information of a child that is 16 years of age or younger, if the business has actual knowledge of the child's age, unless the child, or the child's parent or guardian in the case of children less than 13 years old has affirmatively authorized the sharing of selling of the personal information. (Civ. Code § 1798.120(c).)

3) Provides a consumer, subject to exemptions and qualifications, various rights, including the following:

    a) The right to know the business or commercial purpose for collecting, selling, or sharing personal information and the categories of persons to whom the business discloses personal information. (Civ. Code § 1798.110.)

    b) The right to request that a business disclose the specific pieces of information the business has collected about the consumer, and the categories of third parties to whom the personal information was disclosed. (Civ. Code § 1798.110.)

    c) The right to request deletion of personal information that a business has collected from the consumer. (Civ. Code § 1798.105.)

    d) The right to opt-out of the sale of the consumer's personal information if the consumer is over 16 years of age. (Sale of the personal information of a consumer below the age of 16 is barred unless the minor opts-in to its sale.) (Civ. Code § 1798.12.)

    e) The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses. (Civ. Code § 1798.121.)

f) The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data. (Civ. Code § 1798.125.)

4) Requires a business to provide clear and conspicuous links on its homepage allowing consumers to opt-out of the sale or sharing of their personal information and use or disclosure of their sensitive personal information. (Civ. Code § 1798.135(a).)

5) Establishes the California Privacy Protection Agency (Privacy Agency), vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. The Privacy Agency is governed by a five-member board, with the chairperson and one member appointed by the Governor, and the three remaining members are appointed by the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly. (Civ. Code § 1798.199.10.)

6) 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).)

COMMENTS:

1) **Author's statement**. According to the author:

> We are seeing more instances of companies using our own phones and computers against us to engage in predatory pricing practices. Your battery running low, the type of browser you use, or the neighborhood you live in should not determine the price charged to a consumer. SB 259 addresses these issues by ensuring these characteristics cannot be used as a determinant of the price presented to a consumer. According to the PPIC, 69% of Californians expect bad times economically in the coming year. Meanwhile, these discriminatory pricing tools are being used to extract more and more money from consumers for the same goods and services being offered to their neighbor for a lower price. According to a January poll by Consumer Reports on loyalty programs, consumers don't even want retailers using this type of data as a consideration for discounts they are given. These pricing tools are crushing both consumers and innovation, as businesses no longer need to improve their products and services to earn customer confidence— they simply scrape customer data to figure out how much they can squeeze out of a customer.

2) **Surveillance pricing**. 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."[1]

It is important to distinguish surveillance pricing from dynamic pricing, which adjusts prices in response to market demand. For example, Ticketmaster uses dynamic pricing to increase ticket prices for all consumers when demand rises.[2] In contrast, surveillance pricing treats each 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. In 2012, *The Wall Street Journal* reported that the retailer Staples used an algorithm that set higher prices for consumers who lived further

---

[1] 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.

[2] Cody Mello-Klein, "What is dynamic pricing and why is it hiking ticket prices for Oasis, Taylor Swift and your favorite artist?", *Northeastern Global News* (Oct. 2, 2024), https://news.northeastern.edu/2024/10/02/dynamic-pricing-ticketmaster-oasis-taylor-swift/.

from a rival store.[3] Target also used an algorithm to adjust the price of a TV once a customer entered the parking lot, leading to a $5 million settlement with the City of San Diego for false advertising and unfair business practices related to surveillance pricing.[4] The *SF Gate* recently reported that Bay Area consumers are offered a higher price than users in either Phoenix or Kansas City for the same exact hotel reservations on various hotel booking websites.[5] Additionally, some reporting has indicated that iPhone or Mac users may receive higher prices because of their presumed higher socio-economic status.[6]

Moreover, the use of AI to set prices 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.[7] While it is unclear whether these disparities stem from market forces or algorithmic bias because these companies use opaque algorithms to set prices, a possible conclusion is that algorithmic price setting could reinforce structural inequities.

The extent of surveillance pricing remains uncertain. In the summer of 2024, the FTC 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."[8]

More efficient markets vs competition. Surveillance pricing has the potential to create more efficient markets. By accurately scaling prices to a consumer's willingness to pay, businesses can

---

[3] Jennifer Valentino-DeVries, Jeremy Singer-Vine and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," *Wall Street Journal* (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
[4] Chris Hrapsky, "Target settles lawsuit alleging false advertising, overpricing; fined $5M", *KARE* (Apr. 27, 2022), 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.
[5] Keith A. Spencer, "Hotel booking sites show higher prices to travelers from Bay Area," *SFGATE* (Feb. 3, 2025), https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php. While it is likely that some differences in prices could be due to the compelled fee disclosures, the difference per night for an SF resident compared to a Phoenix resident at the same hotel for the same booking was $511 higher – which simply cannot be due solely to discrepancies from transparency.
[6] *See e.g.* Ram Sundaram, "Do apps charge higher cab fares on iPhones than on Android devices?" *The Times of India* (Dec. 26, 2024), https://timesofindia.indiatimes.com/india/do-apps-charge-higher-cab-fares-on-iphones-than-on-android-devices/articleshow/116665663.cms.
[7] 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.
[8] 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.

sell more goods and services to a broader customer base. Underserved populations could benefit from greater discounts, increasing their access to markets that were previously unavailable to them. In theory, this could enhance overall consumer welfare.

However, this would also suggest that someone with a high willingness to pay would be charged a higher price to offset those discounts. This raises concerns about fairness and could have a chilling effect on those high willingness consumers, making them less likely to participate in the marketplace.

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 what they actually pay disappears as each consumer is charged exactly what they are willing to pay.[9] Therefore, all surplus in the market is captured by the producer, which can reduce consumer welfare. The FTC has reported on this phenomena finding that businesses that had implemented surveillance pricing had already seen 1-5% increases in revenue.[10] 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.[11] However, this outcome depends on consumer data being used solely for pricing, equally available, and 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, leading 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.

3) **What this bill would do.** This bill prohibits prices that are offered to a consumer through the consumer's online device that are generated based on input data related to the device's (1) hardware or hardware state, including battery life; (2) the presence or absence of software, such as apps; or (3) the device's geolocation, except in two circumstances. First, geolocation data may be used to the extent necessary to reflect differences in the costs associated with providing a good or service to different consumers. Thus, legitimate price differences based on providing a good or service to customers in different locations continue to be permissible. A delivery service, for example, could continue to charge higher prices for deliveries to more remote locations. Second, geolocation data can be used to determine a surcharge based on the real-time demand for the product or service in the consumer's vicinity, when the product or service is provided

---

[9] 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
[10] Federal Trade Commission, "FTC Surveillance Pricing 6(b) Study: Research Summaries A Staff Perspective" (Jan. 17, 2025), p. 10.
[11] Zhijun Chen, Chongwoo Choe, Noriaki Matsushima, "Competitive Personalized Pricing", *Management science,* vol. 66, No. 9, September 2020, p. 3799

immediately upon request. This would allow for dynamic pricing, such as for ride-hailing. Finally, the bill does not apply to optional coupons that are wholly distinguishable from the price, are available to the general public on the same terms, and that do not incorporate device-specific data as specified above. The bill does not contain enforcement provisions but would be enforceable under the Unfair Competition Law.[12]

4) **Related legislation**. AB 446 (Ward), which passed this Committee on a 10-3 vote, would prohibit 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 – personally identifiable information or aggregate consumer information – collected through electronic surveillance technology, except (1) price differences based solely on actual cost differentials; (2) publicly disclosed promotional discounts; (3) group-based discounts (e.g., for seniors, students, or veterans); (4) discounts offered through loyalty or membership programs affirmatively joined by the consumer; and (5) pricing by insurers regulated under the Insurance Code.

AB 446 requires that eligibility criteria for qualifying discounts be clearly and conspicuously disclosed before any data is collected and that such discounts be offered uniformly to similarly situated consumers. Covered information collected under an exemption may only be used to administer the discount or program and may not be repurposed for profiling, targeted advertising, or further individualized price setting. Civil penalties of up to $12,500 per violation apply, with treble penalties and disgorgement for intentional violations. The bill also provides for injunctive and declaratory relief and attorney's fees for prevailing plaintiffs.

5) **Intersection with the CCPA.** Opponents contend that the bill is unnecessary and inconsistent with the California Consumer Privacy Act (CCPA). Proponents, on the other hand, contend that existing law is insufficient to protect consumers from the predatory use of their device's information.

In 2018, the Legislature enacted the CCPA,[13] which gave consumers certain rights regarding their personal information,[14] such as the right to: (1) know what personal categories of information about them are collected and sold; (2) request the deletion of personal information; and (3) opt out of the sale of their personal information, or opt in, in the case of minors under 16 years of age.

Two years later, California voters passed Proposition 24, the California Privacy Rights Act, to clarify and expand the protections of the CCPA. Among the new rights granted by Proposition 24 were the right to limit sharing of personal information, correct personal information, and limit use of "sensitive" personal information, which includes the precise geolocation of a person.[15] In adopting the Proposition, voters evinced a clear intent that the CCPA serve as a regulatory floor, not a ceiling. Section 25(a) of Proposition 24 expressly grants the Legislature the authority to amend the CCPA by a majority vote, provided that the amendments are consistent with and further the purpose and intent of the CCPA – namely, "to further protect consumers' rights,

---

[12] Bus. & Prof. Code § 17200 et seq.
[13] AB 375 (Chau, Stats. 2018, Ch. 55).
[14] Civ. Code § 1798.140(v).
[15] Civ. Code §§ 1798.121, 1798.140(ae).

including the constitutional right to privacy."[16] Furthermore, the Proposition states that "in the event of a conflict with other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control."[17]

Opponents note that consumers can exercise their opt-out rights and limit sharing of their information, including their geolocation data. Opponents also point to the provision in the CCPA that prohibits businesses from discriminating against customers who exercise their privacy rights. Additionally, opponents note that the CCPA allows businesses to offer financial incentives for the collection, sale, sharing, or retention of personal information, including different prices to consumers so long as the price is reasonably related to the value provided by the consumer's data.[18]

While the CCPA offers significant privacy protections, it applies only to businesses that (1) earn more than $25 million in annual revenue; (2) buy, sell, or share the personal data of 100,000 or more consumers, households, or devices annually; or (3) earn 50 percent or more of their annual revenues from selling personal information. This bill applies regardless of the size of the business. Furthermore, the CCPA's protections generally place the burden on consumers to affirmatively exercise their rights with respect to each business that collects, shares, sells, or uses their personal information. By contrast, 16 other states allow selling and sharing of sensitive information such as geolocation data only if the consumer opts in, and one state, Maryland, prohibits the sharing of sensitive information entirely.[19] These states have concluded that, with respect to sensitive information, privacy should be the default.

This bill, although not a privacy measure, stands for the proposition that there are certain cases in which the exploitation of consumer information for financial gain should not be the norm. Supporters argue that the categories of information covered in the bill have no bearing on the actual cost of the good or service; thus, the use of such information to set targeted prices is exploitative. Absent regulation, they contend, the practice of setting prices based on such information could undermine consumer trust in market fairness and deepen inequality. In essence, both sides view the bill as a "cost driver"; the question for this Committee is whether the direction is up or down.

ARGUMENTS IN SUPPORT: The Open Markets Institute writes:

> For over a decade, media reports have been exposing the price discrimination schemes employed by companies via surveillance algorithms. Examples of businesses actually and allegedly engaging in these practices include The Princeton Review, Uber, and Staples. Earlier this year, the Federal Trade Commission published a report on surveillance pricing, describing how corporations can use troves of data mined from consumers, directly and indirectly, to set individualized prices for consumers, exploiting their needs and vulnerabilities to charge as high a price as possible.

---

[16] Prop. 24, §§ 3, 25.
[17] Civ. Code § 1798.175.
[18] Civ. Code § 1798.125.
[19] A comparison chart of state privacy laws can be accessed at https://45555314.fs1.hubspotusercontent-na1.net/hubfs/45555314/Slides%20and%20one-pagers/US%20state%20law%20comparison%20chart_2024_July_1.pdf.

There is also reporting that indicates the device itself is used to determine pricing. For example, an iPhone or Mac user may be served a higher price because of their presumed higher socio-economic status.

SB 259 will target these discriminatory pricing practices by excluding specific data relative to a consumer's device for the purposes of calculating a price. The excluded data is defined as the hardware, hardware state such as age and battery life, presence or absence of software on the device, and geolocation data.

SB 259 is a critical piece of pro-consumer legislation that will rein in exploitative surveillance pricing practices and support efforts to increase affordability for all Californians

ARGUMENTS IN OPPOSITION: A coalition of industry opponents, led by California Chamber of Commerce, writes:

SB 259 would prohibit offering any price to a consumer through their online device that is generated, even in part, based on any of the following "input data": (1) the hardware or hardware state of an online device; (2) the presence or absence of any software on an online device; or (3) geolocation data of the device. SB 259 seems to assume that any consideration of this information is inherently predatory or otherwise unfair. As a result, the bill would unfairly cause companies to overhaul their pricing models and strategies at significant cost, to the detriment of both the businesses themselves and their consumers. This threatens not only the profitability of businesses, but also potentially reduces the availability of discounts and personalized deals for consumers.

A law that imposes a broad prohibition on the use of certain data—while carving out only narrow exceptions—fundamentally differs in impact from a legal framework that generally permits data use but targets and prohibits specific, harmful practices. The former chills innovation, constrains legitimate business models, and limits consumer benefit by default. The latter enables responsible data use, encourages economic growth, and focuses enforcement on truly harmful conduct. Imagine if SB 259 predated the gig economy: what would the Covid 19 pandemic have looked like? How many more businesses would have permanently shut their doors?

And while we appreciate that the author has sought to and is open to adding amendments with various exceptions that might recognize various legitimate uses of the geolocation data, the inescapable reality is that narrow exceptions may not account for all legitimate applications of geolocation data in pricing models used, today, and simply ***cannot*** account for potential future legitimate applications of this data that could help increase market competition with more fair and less arbitrary pricing models, tomorrow. Given the likelihood of this bill to have devesting [sic] impacts on our economy, we find it troubling that SB 259 seeks to enact the broadest prohibitions possible with the narrowest expectations necessary – as opposed to surgically drafting narrow prohibitions that are tailored to specific, predatory or unfair pricing practices – particularly when there are extensive protections for how businesses set pricing under existing law. (Emphasis in original.)

REGISTERED SUPPORT / OPPOSITION:

Support

American Federation of State, County and Municipal Employees, Afl-cio
California Federation of Labor Unions, Afl-cio
Economic Security California Action
Open Markets Institute
Techequity Action

Oppose

American Property Casualty Insurance Association
Calbroadband
California Apartment Association
California Bankers Association
California Business Roundtable
California Chamber of Commerce
California Credit Union League
California Hotel & Lodging Association
California Restaurant Association
California Retailers Association
California Travel Association
Chamber of Progress
Civil Justice Association of California (CJAC)
National Association of Mutual Insurance Companies
Personal Insurance Federation of California
Software Information Industry Association
Technet

Analysis Prepared by: Josh Tosney / P. & C.P. / (916) 319-2200