Date of Hearing: July 15, 2025

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
SB 259 (Wahab) – As Amended July 10, 2025

SENATE VOTE: 30-9

SUBJECT: FAIR ONLINE PRICING ACT

KEY ISSUE: SHOULD THE LEGISLATURE PROHIBIT BUSINESSES FROM GENERATING OR OFFERING PRICES TO CONSUMERS BASED ON DEVICE-SPECIFIC DATA—SUCH AS HARDWARE CHARACTERISTICS, SOFTWARE PRESENCE, OR GEOLOCATION?

SYNOPSIS

This bill prohibits businesses from generating or offering prices to consumers through online devices based on certain types of device-specific data. In today's digital marketplace, consumers increasingly encounter prices tailored not by supply and demand but by hidden inferences drawn from their own devices. Businesses are quietly using technical data—such as the battery level, device model, installed software, or physical location of a user's phone or laptop—to segment consumers, assess their perceived willingness to pay, and vary prices accordingly. Unlike traditional dynamic pricing, which adjusts prices for everyone based on market conditions, surveillance pricing creates a world where two people shopping for the same product on the same site at the same time may see entirely different prices—simply because one has a newer phone or is browsing from a wealthier ZIP code. Real-world investigations have documented retailers raising prices when consumers' phones enter parking lots, booking platforms charging more to users in high-income areas, and apps using battery status as a proxy for purchase urgency. These practices are not disclosed, and consumers typically have no way to detect that they are being charged more—or why.

To address these concerns, the bill prohibits businesses from using three categories of input data to generate price offers: (1) the hardware or hardware state of a consumer's device; (2) the presence or absence of software; and (3) the geolocation of the device, subject to narrow exceptions for cost-based regional pricing or real-time delivery surcharges. The bill also clarifies that coupons, discounts, rebates, and sales that are made available to the general public on equal terms, and not based on any of the prohibited three inputs remain permissible. For example, a platform may offer a "50% off for Memorial Day" discount to all users, or a travel site may provide airfare promotions based on airport codes voluntarily entered by consumers—but it may not vary prices using a consumer's IP address, battery level, or local Wi-Fi signals. This author-sponsored measure is supported by a coalition of labor and equity groups, including the California Federation of Labor Unions and Economic Security California Action. It is opposed by a broad coalition of industry, financial, insurance, and tech stakeholders including the California Chamber of Commerce. SB 259 was heard and passed by the Assembly Committee on Privacy and Consumer Protection by a 10-4 vote.

SUMMARY: Prohibits businesses from using device-specific data to generate or adjust prices offered to consumers through online devices. Specifically, **this bill**:

1) Defines key terms, including:

   a) "Hardware state" means 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, data that is erased when an online device is restarted or powered down, and data that is retained when an online device is restarted or powered down.

   b) "Online device" means 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 businesses from generating or offering a price to a consumer through their online device based, in whole or in part, on any of the following:

   a) The hardware or hardware state of the device (e.g., battery life, wireless connections, device age).

   b) The presence or absence of software on the device.

   c) The geolocation of the device, with narrow exceptions.

3) Permits use of geolocation data only when necessary:

   a) To reflect legitimate cost or demand differences associated with providing a good or service in different locations.

   b) To apply a real-time surcharge for goods or services delivered immediately upon request (e.g., rideshare pricing).

   c) To provide accurate pricing information based on price variances at different physical locations, due to legitimate cost or demand differentials or state or local government taxes, duties, or other fees.

4) Clarifies that the bill does not apply to any coupon, discount, rebate, sale or other bona fide promotion that reduces the price of goods or service, provided it is (a) made available to the general public on the same terms and (b) not based on any input data specified 2).

5) Affirms that the duties imposed by this chapter are cumulative and do not displace or diminish any obligations imposed under other laws.

EXISTING LAW:

1) Establishes the California Consumer Privacy Act (CCPA). (Civil Code Sections 1798.100-1798.199.100. All further statutory references are to the Civil Code, unless otherwise specified.)

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 or selling of the personal information. (Section 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. (Section 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. (Section 1798.110.)

   c) The right to request deletion of personal information that a business has collected from the consumer. (Section 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.) (Section 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. (Section 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. (Section 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. (Section 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. (Section 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. (Section 1798.140 (v).)

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

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

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

iii) Precise geolocation.

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

v) Email, mail and text messages.

vi) Genetic data.

vii) Information collected and analyzed relating to health.

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

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

COMMENTS: This bill seeks to address the growing use of consumer device surveillance to facilitate individualized pricing in online commerce. As e-commerce platforms increasingly deploy algorithms that scan device characteristics—such as hardware specifications, installed software, and geolocation—businesses may silently tailor prices in ways that disadvantage certain consumers based on inferred purchasing power or location. This bill prohibits businesses from using these specific categories of device data to generate or adjust prices, unless strictly necessary to account for legitimate cost differences or real-time delivery logistics. By establishing clear boundaries around the use of device-based inputs in pricing, SB 259 aims to safeguard marketplace transparency and prevent covert forms of digital price discrimination.

As explained by 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 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.

Surveillance pricing: efficient or unfair? The growing use of personal device data to generate individualized prices—what the Federal Trade Commission and others call surveillance pricing—has emerged as a covert yet widespread practice in the digital marketplace. According to the initial findings from FTC's 2025 Surveillance Pricing 6(b) Study, surveillance pricing is driven by three categories of tools: (1) price targeting tools, (2) consumer segmentation and profiling tools, and (3) search and product ranking tools. (Federal Trade Commission, *FTC Surveillance Pricing 6(b) Study: Research Summaries, A Staff Perspective* (January 2025), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.) This bill specifically targets the second category—profiling tools that use device-level data to infer characteristics about a user, which then influence the price they see. Profiling tools rely on a wide range of "inputs," such as device model, operating system, battery life, browser type, keyboard language, and location. These inputs can serve as proxies for income, race, behavior, or purchasing power, enabling businesses to algorithmically adjust prices for the same product or service based not on objective cost factors but on the perceived characteristics of the user.

Real-world examples illustrate how device-level profiling is already shaping consumer experiences. In 2022, Target paid $5 million to settle a lawsuit in California alleging that it used geolocation signals to increase online prices when a consumer's phone entered a store parking lot—without disclosing the price change. (KARE11, *Target settles CA lawsuit alleging false advertising*, Dec. 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.) Similarly, a 2025 SF Gate investigation found that hotel booking websites charged Bay Area users up to $500 more for identical listings shown to consumers in lower-income regions, based solely on geolocation data. (SF Gate, *Hotel sites quietly raising prices based on your location*, Jan. 2025, https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.) Earlier reporting revealed that Staples adjusted online prices based on a user's ZIP code, often correlating with local income levels. (The Verge, *Retailers adjusting prices depending on income and location*, Dec. 2012, https://www.theverge.com/2012/12/24/3800472/retailers-adjusting-online-prices-depending-on-income-and-location.)

Device surveillance extends well beyond location. Uber has been accused of charging higher surge prices to consumers with low phone battery—interpreted as a sign they are less likely to delay a purchase. (Vice, *Uber surge pricing and phone battery*, Jan. 2024. https://www.vice.com/en/article/uber-surge-pricing-phone-battery.) Researchers have found that apps like Facebook, TikTok, and X (formerly Twitter) routinely collect data from iPhones—

including system uptime, memory, language settings, and battery status—via push notifications (Mashable, *Facebook, TikTok, X collect data when sending iPhone push notifications,* Jan. 2024, https://mashable.com/article/iphone-apps-push-notifications-data-collection-report.) A UK-based mobile developer notes that even basic apps can access device model, display resolution, charging status, regional settings, and network type. (Glance, *What Data Can I Collect in My Mobile App?,* 2023, https://thisisglance.com/learning-centre/what-data-can-i-collect-in-my-mobile-app.)

Most consumers are unaware that these practices are occurring, let alone that they may influence pricing. Consumers often accept vague or misleading privacy policies without understanding that their data may be sold or repurposed for price targeting. (MSU Today, *How companies are using cell phone data,* Feb. 2019, https://msutoday.msu.edu/news/2019/how-companies-are-using-cell-phone-data.) Meanwhile, surveillance infrastructure has become deeply embedded in apps via location tracking mechanisms invisible to the average user (NYT, Smartphones Are Spies, Dec. 2019, https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html; ZDNet, Big Tech is Actually Doing All This, June 2023, https://www.zdnet.com/article/big-tech-is-actually-doing-all-this-with-your-personal-data-true-or-false/.)

Public opposition to these practices is strong. A nationally representative survey by Consumer Reports in January 2025 found that 76% of loyalty program participants opposed the use of demographic information to determine personalized discounts; and 72% opposed using device data or online behavior for pricing. (Consumer Reports, *Loyalty Programs Survey*, Jan. 2025, p. 9.).

Existing law. Although California's existing privacy laws—such as the California Consumer Privacy Act (CCPA)—give consumers certain rights over their data, including the right to opt out of the sale or sharing (Civil Code Section 1798.120), they do not prohibit the use of that data to generate discriminatory prices. In fact, Civil Code Section 1798.125 (b) explicitly allows businesses to charge different prices based on the "value provided to the business by the consumer's data." This statutory permission, even when paired with notice and choice obligations, offers little recourse against opaque, algorithmically driven price disparities that rely on technical device features invisible to consumers. A further discussion of the intersection of this bill and the CCPA is discussed on pp. 7-8 of the Privacy and Consumer Protection Committee's analysis of this measure.

International and federal regulators have taken note. The Organization for Economic Co-operation and Development (OECD) has acknowledged that while personalized pricing may improve efficiency, it poses serious distributional concerns and is perceived by consumers as unfair and deceptive, particularly when implemented without transparency or consent. (OECD, *Personalized Pricing in the Digital Era*, Apr. 2020, available at https://one.oecd.org/document/DAF/COMP/M(2018)2/ANN10/FINAL/en/pdf.) The FTC's 2025 findings similarly emphasize that these tools are primarily valued by firms for their ability to "boost revenue" and "lower costs." (FTC, 6(b) Study, *supra*, p. 10.)

This bill responds to these developments by establishing a narrow but critical restriction: it prohibits price generation based on a consumer's device hardware, software presence, or geolocation, unless justified by real-time logistics or regional cost variation. By setting guardrails around the use of device-level surveillance for price discrimination, this bill aims to preserve transparency, prevent unfair economic profiling, and uphold consumer trust in the digital marketplace. This bill prohibits businesses from using certain device-specific data to generate or offer prices to consumers through online devices. Specifically, the bill makes it unlawful for a price to be generated, in whole or in part, based on the hardware or hardware state of a consumer's internet-connected device, such as its battery life, number of detected wireless connections, or device age. It also bars the use of information about the presence or absence of software installed on the device, as well as the device's geolocation data, except in three narrowly defined circumstances: (1) when location-based pricing reflects legitimate cost differences associated with providing a good or service to a consumer, (2) when it reflects real-time demand for products or services that are delivered immediately upon request (e.g., rideshare surge pricing), or (3) when it accurately reflects price variances at different physical locations, due to legitimate cost or demand differentials or state or local government taxes, duties, or other fees. Pricing based on input data regarding the presence or type of hardware or software on the online device is always prohibited.

In order to assuage opposition's concerns that the bill bans coupons or discounts entirely, subdivision (b) of proposed Section 22949.82 clarifies that coupons, discounts, rebates, promotions, or sales that are offered to the general public and do not use one of the three prohibited inputs ((1) hardware/hardware state, (2) presence/absence of software, (3) geolocation of device) are permitted. This provision clarifies that widely advertised, non-discriminatory discounts—such as 50% off for Memorial Day or other seasonal sales that are offered equally to all users—are not affected by the bill and remain fully permissible.

This provision also seeks to clarify that common marketing practices that rely on user-supplied information, as opposed to data passively or covertly extracted from a consumer's device, likewise remain permitted. For example, if a travel platform such as Expedia is trying to promote air travel out of Sacramento International Airport (SMF), it would be permitted to offer a discount to a consumer who selects "SMF" from the "Departure" field on their site. In contrast, Expedia would be prohibited from offering the same discount to users whose device IP address or GPS signal indicates that they are physically located in the Sacramento area.

In sum, the distinction this bill draws is between pricing that is generated based on affirmative consumer inputs (which remain permissible) and pricing that is generated based on device-level surveillance (which is prohibited).

Enforcement. This bill does not create a standalone enforcement mechanism but instead operates within California's existing consumer protection framework, most notably the Unfair Competition Law (UCL) (Business and Professions Code Section 17200 *et seq*.). The bill's core prohibitions—against generating or offering prices based on certain inputs—establish clear statutory duties that may be enforced through public and private actions under the UCL and related statutes.

This allows the Attorney General, district attorneys, city attorneys, and county counsel to seek injunctive relief, restitution, and civil penalties. Injured private plaintiffs may also bring actions for injunctive relief and, where appropriate, restitution. Thus, while SB 259 does not impose administrative fines or create a private right of action for damages, it establishes clear statutory boundaries that may serve as predicates for enforcement under existing consumer protection laws.

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.
>
> 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 the California Chamber of Commerce, argue that this bill is a COST DRIVER "due to its significant implications for businesses that rely on dynamic or targeted algorithmic pricing models or strategies." The coalition argues that the SB 259 incorrectly assumes that the collection of the data targeted by the bill is inherently predatory or otherwise unfair. They oppose the broad prohibition with limited exceptions, arguing that it closes the door on potentially unknown and innovative use of such data:

> 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.

They are particularly opposed to the prohibition on the use of geolocation data, arguing that at the very least the term should be narrowly defined:

> As it stands, the bill provides no definition of "geolocation data" leaving it open to interpretation as to what level of granularity would suffice to be considered "geolocation data"—would the mere presence in a city, let alone region or state be geolocation data under the bill?

The coalition argues that there are already legal disincentives to unfair pricing under California's robust consumer protection statutes, and that market forces themselves provide a sufficient disincentive:

> Specifically, in a free market, businesses must compete to survive, which drives better pricing and innovation for consumers. Start-ups disrupt markets by introducing innovative products, forcing inefficient incumbents to adapt or fail. Manufacturers provide discounts to resellers who promote their products over competitors. Loyalty programs are utilized to reward customers who consistently choose one brand over another. Companies generally compete by undercutting rivals with lower prices, improving products, and offering incentives such as rebates and exclusive reseller discounts. They shift constantly based on consumer trends, or market demand.
>
> To make these strategic decisions, businesses rely on data and use algorithmic pricing to understand market conditions and respond in real-time to competitive changes, such as by personalizing deals, offering discounts, and optimizing prices based on demand. Restricting this flexibility by prohibiting the use of certain data or technologies only impairs their ability to respond to market changes, leading to less competitive pricing and reduced consumer benefits, and leading to higher baseline prices for everyone, rather than lower prices under certain times and conditions if you allow businesses to respond to market conditions. And, because so many more small businesses and startups rely on dynamic pricing to compete, overregulation in this area will disfavor them over larger companies, further widening the gap between them and the companies that have fixed pricing structures.
>
> Again, those same market forces that businesses respond to also naturally help keep businesses in check. If they were to truly engage in unfair pricing practices, they would not only risk facing backlash from their own customer base that they need to survive, but they also risk losing customers to their competition, which they cannot afford to do if they wish to thrive. In the end, overregulating legitimate pricing mechanisms limits the ability of businesses to respond to market changes, leading to less competitive prices, and also harming small businesses who rely more heavily on dynamic pricing to compete.

REGISTERED SUPPORT / OPPOSITION:

Support

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

Opposition

American Property Casualty Insurance Association
Association of National Advertisers
Calbroadband
California Apartment Association
California Bankers Association
California Business Roundtable

California Chamber of Commerce
California Credit Union League
California Fuels and Convenience Alliance
California Grocers Association
California Hotel & Lodging Association
California Restaurant Association
California Retailers Association
California Travel Association
Chamber of Progress
Civil Justice Association of California (CJAC)
CTIA
National Association of Mutual Insurance Companies
Personal Insurance Federation of California
Software Information Industry Association
Technet

Analysis Prepared by: Shiran Zohar / JUD. / (916) 319-2334