SB 259 (Wahab)
Version: April 8, 2025
Hearing Date: April 22, 2025
Fiscal: No
Urgency: No
AWM

SUBJECT

Fair Online Pricing Act

DIGEST

This bill prohibits a price from being offered to the seller based on specified data about the consumer's device or location, and requires sellers that use surveillance pricing to disclose their pricing inputs to a consumer upon request, as specified.

EXECUTIVE SUMMARY

Broadly speaking, "surveillance pricing" is the use of advanced algorithms, artificial intelligence and other technologies, along with personal information about consumers—such as their location, demographics, credit history, and browsing or shopping history—to categorize individuals and set a targeted price for a product or service. Surveillance pricing can include sending consumers different ads based on their demographic data, arranging products in different orders based on consumers' locations, and even sending targeted emails to consumers based on their proximity to natural disasters. There are also reports that some businesses are using surveillance pricing to actually offer different prices to consumers for the same product, based on information the business knows, or thinks it knows, about the consumer.

This bill is intended to prohibit surveillance pricing when it results in two consumers being offered different prices for the exact same good or service, when the difference in price is calculated based on information about the consumers' device or location. To that end, the bill prohibits a seller from incorporating into its pricing offer (1) information about the device's hardware or hardware state (this includes battery life); (2) the presence or absence of any software on the online device (such as apps); or (3) the device's geolocation data, with an exception for services that explicitly need to take the consumers location into account (e.g. a ride-sharing service). The bill also requires a seller that uses surveillance pricing to provide a link adjacent to any online price offer that allows a consumer to view or download the input data used to generate the price.

The author has agreed to amend the bill to eliminate the link requirement and instead require a notice to a consumer that a price was generated via an algorithm, and also to clarify that this bill does not displace other existing law that may address practices related to surveillance pricing.

This bill is sponsored by the author and is supported by Economic Security California Action and TechEquity Action. This bill is opposed by the American Property Casualty Insurance Association, the California Chamber of Commerce, the California Credit Union League, the California Retailers Association, Chamber of Progress, the Civil Justice Association of California, the National Association of Mutual Insurance Companies, the Personal Insurance Federation of California, the Software Information Industry Association, and TechNet.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code, pt. 4, tit. 1.81.5, §§ 1798.100 et seq.)

2) 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, div. 7, pt. 2, ch. 4, §§ 17000 et seq.)

3) Defines the following relevant terms within the UPA:
   a) "Person" includes any person, firm, association, organization, partnership, business trust, company, corporation, or municipal or other public corporation. (Bus. & Prof. Code, § 17021.)
   b) "Locality discrimination" means a discrimination between sections, communities, or cities, or portions thereof, or between different locations in such sections, communities, cities, or portions thereof, in this State, by selling or furnishing an article or product, at a lower price in one segment of a location than in another. (Bus. & Prof. Code, § 17301.)

4) Provides that it is unlawful for any person engaged in the production, manufacture, distribution, or sale of any article or product of general use or consumption, with intent to destroy the competition of any regular established dealer in such article or product, or to prevent the competition of any person who, in good faith, intends and

attempts to become such a dealer, to create locality discriminations; nothing prevents a person from meeting, in good faith, a competitive price; however, a seller may not embrace any scheme of special rebates, collateral contracts, or any device of any nature whereby such discrimination is in substance or fact effected in violation of the spirit of the UPA. (Bus. & Prof. Code, §§ 17040, 17049.)

5) Provides that, notwithstanding 4), a person may engage in locality discrimination to the extent it makes allowances for differences, if any, in the grade, quality, or quantity when based and justified in the cost of manufacture, sale, or delivery, or the actual cost of transportation from the point of production, if a raw product or commodity, or from the point of manufacture if a manufactured product or commodity, or from the point of shipment to the point of destination. (Bus. & Prof. Code, § 17041.)

6) Provides that nothing in the UPA prevents:
   a) A selection of customers.
   b) A functional classification by any person of any customer as broker, jobber, wholesaler, or retailer.
   c) A differential price for any article or product as between any customers in different functional classifications. (Bus. & Prof. Code, § 17042.)

7) Provides that the secret payment of allowances of rebates, refunds, commissions, or unearned discounts, whether in the form of money or otherwise, or secretly extending to certain purchasers special services or privileges not extended to all purchasers upon like terms and conditions, to the injury of a competitor and where such payment or allowance tends to destroy competition, is unlawful. (Bus. & Prof. Code, § 17045.)

8) Establishes a general prohibition on unfair competition, known as the Unfair Competition Law (UCL), which covers any unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue, or misleading advertising, and any act prohibited under the False Advertising Law (FAL). (Bus. & Prof. Code, div. 7, pt. 2, ch. 5, §§ 17200.)

9) Provides remedies for a violation of the UCL as follows:
   a) Any person who has been injured by a violation of the UCL may seek restitution injunctive relief in a court of competent jurisdiction. (Bus. & Prof. Code, §§ 17203, 17204.)
   b) The Attorney General, a district attorney, a county counsel authorized by agreement with the district attorney in actions involving violation of a county ordinance, a city attorney of a city having a population in excess of 750,000, a county counsel of any county within which a city has a population in excess of 750,000, a city attorney in a city and county, or, with the consent of the district attorney, a city prosecutor in a city having a full-time city prosecutor,

may, in an action in the name of the people of the State of California, seek injunctive relief, restitution, and a civil penalty. (Bus & Prof. Code, §§ 17204, 17206.)

c) Unless otherwise expressly provided, the UCL's remedies are cumulative to each other and to any other remedies or penalties available under state law. (Bus. & Prof. Code, § 17205.)

This bill:

1) Establishes the Fair Online Pricing Act.

2) Defines the following terms:
    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, and the content of the volatile data and nonvolatile data.
    b) "Nonvolatile data" means data that persists even after an online device is powered down.
    c) "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.
    d) "Volatile data" means data on a live system that is lost after an online device is powered down.

3) Provides that a price offered to a consumer through the consumer's online device shall not be generated in whole, or in part, based upon any of the following input data:
    a) The hardware or hardware state of the online device.
    b) The presence or absence of any software on the online device.
    c) Geolocation data of the online device.

4) Provides that, notwithstanding 3)(c), the geolocation data of the online device may be used, and the consumer's location may be accounted for, to generate a price for any of the following reasons:
    a) To account for the estimated distance and travel time necessary for a service provider to reach the consumer.
    b) To account for the estimated distance and travel time necessary for a service provider to transport the consumer to another location, or to transport a product to the consumer.
    c) To determine a surcharge based on the real-time demand for the product or service in the consumer's immediate vicinity, when the product or service is provided immediately upon request.

5) Provides that, subject to 6) and 7), below, a person shall cause to be placed adjacent to any price displayed by the person to a consumer on the consumer's online device a conspicuous link that meets all of the following criteria:
   a) The link is clickable text that, if clicked, displays or links to a list containing any input data used to generate the price.
   b) The text of the link is in a type size that is at least 90 percent of the type size of the displayed price.
   c) The link can be used to download a list of input data or to have the list of input data sent to an email address of the consumer's choice.

6) Provides that, if an online device cannot display a link pursuant to 5) because the online device lacks a physical display, the person shall create an alternate mechanism for providing access to the list of input data, which shall be available for no fewer than 14 calendar days.

7) Provides that 5) does not apply to a pricing offer that is made on the same terms to the general public and does not incorporate device-specific data in devising the price.

COMMENTS

1. Author's comment

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 directly targets these issues. According to the Public Policy Institute of California, 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. 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: Big Business is watching

Broadly speaking, "surveillance pricing" is "the use of advanced algorithms, artificial intelligence and other technologies, along with personal information about consumers—such as their location, demographics, credit history, and browsing or shopping history—to categorize individuals and set a targeted price for a product or

service.[1] The FTC is currently conducting an investigation into surveillance pricing and identified, in its initial findings, three main types of surveillance pricing:

1. Price-targeting tools: these tools "use algorithms that take data collected about consumer behavior and market conditions as inputs and generate targeted prices for a buyer."[2]
2. Consumer segmentation and profiling tools: these tools "create unique consumer profiles and divide consumers into segments based on attributes or behaviors that are either inferred or explicitly defined."[3]
3. Search and product ranking tools: these tools "can use consumer segments or real-time behavioral data associated with a shopper to affect what products are given prominence on a given webpage."[4]

These tools are enabled by data gleaned from browser cookies and mobile software development kits, data provided directly to the seller by the consumer, and inferences made by the seller (or, more likely, the seller's algorithm or AI) based on other information gleaned about the consumer.[5]

There are too many real-world applications of surveillance pricing to list, but examples include:

- The Princeton Review charged higher fees for its test preparation services based on customers' zip codes—prices ranged from $6,600 to $8,400—and "Asians [were] almost twice as likely to be offered a higher price than non-Asians."[6]
- Target was found to offer different prices based on the consumer's proximity to a Target store, increasing the offered price of a television by $100 and the offered price of a car seat by $72 when the user was in a Target parking lot.[7]
- United Airlines charged more for fares based on whether the user purchased the ticket through the airline's mobile app (lower price) or a desktop computer (higher price).[8]

---

[1] Federal Trade Commission (FTC), Press Release: FTC Issues Orders to Eight Companies Seeking Information on Surveillance Pricing (Jul. 23, 2024), *available at* https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing. All links in this analysis are current as of April 17, 2025.

[2] FTC, FTC Surveillance Pricing 6(b) Study: Research Summaries (Jan. 2025), p. 3, *available at* https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[3] *Id.* at p. 4.

[4] *Id.* at pp. 4-5.

[5] *Id.* at pp. 5, 8.

[6] Angwin, et al. *The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review* (Sept. 1, 2015) ProPublica, *available at* https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review.

[7] Hrapsky, *The Target app price switch: What you need to know* (Jan. 27, 2019; updated Feb. 6, 2019) KARE11.com, https://www.kare11.com/article/money/consumer/the-target-app-price-switch-what-you-need-to-know/89-9ef4106a-895d-4522-8a00-c15cff0a0514.

- Orbitz changes its ordering of suggested hotels based on the brand of device the consumer is using, displaying pricier hotels more prominently to Mac users than PC users.[9]

The FTC also floated a number of hypothetical "use cases" in its preliminary findings that it did not attribute to a particular company:

- A "health supplies company that has identified some of its customers as homeowners living in an area that is undergoing flooding could target them with promotional campaigns for stress-relief supplements."[10]
- If a "customer who visits a sports betting website demonstrates hesitation by lingering on the homepage longer than expected or moves their cursor towards the button to close out their browser, the website may trigger a pop-up showing popular sporting events to incentivize the visitor to remain on the website and place a bet."[11]
- "[I]f a consumer is profiled as a new parent, the consumer may be intentionally shown higher[-]priced baby thermometers on the first page of their in-app purchases based on their residential zip code and time of purchase. These tools could also potentially be used to collect behavioral details that a retailer could use to forecast a customer's state of mind, like using a shopper's selection of "fast-delivery" shipping on an order of infant formula to infer that a shopper could be a rushed parent who may be less price-sensitive."[12]

Letters from the opposition to this bill also appear to confirm that businesses are using data collected about a consumer's device, the device's battery life, and the consumer's location when determining what prices to offer a consumer: a coalition of the bill's opponents state that the surveillance pricing prohibitions in this bill would "unfairly cause companies to overhaul their pricing models and strategies at significant cost."

3. <u>This bill prohibits a narrow category of surveillance pricing and requires sellers who use surveillance pricing to disclose their inputs</u>

This bill is intended to prohibit surveillance pricing when it results in two consumers being offered different prices for the exact same good or service, when the difference in price is calculated based on information about the consumers' device or location. To that end, the bill prohibits a seller from incorporating into its pricing offer (1)

---

[8] Elliott, *Why you're seeing wild price differences on 2 tickets for the same flight, and how to beat that* (Aug. 31, 2020; updated Sept. 21, 2020) Seattle Times, https://www.seattletimes.com/life/travel/understanding-dynamic-pricing-for-airfare-travel-troubleshooter/.
[9] Memmott, *Orbitz Shows Mac Users Pricier Hotel Options: Big Deal or No Brainer?* (Jun. 26, 2012) NPR, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.
[10] Surveillance Pricing 6(b) Study: Research Summaries, *supra*, at p. 6.
[11] *Ibid.*
[12] *Id.* at p. 5.

information about the device's hardware or hardware state (this includes battery life); (2) the presence or absence of any software on the online device (such as apps); or (3) the device's geolocation data. The bill contains exceptions to the geolocation prohibition to ensure that a seller can still use geolocation data where the information is relevant (e.g., when Lyft needs to know where the customer needs to be picked up and how far they need to be driven).

The bill also requires a seller that uses surveillance pricing to provide a link adjacent to any online price offer that allows a consumer to view or download the input data used to generate the price. A seller that does not use surveillance pricing—i.e., by offering the same price to all potential buyers—is not required to include such a link. In response to concerns from opposition about the practicality of this provision, the author has agreed to remove the link requirement and replace it with a requirement that a seller that uses an algorithm to generate a price include a clear and conspicuous notice of that fact adjacent to the price. The author has also agreed to amend the bill to make clear that this bill is intended to apply in addition to, not instead of, other existing laws that may bear on surveillance pricing conduct.[13] The amendments are set forth in Part 5 of this analysis.

SB 259 does not contain an independent remedy; however, a person harmed by a violation of the bill's requirements could seek restitution or injunctive relief under the UCL, and the Attorney General and other public prosecutors could seek civil damages from a violator in the name of the People of the State of California.

4. Is surveillance pricing already prohibited by law?

California has a web of legal frameworks which could overlap with some forms of surveillance pricing. As discussed below, however, it does not appear that any legal regime squarely addresses the types of surveillance pricing addressed in this bill. As noted above, the author has agreed to amend the bill to make clear that this bill does not preclude recovery under any other relevant law. This Part discusses three frameworks which may, but do not directly, address surveillance pricing.

a. *The CCPA*

The CCPA grants consumers certain rights with regard to their personal information, as defined.[14] With passage of the California Privacy Rights Act in 2020, the CCPA got an overhaul. Consumers are now afforded the right to receive notice from businesses at the point of collection of personal information and the right to access that information at any time.[15] The CCPA also grants a consumer the right to request that a business delete

---

[13] For example, offering the same product to different consumers on the basis of the consumer's membership in a protected class could violate the Unruh Civil Rights Act. (*See* Civ. Code, § 51.)
[14] Civ. Code, div. 3, tit. 1.81.5, §§ 1798.100 et seq.
[15] *Id.*, §§ 1798.100, 1798.110, 1798.115.

any personal information about the consumer the business has collected from the consumer.[16] A coalition of the bill's opponents argues that this bill is, at least in spirit, contrary to the CCPA. Under this theory, the CCPA's provisions allowing a user to opt out of the sale of their data, and allowing them to limit the use of their precise geolocation data, prevent the state from adopting any other laws relating to the use of consumer data. But the CCPA does not purport to occupy the field: "in the event of a conflict between other laws and the provision of the [CCPA], the provisions of the law that afford the greatest protection for the right of privacy shall control."[17] And more fundamentally, this bill is a consumer protection measure, not a privacy-focused measure; the opponents have not cited, and Committee staff are not aware of, anything suggesting the CCPA is intended to prevent the Legislature from enacting consumer protection measures that happen to relate to the use of consumer data. It therefore seems unlikely that the CCPA already provides the protections this bill seeks to provide, or that the CCPA would prevent this bill from taking effect.

> b. *The UPA*

The UPA bans a range of business practices, including locality discrimination and offering "secret payments" in the form of discounts or rebates, but with the caveat that the person engaging in these practices is doing so to thwart competition.[18] While the California Supreme Court has held that the UPA's protection of competition sometimes extend to purchasers[19]—so that a seller cannot discriminate between purchasers who are competitors in the market—it does not appear that the UPA's protections have been extended to consumers in a case where the seller did not intend to harm its competitors or to destroy competition among its purchasers.[20] To the extent surveillance pricing is used to raise consumer prices, without an intent to harm competition, it is not clear that surveillance pricing could fall under the UPA.

> c. *The UCL*

Finally, there's the UCL. As explained by the California Supreme Court:

> The [UCL] defines "unfair competition" to mean and include "any unlawful, unfair, or fraudulent business practice act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by the [FAL]. The UCL's purpose is to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.[21]

---

[16] *Id.*, § 1798.105.

[17] *Id.*, § 1798.175.

[18] Bus. & Prof. Code, §§ 17040-17151.

[19] *See ABC International Traders, Inc. v. Matsushita Electric Corp.* (1997) 14 Cal.4th 1247,

[20] *Id.* at p. 1268.

[21] *Kasky v. Nike* (2002) 27 Cal.4th 939, 949 (cleaned up).

The UCL's prohibition on unlawful, unfair, or fraudulent business practices creates three separate theories of liability: a business practice violates the UCL if it is unlawful <u>or</u> unfair <u>or</u> fraudulent.[22] "In creating this distinction, the Legislature recognized that unfair or fraudulent business practices may run the gamut of human ingenuity and chicanery and sought to account for the creative nature of the scheming mind."[23] Committee staff are not aware of any case law considering whether the UCL is broad enough to cover surveillance pricing under the unfair or fraudulent prongs.

5. <u>Amendments</u>

As discussed above, the author has agreed to amend the bill to include (1) a scaled-back disclosure mechanism, and (2) a provision clarifying that the bill's obligations and remedies are not exclusive. The amendments also include additional definitions required for the new disclosure mechanism. The amendments are as follows, subject to any nonsubstantive changes the Office of Legislative Counsel may make:

<u>Amendment 1</u>

At page 2, between lines 8 and 9, add the following:

> (a) "Algorithmic pricing system" means a software, computer system, computer process, algorithmic program, or artificial intelligence that automates the setting of price.

> (b) "Artificial intelligence" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

<u>Amendment 2</u>

At page 3, delete lines 13 through 31, and insert:

> (b) Subject to subdivision (c), to the extent it is technically feasible, a person shall cause to be placed clearly and conspicuously and adjacent to any price for which an algorithmic pricing system was used in whole, or in part, to determine the price, the following disclosure: "Price generated with an algorithmic pricing system".

<u>Amendment 3</u>

At page 3, in line 32, delete "(d)" and insert "(c)"

---

[22] *E.g.*, *Beverage v. Apple, Inc.* (2024) 101 Cal.App.5th 736, 747-748.
[23] *Id.* at p. 748.

Amendment 4

At page 3, after line 34, insert the following:

22949.81.2 (a) The duties and obligations imposed by this chapter are cumulative with any other duties or obligations imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law.

(b) The remedies or penalties provided by this chapter are cumulative to each other and to the remedies or penalties available under all other laws of the state.

6. Arguments in support

According to Economic Security California Action:

SB 259 addresses discriminatory pricing practices that exploit consumers based on their device, including:
- tracking whether a competing app is installed and using that fact to adjust pricing in their favor;
- charging a consumer using an older phone or one with low battery life more than someone with a newer device in perfect condition; or
- using the device's s geographic location to determine what price the user sees, regardless of the actual cost of the good or service

None of these factors have any legitimate bearing on the value of the product or service being sold. Instead, they reflect a troubling trend: the use of one's personal device to segment consumers and extract maximum profit, often at the expense of those with fewer resources.

SB 259 brings much-needed transparency and fairness to online pricing by limiting how information about a l device can be used and requiring clear disclosures when differential pricing is employed.

7. Arguments in opposition

According to the Chamber of Progress:

SB 259 adopts an expansive and inflexible approach to regulating how companies use device-related information in pricing, prohibiting consideration of factors such as hardware state, device type, and software presence. The sweeping restrictions in Section 22949.82.1(a) risks outlawing many legitimate and consumer-benefiting uses of contextual data. For example, a retailer might reasonably use the age or operating system of a device to offer relevant

promotions to users on mobile devices, time-sensitive discounts to users on older smartphones, provide promotional pricing for users on budget devices that often correlate with price sensitivity, or test regionally relevant price points based on common device types—all actions that are not exploitative, but rather tailored to expand access and deliver more affordable options to consumers.

Banning the use of this information entirely assumes a one-size-fits-all model of fairness that ignores the diversity of consumer needs and preferences. In doing so, it risks stifling innovation in dynamic pricing and digital commerce, particularly innovations that aim to reduce friction, increase inclusivity, and lower costs for consumers.

SUPPORT

Economic Security California Action
TechEquity Action

OPPOSITION

American Property Casualty Insurance Association
California Chamber of Commerce
California Credit Union League
California Retailers Association
Chamber of Progress
Civil Justice Association of California
National Association of Mutual Insurance Companies
Personal Insurance Federation of California
Software Information Industry Association
TechNet

RELATED LEGISLATION

Pending legislation: AB 446 (Ward, 2025) prohibits a person or business from engaging in surveillance pricing, defined as using specific or aggregated information about a consumer or consumers gathered through the use of electronic surveillance technology to set the price of a commercial good or service that differs from the standard price, unless certain conditions are met. AB 446 is pending before the Assembly Judiciary Committee.

Prior legislation: None known.

****