The Computer & Internet Lawyer

Volume 44 ▲ Number 1 ▲ January 2027

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

All Eyes on Personalized Pricing: What Stakeholders Need to Know

By Raqiyyah Pippins, William Hallett Efron, Danait Mengist and Kayla Hill-Jones

The Federal Trade Commission (FTC) recently put forth a "Proposed Enforcement Policy Statement Regarding Personalized Pricing."[1] The proposed statement comes during a time of increasing concern by federal and state enforcers that modern data collection practices can allow businesses to use consumers' personal data to set prices according to the amount they believe an individual consumer is willing to pay.

Personalized pricing (also referred to as surveillance pricing) has become an enforcement priority for many state legislatures and attorneys general. Importantly, while, until recently, much of the state activity was centered on grocery retail and online food delivery industries, the FTC's statement is industry agnostic, instead centering on whether consumers reasonably expect that the prices they see "will not be any different for them than they will be for their friends or neighbors."[2] The FTC's proposed statement also arrives on the heels of New Jersey passing the first state law on personalized pricing that includes a private right of action.

Dozens of surveillance pricing bills, and a parallel set addressing electronic shelf labels, are pending across roughly two dozen states, reinforcing the importance of companies anticipating the legal and regulatory risks that can be triggered by the use of personalized pricing in the United States.

This article summarizes the proposed statement, evaluates it against the backdrop of state personalized pricing laws, and closes with key takeaways for companies considering personalized pricing in the United States.

FTC'S PROPOSED ENFORCEMENT POLICY STATEMENT

The FTC's draft statement acknowledges that "Congress has not given the Commission the authority to prohibit personalized pricing in all circumstances." However, in the FTC's view, where consumers reasonably expect that prices will not vary based on their personal data, businesses engaged in personalized pricing would likely violate Section 5 of the FTC Act if they fail to clearly and conspicuously disclose when prices are personalized, the basis for the

The authors, attorneys with Arnold & Porter Kaye Scholer LLP, may be contacted at raqiyyah.pippins@arnoldporter.com, william.efron@arnoldporter.com, danait.mengist@arnoldporter and kayla.hill-jones@arnoldporter.com, respectively.

personalization, and the types of data used. The FTC presents its statement as an extension of the Trump administration's stated commitment to transparent pricing and affordability and expresses its intent "to enforce the law aggressively against any deceptive or unfair personalized pricing practices that violate Section 5 of the FTC Act or any other law enforced by the Commission."[3]

According to the FTC, modern forms of data collection may enable companies to engage in personalized pricing in places that reasonable consumers would not expect, thereby causing consumer harm. As an example, the FTC asserts that consumers "reasonably expect" a product listing on a retailer website to be the same price that anyone else browsing to that listing would see, and that not knowing the pricing is personalized could impact "consumers' decisions regarding where to shop, whether and where to comparison shop, and other important considerations impacting the purchase process."

The FTC also emphasizes that many Americans do not understand just how much data they generate, nor how the data may be used, "including, potentially, to price products and services uniquely for them on the basis of their intimate details." Further, according to the proposed statement, "the limited economic research" on personalized pricing suggests "the more sophisticated personalized pricing practices become, the less likely consumers are to benefit."

These premises underpin the proposed approach to enforcement articulated in the draft statement.

APPLICATION OF SECTION 5 OF THE FTC ACT TO PERSONALIZED PRICING

The FTC acknowledges that consumers do not expect prices to never vary and notes prices presented to individual consumers may vary because of supply and demand, geography, taxes, market conditions, risk-based underwriting, or the nature of certain products such as insurance and credit. The FTC's concern with varying prices arises when the personalized pricing is "deceptive" or "unfair."

Under Section 5 of the FTC Act, an act or practice is deceptive if it involves a representation, omission, or practice that is material and likely to mislead the consumer acting reasonably in the circumstances to the consumer's detriment.[4] An act or practice is unfair under Section 5 if it causes, or is likely to cause, substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition.[5] The FTC's statement explains that these principles apply with the same force to personalized pricing as to any other commercial conduct.

The FTC frames personalized pricing as potentially deceptive where a business expressly or impliedly represents that a price is standard, static, broadly available, or based on ordinary commercial factors when, in fact, the price is personalized to the individual consumer. Examples include:

- Representing, expressly or by implication, that a price is static or widely offered when it is in fact personalized;
- Failing to disclose personalization where the consumer reasonably believes the price is static or widely offered; and
- Misrepresenting the basis or effect of the personalization, for example, presenting a price derived from inferences about disposable income or shopping behavior at other firms as a loyalty discount based on purchase history.[6]

According to the FTC, the failure to disclose this information is material because consumers who are unaware of personalization cannot take steps to avoid a higher price, such as using a virtual private network or private browsing, switching to a retailer that does not personalize, or declining the transaction altogether.[7]

Per the FTC, personalized pricing may be unfair when it causes a consumer to pay a higher price and the consumer cannot avoid the higher price because the fact or nature of the personalization has been concealed. Under this unfairness theory, the FTC explains that the higher price constitutes the substantial injury and the injury is not reasonably avoidable because the consumer lacks the practical tools to identify, dispute, correct, or avoid the data or inferences used to set the higher personalized price. The FTC declined to take a position on whether personalized pricing can be unfair when clearly and conspicuously disclosed.

ADEQUATE DISCLOSURES UNDER THE PROPOSED ENFORCEMENT POLICY STATEMENT

In the FTC's view, when consumers reasonably expect that prices will not vary based on personal data, businesses that engage in personalized pricing without making adequate disclosures would likely violate Section 5. The proposed statement provides that, "[t]o be effective, personalized pricing disclosures should be clear and conspicuous and include all relevant information, such as the fact that the price is personalized, the

basis of that personalization, and the type of data used."[8] The statement further asserts that a vague statement that a consumer has received a "specially selected" price would likely be misleading if it omits material information about how the price was determined. Conversely, according to the FTC, a clear and conspicuous disclosure that "a personalized price is based on a consumer's estimated willingness to pay derived from data about that consumer's previous purchases from the same retailer through the same login account" would likely be adequate (if accurate and complete).[9] Such a disclosure, the FTC explains, would likely be enough to dispel any reasonable expectation that the posted price is not personalized and give the consumer the information needed to identify potentially incorrect information, take measures to avoid the personalized price, or avoid the future collection of data for personalized pricing.[10]

REPRESENTATIVE EXAMPLES OF PERSONALIZED PRICING PRACTICES THAT MAY VIOLATE THE FTC ACT

The statement offers a non-exhaustive list of scenarios in which personalized pricing without adequate disclosure would raise Section 5 concerns.[11] The examples range well beyond the grocery and food delivery sectors that have dominated state activity and include:

- A food delivery company pricing higher based on data suggesting a consumer cannot leave home to buy food;
- A grocery chain pricing milk higher based on data showing children live in the household;
- A hotel pricing higher based on inferred funeral travel;
- A rideshare company pricing higher for transport to a medical facility based on data suggesting an emergency or charging customers more based on the absence of competitor apps on their phones;
- A retailer pricing a home-security system higher based on court filings showing recent crime victimization; and
- A retailer pricing higher on its website based on the consumer's in-store location while browsing.

A common thread among the FTC's examples is the use of sensitive or vulnerability-adjacent data that suggests that the consumer will pay a higher price than others, such as household composition, health, bereavement, crime victimization, physical location, or the absence of comparison-shopping options.

PARALLEL DEVELOPMENTS AT THE STATE LEVEL

The policy statement comes during a time where states are attempting to tackle personalized pricing on their own. Four states have already enacted laws directly addressing personalized pricing, with approaches spanning from disclosure requirements to outright prohibition. For example:

- New York's Algorithmic Pricing Disclosure Act requires companies to disclose to consumers when their personal data is used to set a price, using a prescribed disclosure stating: THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA.[12]
- Maryland's Protection from Predatory Pricing Act, which applies only to large food retailers and third-party food delivery providers, bars use of personalized pricing by these companies out right, with a few exceptions.[13]
- Connecticut's omnibus privacy law takes a hybrid approach, imposing a disclosure requirement on businesses that use consumers' personal data to set prices (THIS PRICE WAS INCREASED BY A PRICE SETTING DEVICE USING YOUR PERSONAL DATA), while barring retail sellers and third-party food delivery services from surveillance pricing outright.[14]

Each of these laws can only be enforced by the state attorney general.

In July 2026, New Jersey became the first state to prohibit the use of personalized pricing, while including a private right of action. New Jersey's Fair Price Protection Act, signed on July 23, 2026, makes it an unlawful practice to use surveillance pricing for groceries and other foodstuffs (subject to a few exceptions including cost-based price differences and bona fide discounts). A violation of the Fair Price Protection Act is also deemed a violation of New Jersey's UDAP statute, the New Jersey Consumer Fraud Act, which enables consumers to enforce the statute directly, including on a class basis, for treble damages, attorneys' fees, and costs. The attorney general may separately recover actual damages or $50,000 per violation, whichever is greater. The Fair Price Protection Act also reaches pricing hardware, barring electronic shelf labels connected to surveillance pricing technology and imposing a one-year

moratorium on new electronic shelf label deployments beginning February 1, 2027.[15] The other enforcement provisions take effect on August 1, 2027.

Other notable state bills under consideration include the following:

- New York's One Fair Price Act (S.8623B/A.9349B), which passed both chambers in June 2026 and awaits signature by Governor Hochul. The bill would amend Section 349-a of the General Business Law to prohibit surveillance pricing outright, moving New York from disclosure to prohibition and reaching well beyond the grocery sector. Bona fide discounts, coupons, loyalty programs, and senior pricing that are uniformly available to consumers meeting the required eligibility would be preserved. The attorney general would enforce the prohibition as an unfair and deceptive practice. If signed, the act would take effect 180 days later.[16]

- California's AB 2564, which would bar retailers who sell tangible personal property from setting a customized price for a good based on personally identifiable information collected through electronic surveillance. The bill passed the California Assembly in May 2026 and remains before the Senate, where it was further amended in August 2026; the scope of its carve-outs for discounts and loyalty programs has been a focus of that process.[17]

- Washington's companion bills HB 2481 and SB 6312, which would ban use of personalized pricing for groceries, restrict surge pricing on essential goods, and impose a four-year moratorium on electronic shelf labels, with violations enforceable under the state Consumer Protection Act.[18] Washington's Consumer Protection Act would be enforceable by the attorney general, while also providing a private right of action under the state UDAP statute.

Illinois, with its HB 4248 and SB 2255, is among the other states considering outright bans, and by some counts, more than 40 personalized pricing bills are pending across two dozen states. However, not all advance: in June 2026, Colorado's governor vetoed HB 26-1210, a comparable bill that would have prohibited using data analytics to set individualized prices for consumers and individualized wages for employees.

CONCLUSION

To mitigate risk, companies that use, or are considering use of personal data as a pricing input may want to consider steps discussed below.

Continue to Monitor and Account for Legal Developments at the Federal and State Level

There are notable differences between the FTC's proposed enforcement policy statement and the approach taken by some states with respect to personalized pricing. As such, a compliance program calibrated to New York's or Connecticut's prescribed disclosure language, may not be adequate in the FTC's view. Conversely, the clear and conspicuous disclosures outlined by the FTC will not facilitate compliance with the Maryland, Connecticut, or New Jersey laws to the extent they bar personalized pricing for certain goods outright. These differences may become more pronounced if states pass broader bans. Accordingly, compliance and risk assessment in this area must account for an evolving (and at times inconsistent) enforcement and regulatory landscape at the federal and state level.

Inventory the Pricing Inputs

Identify whether any pricing model — in-house or vendor-supplied — uses individual-level data, including browsing patterns and purchase history, location, device information, household composition and income, or inferences from such data.

Audit Disclosures Against the FTC's Proposed Criteria

Confirm that disclosures convey the fact of personalization, its basis, and the categories of data involved, and that disclosures appear clearly and conspicuously where consumers see the affected prices rather than in linked terms.

Screen for Sensitive Inferences

Evaluate whether any pricing model uses sensitive or other individual level data as proxies for conditions that might make consumers more vulnerable to paying higher prices, including those identified in the FTC's statement: medical emergencies bereavement, household composition, crime victimization, and constrained shopping alternatives. Using such individual data in this manner to charge higher prices without adequate disclosures is more likely to draw enforcement scrutiny.

Confirm the Consent Chain

The FTC's statement also cautioned that businesses that collect, use, or disclose consumers' personal data for the purpose of personalized pricing without adequate disclosures or without obtaining consent may violate Section 5. Accordingly companies should verify and document that data used for pricing, including data

obtained from third parties, was collected with disclosure and consent covering that use.

Reassess How Prices Are Presented

Representations that a price is a "standard," "everyday," or "member" price may create the static-price expectation the FTC treats as the predicate for a deception claim, and the proposal indicates that labeling a price "special" or "selected" without explaining how it was determined would likely be misleading.

Treat Pricing-Data Governance as Litigation Risk Management

New Jersey's new law (which provides for a private right of action and deems violations to also be violations of its UDAP statute) coupled with the FTC's unfairness and deception theories as articulated in the proposed statement[19] could be relied upon by the plaintiffs' bar to challenge personalized pricing practices under other state UDAP statutes. Thus, it is prudent to contemplate nuisance demands and litigation when assessing the potential risks associated with implementing personalized pricing strategies.

Notes

1. Fed. Trade Comm'n, Proposed Enforcement Policy Statement Regarding Personalized Pricing (Aug. 19, 2026) (hereinafter Proposed Statement).
2. Proposed Statement, supra note 1.
3. Proposed Statement, supra note 1.
4. FTC Policy Statement on Deception, 103 F.T.C. 174 (1984) (appended to In re Cliffdale Assocs., Inc., 103 F.T.C. 110 (1984)).
5. FTC Policy Statement on Unfairness, 104 F.T.C. 949, 1070 (1984) (appended to In re Int'l Harvester Co., 104 F.T.C. 949 (1984)).
6. Id. at 4-5.
7. Id. at 5.
8. Id. at 6.
9. Id. at 7.
10. Id. at 7.
11. Id. at 7-8. The examples are illustrative only. Id. at 5 n.18.
12. N.Y. Gen. Bus. Law § 349-a (Algorithmic Pricing Disclosure Act).
13. Protection from Predatory Pricing Act, H.B. 895, 2026 Gen. Assemb., Reg. Sess. (Md. 2026).
14. An Act Concerning Consumer Privacy and Protection, Conn. Pub. Act No. 26-64 (S.B. 4) (2026).
15. Fair Price Protection Act, P.L. 2026, c. 65 (A4085/A4523) (N.J., signed July 23, 2026), available at https://pub.njleg.gov/Bills/2026/A4500/4085_U1.HTM.
16. One Fair Price Act, S. 8623-B / A. 9349-B, 2025-2026 Reg. Sess. (N.Y. 2026).
17. A.B. 2564, 2025-2026 Reg. Sess. (Cal. 2026).
18. H.B. 2481 & S.B. 6312, 2026 Reg. Sess. (Wash. 2026).
19. There is no private right of action under Section 5 of the FTC Act. However, many states have UDAP laws (sometimes referred to as "Little FTC Acts") that both provide a private damages remedy and look to interpretations of Section 5 either as a matter of statutory command or judicial interpretation. Accordingly, the risk of private actions in such states exists even in the absence of a specific ban on or regulation of personalized pricing.

Copyright © 2027 CCH Incorporated. All Rights Reserved.
Reprinted from *The Computer & Internet Lawyer*, January 2027, Volume 44, Number 1, pages 3–7 with permission from Wolters Kluwer, New York, NY, 1-800-638-8437, www.WoltersKluwerLR.com

