CLIENT ALERTS & INSIGHTS

AI-Driven Personalized Pricing: The FTC's New Enforcement Posture and the Broader Legal Landscape

SEPTEMBER 10, 2026

Authors: Michael D. Meuti, Ruddy S. Abam

Featured Practices: Litigation, Artificial Intelligence (AI)

Featured Industries: Retail & E-Commerce

Key Takeaways

- The FTC's proposed August 2026 enforcement policy makes AI-driven personalized pricing a key enforcement focus, warning that businesses may violate Section 5 if they use consumer data to tailor prices without clearly disclosing the practice and the data behind it.
- The proposal is the most-significant federal regulatory action to date targeting AI-powered pricing and signals heightened scrutiny of personalized pricing practices.
- Companies should review any personalized pricing practices, ensure clear disclosures and appropriate consent for data use, and assess compliance risks across consumer-protection, privacy, and AI-governance frameworks.

By now, we all know that artificial intelligence is a transformative tool for business. Companies are already using it to optimize supply chains, automate customer service, and generate novel insights from vast datasets. Among AI's more controversial commercial applications, however, is a practice that strikes at the heart of consumer expectations: using AI to analyze personal data and set individualized retail prices for each consumer based on that consumer's estimated willingness to pay.

On August 19, 2026, the Federal Trade Commission signaled that this practice is in its enforcement crosshairs. The FTC's proposed enforcement policy statement on personalized pricing stopped short of an outright ban, but establishes a framework under which inadequately disclosed personalized pricing may violate Section 5 of the FTC Act as either deceptive or unfair. The policy statement represents the most-significant federal regulatory action to date targeting a specific commercial application of artificial intelligence: using personal consumer data to differentiate the prices offered to different consumers.

This article examines the FTC's proposed policy in context. Part I surveys the commercial promise of AI-driven individualized pricing and the economic literature on its welfare implications. Part II details the Commission's new enforcement framework. Part III maps the broader legal risks that companies face when deploying personalized pricing-including exposure under state unfair-and-deceptive-practices laws, data-privacy statutes, the Fair Credit Reporting Act, emerging state personalized-pricing legislation, civil-rights laws, and class-action theories.

I. AI's Promise for Individualized Marketing and Pricing

Nearly every industry is embracing AI's commercial potential. Among the most frequently cited use cases is AI's ability to sift through massive troves of consumer data-browsing behavior, purchase history, location data, income proxies, demographic information, and other personal data-to help companies better market to individual customers. But the promise extends beyond such targeted marketing. AI now makes it feasible for businesses to move from broad segmentation to genuinely *individualized* pricing: estimating each consumer's willingness to pay and adjusting the price (or discount) offered accordingly.

The concept is not new. Airlines and hotels have long employed dynamic-pricing strategies. Ticket brokers, too. What AI changes is the scale and granularity of the enterprise. Modern machine-learning models can process thousands of data points per consumer, including browsing patterns, app usage, time of day, device type, geographic location, proximity to competitors, and inferred income levels. And they can use that data to generate individualized price estimates in real time.[1] As the FTC's Chairman, Andrew Ferguson, has observed, consumer data can reveal "some of our most intimate details-our identities, interests, locations, credit histories, medical conditions, sexual interests, and religious and political views."[2]

The economic literature suggests that personalized pricing can substantially increase profits. Dubé and Misra (2023) documented the feasibility and implications of scalable personalized pricing, finding meaningful profit increases when firms can tailor prices to individual consumers.[3] Shiller (2020) demonstrated that companies can use broad consumer-tracking data-web-browsing histories, social-media activity, and purchase patterns-to approximate with striking accuracy individual consumers' reservation prices.[4]

Recent scholarship suggests that the welfare implications for consumers are far less clear. Buchholz et al. (2025) found that the welfare effect of personalized pricing is ambiguous-some consumers may benefit, but others are made worse off.[5] Rhodes and Zhou (2024) showed that when only some companies personalize prices, consumers can be systematically worse off because personalization undermines the competitive discipline that uniform pricing creates.[6] Jin et al. (2025) summarized potential harms and solutions, cautioning that the more sophisticated personalized pricing becomes, the less likely consumers are to significantly benefit overall.[7]

Meanwhile, consumer awareness of these practices remains strikingly low. According to Pew Research, approximately 67% of the American public say they understand little to nothing about what companies are doing with their personal data.[8] This asymmetry-between sophisticated corporate data analytics and consumers' limited understanding of how their data is used-has drawn regulatory attention. The FTC's newly proposed enforcement policy statement emphasizing transparency in personalized pricing represents the most significant federal response to date.

II. The FTC's New Enforcement Policy on Personalized Pricing

On August 19, 2026, the FTC issued a proposed enforcement policy statement addressing personalized pricing. The FTC describes personalized pricing as the practice of businesses' setting individualized prices “based on analysis of consumers’ personal data and resulting conclusions, such as estimates of how much an individual consumer is willing to pay for a product or whether that consumer is likely to engage in comparison shopping.”[9] While the policy statement is currently only proposed for public comment and does not formally bind the Commission, it provides the clearest signal yet of the FTC’s enforcement priorities in this rapidly evolving area.

A. Scope and Authority

The Commission expressly acknowledges that Congress has not empowered it to prohibit personalized pricing outright. Nevertheless, the FTC states that it “intends to enforce the law aggressively against any deceptive or unfair personalized pricing practices that violate Section 5 of the FTC Act.”[10] The policy statement ties its enforcement rationale, in part, to the Trump administration’s executive orders on cost-of-living, pricing transparency, and anticompetitive behavior, framing personalized pricing as a consumer-welfare concern.

B. The Core Disclosure Requirement

The heart of the policy statement is a disclosure mandate. When consumers “reasonably expect that prices for a product or service will not vary based on their personal data,” businesses that engage in personalized pricing must clearly and conspicuously disclose: (1) that the price is personalized; (2) the basis for that personalization; and (3) the types of data on which the personalization is based.[11] Failing to make these disclosures, the FTC warns, “is likely to constitute an unfair or deceptive act or practice in violation of Section 5.”

The FTC grounds its consumer-expectation analysis in everyday experience. Consumers, the Commission reasons, “reasonably expect the price on the shelf to be the same price offered to any other consumer shopping at the same store at the same time.” Online, consumers “reasonably expect the price to be the same price that anyone else browsing to that listing would see, not a price set based on the retailer’s analysis of their personal data.”[12]

C. Theories of Liability

Deception: Under its deception authority, the FTC states that “[r]etailers may deceive consumers in violation of Section 5 when they represent, expressly or by implication, that a price is static or widely offered when in fact it is personalized.”[13] Deception may also occur when businesses mislead consumers about the basis or effect of personalization. The FTC provides the example of a retailer that leads consumers to believe a markup is a “loyalty discount,” when it is actually based on the retailer’s analysis of the consumer’s income or shopping-habit data.

Unfairness: The FTC also applies its unfairness authority to personalized pricing. Under longstanding Commission guidance, a practice is unfair if it causes a substantial injury that consumers cannot reasonably avoid, and it provides no countervailing benefit.[14] The Commission’s new policy statement reasons that “[t]he higher price paid by a consumer due to personalized pricing may be a substantial injury.”[15] Consumers cannot reasonably avoid the injury if “the fact or nature of personalization of the price has been concealed by the retailer.” And the Commission concludes that any countervailing benefits of personalized pricing-such as lower prices for some consumers-“can be realized without concealment,” satisfying the third prong of the unfairness test.

D. Data-Practices Liability

Separately from the pricing disclosure itself, the FTC identifies an independent basis for liability rooted in data practices. "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."[16] Moreover, businesses that base personalized prices on personal data "without sufficiently verifying that consumers consented to the collection of those data for that purpose" may also violate the law, even if the consumer originally provided the data for an unrelated purpose.

E. Illustrative Examples

The Commission provides seven illustrative examples of personalized pricing practices that could violate Section 5:

- **Food delivery:** A food delivery company charges more to consumers it believes are homebound and thus less likely to seek alternatives.
- **Grocery/milk:** A grocery chain charges more for milk based on data showing the consumer has several children in the household, inferring higher demand and lower price sensitivity.
- **Hotel/funeral:** A hotel charges a higher rate based on data suggesting the traveler is attending a funeral, and therefore unlikely to comparison-shop.
- **Rideshare/competitor apps:** A rideshare company charges more when its data shows the user has not installed competitors' apps, inferring limited outside options.
- **Rideshare/medical facility:** A rideshare company charges more for transport to a medical facility based on data suggesting the consumer is experiencing a medical emergency.
- **Retailer/crime victim:** A retailer charges more for a security camera based on court filings showing the customer was a recent crime victim.
- **Retailer/physical location:** A retailer charges more for an item viewed online when data shows the consumer is currently in the retailer's physical store or parking lot, inferring the consumer has already committed to making the purchase.

F. Open Questions and Limitations

Notably, the Commission "declines at this time to take any position on whether some personalized pricing practices are unfair even when fully disclosed to consumers."[17] This reservation leaves open the significant question of whether transparent personalized pricing could nonetheless be challenged under the unfairness prong-a question that future enforcement actions or rulemakings may address.

Again, the policy statement does not represent a final Commission position. But it signals the agency's enforcement priorities, and businesses that fail to conform their practices to its framework do so at their own risk.

III. Legal Risks Beyond the FTC Policy: State UDAP Laws and Other Exposure

The FTC's proposed policy statement does not operate in a vacuum. Companies deploying AI-driven personalized pricing face a complex web of potential legal exposure at both the federal and state levels. This Part surveys the principal sources of risk beyond Section 5 of the FTC Act.

A. State Unfair and Deceptive Acts and Practices (UDAP) Laws

Every state has enacted its own unfair-and-deceptive-acts-and-practices statute-often referred to as a "little FTC Act." Those laws prohibit unfair, deceptive, or unconscionable trade practices.[18] Many of these statutes track the FTC Act's Section 5 standards or expressly incorporate FTC interpretations. When the FTC has articulated a theory of deception or unfairness-as it has now done with respect to undisclosed personalized pricing-state enforcers and private plaintiffs may adopt that theory under these analogous state laws.

Companies deploying AI-driven personalized pricing thus face potential enforcement actions by state attorneys general and, in many states, private lawsuits brought directly by consumers. State UDAP remedies frequently include statutory damages, treble damages, and awards of attorneys' fees-making state enforcement potentially more punitive than federal action. In states that follow the FTC's interpretive lead, the Commission's proposed policy statement could effectively serve as a roadmap for state-level enforcement even before it is finalized. And in states like California, where UDAP statutes "borrow" violations of other laws or regulations, the plaintiffs' bar is certain to argue that violating the enforcement guidelines will support a UDAP claim.

B. State Data-Privacy Laws

Many state privacy statutes impose independent transparency and consent obligations for collecting, using, and selling consumers' personal data. California's Consumer Privacy Act and California Privacy Rights Act (CCPA/CPRA), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Virginia Consumer Data Protection Act, and similar laws in a growing number of states require businesses to disclose the purposes for which they collect and process personal data and, in many cases, to provide consumers with opt-out rights.[19]

Using consumer data for personalized pricing without adequate disclosures-or without honoring applicable opt-out mechanisms-could trigger independent violations of these statutes. Moreover, several state privacy laws impose heightened obligations when businesses engage in "profiling" that significantly affects consumers. An AI system that determines the price a consumer is offered for a product or service could readily qualify as profiling, triggering additional consent requirements, data-protection impact assessments, or opt-out rights under applicable state law.

C. State-Specific Disclosure Rules Cited by the FTC

The FTC's policy statement itself identifies existing state-level disclosure requirements in regulated industries as instructive analogs. Specifically, the Commission cites:

- **California Insurance Code §§ 791.02, 791.10** (1981/2013), requiring insurers to disclose the bases for adverse underwriting or pricing decisions;

- **Virginia Code § 38.2-602** (1986/2003), imposing similar disclosure obligations on Virginia insurers; and
- **Washington Administrative Code § 284-30A-070 (2024)**, establishing detailed disclosure requirements for individualized adverse pricing actions in the insurance context.[20]

These existing disclosure regimes in the insurance sector show that states are already sensitive to individualized pricing practices and have concluded, at least in regulated industries, that consumers are entitled to know the bases on which they are charged individualized rates. As AI-driven personalized pricing proliferates beyond insurance into retail, transportation, entertainment, and other services, states may extend similar disclosure requirements through new legislation or through expansive interpretation of existing UDAP statutes.

D. Fair Credit Reporting Act (FCRA) Exposure

The FTC draws an explicit analogy between its proposed personalized-pricing disclosure framework and the Fair Credit Reporting Act's adverse-action notice requirements.[21] Under the FCRA, when a business takes an "adverse action" against a consumer based in whole or in part on information contained in a consumer report, the business must notify the consumer, identify the consumer-reporting agency that furnished the report, and inform the consumer of the right to obtain the report and dispute its accuracy.[22]

If companies rely on consumer-report data-credit scores, purchase histories obtained from third-party data brokers, or other information that qualifies as a "consumer report" under 15 U.S.C. § 1681a(d)-to set personalized prices, they may trigger FCRA obligations. A personalized price that is higher than the price offered to other consumers could constitute an "adverse action" requiring notice under § 1681m(a). Companies that fail to provide such notices risk statutory damages, actual damages, and class-action liability under the FCRA's private right of action.

E. Emerging State Personalized-Pricing Legislation

Several states are moving toward laws that specifically address personalized pricing. These laws generally focus on disclosure-requiring businesses to notify consumers when prices are set or adjusted based on personal data, automated decision-making, or similar forms of individualized pricing logic. For example, New York has already enacted disclosure requirements for personalized algorithmic pricing and continues to consider additional legislation aimed at personalized-pricing practices.[23] California, Connecticut, and Maryland have likewise considered or enacted measures directed at surveillance pricing, personalized pricing, or consumer-price inequity based on personal data.[24]

Although these laws may vary in scope and terminology, they share a common premise with the FTC's proposed policy statement: pricing practices may be unfair, abusive, or deceptive when businesses personalize prices to individual consumers based on data about them-without meaningful disclosure-rather than offering generally applicable market pricing.

F. Civil Rights and Discrimination Risk

Perhaps the most significant long-term legal risk of AI-driven personalized pricing lies in civil-rights law. If personalized-pricing models-trained on historical data that reflects existing social and economic disparities-produce pricing outcomes that correlate with protected characteristics such as race, national origin, gender, disability, or age, companies could face liability under federal civil-rights statutes and state anti-discrimination laws.

Crucially, such liability does not necessarily require proof of discriminatory intent. Under disparate-impact theories-well-established in housing, lending, and employment contexts-a facially neutral practice that disproportionately affects members of a protected class may be unlawful absent a sufficient business justification.[25] AI pricing models that rely on geographic data (which correlates with race), device data (which may correlate with income and race), or browsing behavior (which may correlate with age or gender) could produce pricing outcomes that are vulnerable to disparate-impact challenges.

G. Class Action Exposure

Finally, the combination of widespread data collection, uniform algorithmic pricing practices, and readily identifiable consumer harm-paying more than other consumers for the same product or service-may amplify the risk of a class action. While the label of *personalized* pricing may suggest predominant individual inquiries that would tank class certification under Federal Rule of Civil Procedure 23(b)(3),[26] the plaintiffs' bar will focus on the uniform policy of using generative AI and algorithms to set prices, rather than the (often hidden) individual calculations that produce the prices in question.

And assuming that this theory could support damages (after all, all consumers paid the price they intended to pay and got the products they intended to receive), damages are potentially calculable on a class-wide basis by comparing the personalized price charged to each consumer against the baseline or lowest price offered for the same product. The availability of statutory damages under state UDAP statutes and the FCRA further suggests that class claims would be economically viable, even if individual overcharges are modest.

* * *

The FTC's proposed enforcement policy statement on personalized pricing marks a significant development in the regulatory landscape for AI-driven commerce. But it is only one piece of a much-larger legal puzzle. Companies considering or already deploying AI-driven personalized pricing strategies should assess their exposure holistically-across federal and state consumer protection law, data privacy law, credit reporting law, civil rights law, and emerging AI-specific regulation. The legal risks are not speculative; they are concrete, multi-dimensional, and growing.

---

[1] *See generally Kehoe et al., Dynamic Competition in the Era of Big Data* (Nov. 3, 2020) (discussing how firms leverage big data for pricing).

[2] Statement of Commissioner Andrew N. Ferguson on Surveillance Pricing (July 23, 2024).

[3] Jean-Pierre Dubé & Sanjog Misra, *Personalized Pricing and Consumer Welfare*, 131 J. Pol. Econ. 131 (2023).

[4] Benjamin Shiller, *Approximating Purchase Propensities and Reservation Prices From Broad Consumer Tracking*, 61 Int'l Econ. Rev. 847 (2020).

[5] Nicholas Buchholz et al., *Personalized Pricing and the Value of Time: Evidence from Auctioned Cab Rides*, 93 Econometrica 929 (2025).

[6] Andrew Rhodes & Jidong Zhou, *Personalized Pricing and Competition*, 114 Am. Econ. Rev. 2141-70 (2024).

[7] Ginger Zhe Jin et al., *Surveillance Pricing: A Cautionary Summary of Potential Harms and Solutions*, CPI Antitrust Chronicle (July 14, 2025).

[8] Pew Research Center, *How Americans View Data Privacy* (Oct. 18, 2023).

[9] FTC, Proposed Enforcement Policy Statement Regarding Personalized Pricing 1 (Aug. 19, 2026).

[10]*Id.* at 1.

[11]*Id.* at 1.

[12]*Id.* at 2.

[13]*Id.* at 5.

[14] *See* FTC Unfairness Policy Statement, Letter from the FTC to Hon. Wendell H. Ford and Hon. John C. Danforth, Senate Comm. on Com., Sci., and Transp. (Dec. 17, 1980), available at https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.

[15] FTC, Proposed Enforcement Policy Statement Regarding Personalized Pricing (Aug. 19, 2026).

[16] *Id.* at 7.

[17] *Id.* at 6 at n.20.

[18] *See, e.g.*, Carolyn Carter, *Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws*, Nat'l Consumer Law Ctr. (2018).

[19] *See* Cal. Civ. Code §§ 1798.100-199.100 (CCPA/CPRA); Colo. Rev. Stat. §§ 6-1-1301 to -1314; Conn. Gen. Stat. §§ 42-515 to -525; Va. Code Ann. §§ 59.1-575 to -585.

[20] *Supra* n.9 (FTC Proposed Enforcement Policy Statement at 6 n.23, citing Cal. Ins. Code §§ 791.02, 791.10; Va. Code § 38.2-602; Wash. Admin. Code 284-30A).

[21] *Id.* at 6 (analogizing to FCRA adverse-action notice requirements).

[22] 15 U.S.C. § 1681m(a); *see also Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 52-53 (2007) (analyzing 15 U.S.C. § 1681m(a) as it applies to insurance and noting that "adverse action" can include the denial or cancellation of, or "an increase in any charge for," or the reduction of, or "unfavorable change" in terms or existing amounts).

[23] N.Y. G.B.L. § 349-a (effective July, 2025).

[24] AB-2564, 2025-2026 Legis. Reg. Sess. (Cal. 2026); Public Act No. 26-64 (Conn. 2026); HB 895 (Md. 2026).

[25] *See, e.g.*, *Griggs v. Duke Power Co*., 401 U.S. 424 (1971); *Texas Dep't of Hous. & Cmty. Affairs v. Inclusive Communities Project, Inc*., 576 U.S. 519 (2015).

[26] *See* Fed. R. Civ. P. 23(b)(3), available at: https://www.law.cornell.edu/rules/frcp/rule_23.