Center for American Progress

5 Ways the FTC Can Protect Americans From AI-Fueled Surveillance Pricing

By: Megan Shahi, Zoë Baird, and Jared Bernstein

Authors' note: Several terms are used to describe the practice of using data about individual consumers to inform the prices they are offered, including "personalized pricing," "individualized pricing," and "surveillance pricing." This piece primarily uses "surveillance pricing," which more accurately reflects the extensive collection and use of personal and behavioral data that can underlie these practices and avoids the more benign connotations of terms such as "personalized pricing."

In August 2026, the Federal Trade Commission (FTC) released a proposed policy statement regarding personalized pricing—also called surveillance pricing—with a request for public comments. The FTC and its authorities are central to keeping Americans safe, including from unfair pricing methods, such as price discrimination and hidden costs, and false, misleading, or deceptive advertising. This mandate is more important than ever against a backdrop of the rapid acceleration of artificial intelligence (AI) technology, which can amplify existing consumer harms, including fraud and scams, deceptive advertising, discriminatory practices, and increasingly sophisticated forms of personalized pricing that are easier and cheaper to deploy. The FTC's proposed focus on disclosure is an important first step, but transparency alone is insufficient to protect consumers from the harms of surveillance pricing. The commission should pair disclosure requirements with substantive safeguards that limit harmful uses of personal information and give Americans meaningful control over whether and how their data are used to determine the prices they pay.

This issue brief lays out five ways the FTC can protect Americans from surveillance pricing:

1. Pair disclosure requirements with substantive protections against harmful surveillance pricing.
2. Distinguish between legitimate dynamic pricing and surveillance pricing.
3. Establish guardrails around the data that can be used to set prices.
4. Clarify where surveillance pricing is and is not reasonably expected.
5. Preserve legitimate loyalty and rewards programs.

The harms of surveillance pricing

Businesses have long adjusted prices based on supply, demand, inventory, timing, and other market conditions. The concern surrounding AI-fueled surveillance pricing is not simply that prices change but—as the FTC's policy statement makes clear—that businesses have a growing ability to use personal, individualized information about who a consumer is, including their socioeconomic status, preferences, and private circumstances, to determine the price presented to them. Moreover, the consumer can experience this without the ability to control such granular scrutiny or even be aware that it occurs.

As the FTC's policy statement acknowledges, surveillance pricing is a nascent practice, and there is little research on the potential impacts to consumers. Those studies that exist demonstrate that some consumers benefit, while others pay more. And as the FTC's policy statement points out, "the more sophisticated personalized pricing practices become, the less likely consumers are to benefit."

Surveillance pricing is especially concerning when consumers receive no offsetting benefit. One investigation found that Instacart used AI pricing software from its subsidiary Eversight to test different prices on shoppers without these users' knowledge. Some customers paid up to 23 percent more than others for the same grocery items from the exact same locations at the exact same time. Following the investigation, Instacart ended the price-testing practice and the FTC opened an inquiry. This episode also underscores concerns that have prompted growing state scrutiny of surveillance pricing, including laws such as New York's disclosure requirement for personalized algorithmic pricing.

Other research has found that firms generally benefit from personalized pricing, while its effects on consumers tend to be unfavorable. For example, using two randomized field experiments at ZipRecruiter, Dubé and Misra (2022) found that personalized pricing increased the firm's expected profits and reduced the total economic benefit received by consumers. Some individual consumers were better off, not because they gained more power but because the algorithm offered lower prices to those less willing to pay. In another study, Buchholz and others (2025) examined auctioned rides on a ride-hailing platform. The authors estimate that, relative to uniform platform pricing, personalized pricing reduced the total economic benefit received by consumers by 2.5 percent but increased the combined economic benefit received by consumers, drivers, and the platform by 5.2 percent, as gains to the platform and drivers outweighed the losses to consumers. Across these studies, gains accrued unevenly, mostly to firms and not to consumers.

The FTC's current work also builds on an important foundation established by the commission's prior investigation into surveillance pricing. In July 2024, the FTC unanimously used its Section 6(b) authority to seek information from eight companies offering pricing products and services that used AI and other technologies alongside consumers' personal information to target prices. The FTC's initial findings, released in January 2025, showed that pricing intermediaries could use highly granular information—including precise location, browser and shopping history, and even consumers' interactions with webpages and items left in online shopping carts—to tailor prices, promotions, and product offerings to individual consumers. The study also found that the intermediaries examined worked with at least 250 clients across sectors ranging from grocery stores to apparel retailers. Importantly, the FTC described those findings as preliminary and stated that its review of the information collected through the 6(b) orders was ongoing. The Center for American Progress encourages the commission to continue and complete this work, including by referencing the findings and prior study in the forthcoming policy statement. The information already collected through the study can provide an important empirical foundation for understanding how surveillance pricing is deployed in practice and for informing the commission's enforcement approach going forward.

The commission has both the authority and the responsibility under Section 5 of the FTC Act to address unfair or deceptive surveillance pricing practices, particularly where consumers ought to be able to reasonably expect that they are offered the same price as others. The FTC's proposed policy statement provides an important foundation for enforcement, but greater clarity and stronger protections are needed to address how increasingly sophisticated surveillance pricing practices affect consumers. The FTC can strengthen its approach through clearer guidance and substantive guardrails, but federal action should not end there. Congress should build on ongoing state efforts to develop protections against harmful surveillance pricing practices to establish durable federal protections for consumers. (see text box) As policymakers consider how to protect consumers from the risks of surveillance pricing while preserving legitimate pricing practices, the five principles below should guide the way forward.

1. Pair disclosure requirements with substantive protections against harmful surveillance pricing

The FTC's proposed policy statement appropriately emphasizes the importance of clear and conspicuous disclosure when businesses engage in surveillance pricing. Consumers should know when the price they are offered has been determined using their personal information and understand the basis for that personalization. But simply informing a consumer that a price has been personalized does not give them meaningful control over the practice, nor does it allow them to determine whether they are paying more than another consumer would for the same product or service. A disclosure regime alone risks placing the burden on consumers to identify, understand, and respond to sophisticated pricing practices that companies themselves design and control.

The data privacy context illustrates the shortcomings of a disclosure-only approach. For decades, consumer privacy protections have often relied on a notice and consent framework, in which companies disclose their data practices and consumers are expected to either accept them or stop using the product or service. This presents consumers with a false choice—particularly when they lack realistic alternatives or cannot reasonably avoid the service. Disclosures of this kind are also often lengthy and complex, and individuals are poorly positioned to assess how their data may be combined, inferred from, or used later. Surveillance pricing raises the same concerns, and in some contexts may make them even more acute. Consumers who need groceries, transportation, medicine, or other essential products or services may have little practical ability to walk away. Simply notifying consumers that their personal information is being used to determine a price therefore does little to address the underlying market power imbalance.

Where surveillance pricing is permitted, disclosure should be paired with meaningful consumer choice. The option to forgo a product or service altogether in order to avoid surveillance pricing is not a meaningful consumer choice; it simply conditions access on a consumer's willingness to submit to individualized price-setting. Consumers should be able to opt out of the collection and use of personal information for individualized price-setting and continue to access the underlying product or service at a nonpersonalized price. A consumer should not have to surrender access to a service simply because they do not want their personal information used to determine how much they will be charged. Together, clear disclosure, substantive limits on particularly harmful uses of personal information, and a meaningful ability to opt out would provide consumers with considerably stronger protections than transparency alone.

The concern is not limited to the most sensitive types of data or the most extreme forms of exploitation: The underlying practice of surveillance pricing raises consumer protection concerns even where the information itself may appear relatively innocuous. Those concerns are particularly acute where businesses use sensitive information or inferences about a consumer's vulnerability, urgency, or willingness to pay to charge that consumer more. The FTC should therefore clarify the circumstances in which surveillance pricing may constitute an unfair practice under Section 5 even when the practice has been disclosed to the consumer. For example, a company should not be able to use data suggesting that a consumer is urgently searching for medicine for a sick child, facing a financial emergency, or otherwise has highly inelastic demand to infer that the consumer has little practical ability to walk away and therefore charge that individual a higher price.

For example, a company should not be able to use data suggesting that a consumer is urgently searching for medicine for a sick child, facing a financial emergency, or otherwise has highly inelastic demand to infer that the consumer has little practical ability to walk away and therefore charge that individual a higher price.

Notably, existing laws already prohibit certain forms of discrimination in specific contexts: The Equal Credit Opportunity Act and Fair Housing Act, for example, prohibit discrimination on the basis of specified protected characteristics in covered credit and housing transactions.

2. Distinguish between legitimate dynamic pricing and surveillance pricing

Businesses have long employed dynamic pricing in response to impersonal market conditions, such as changes in supply, demand, inventory, or timing. But these practices are fundamentally different from pricing systems that use personal data, behavioral profiles, or inferences about an individual consumer to determine the price that a person is offered. In its final policy, the FTC should draw a clear distinction between legitimate dynamic pricing and surveillance pricing.

The relevant question for regulators should be why a consumer received a particular price, not simply whether AI or an algorithm was involved in setting it. Consumers may reasonably expect the price of a flight to increase as seats sell out or the cost of a rideshare to rise when demand exceeds the number of available drivers, neither of which requires personalized information. But that does not mean consumers should reasonably expect to pay more because a company has inferred from their browsing history, location, income, past purchases, device data, or other personal information that they are particularly willing or able to pay a higher price or are particularly in need of the service.

This distinction is important because an overly broad approach to surveillance pricing could sweep in ordinary and potentially beneficial pricing practices while failing to target the conduct that creates the greatest consumer protection concerns. The FTC should focus its policy on the use of individualized information to assess a particular consumer's willingness or ability to pay and extract a higher price from that consumer, rather than on dynamic pricing or the use of algorithmic tools in this context.

3. Establish guardrails around the data that can be used to set prices

Where it is appropriate, the FTC should provide greater clarity about the categories of personal information that businesses may use to determine individualized prices. It should give particular concern to sensitive personal information and data used to infer a consumer's vulnerability or willingness to pay, including health or financial information, precise location, browsing or search behavior, psychographic or behavioral profiles, and inferences about urgency, emotional state, or financial distress.

Using these types of information to determine what an individual consumer can or will pay risks turning information collected about consumers into a tool to exploit their individual circumstances.

Importantly, a consumer's consent to the collection of personal information should not be treated as consent for that information to be used for individualized price-setting. Consumers routinely provide information to businesses for purposes unrelated to pricing, and permitting that information to be repurposed to estimate an individual's maximum willingness to pay creates an entirely different use and potential harm. Moreover, businesses should not be permitted to avoid scrutiny simply because the individualized price remains below the maximum amount an algorithm predicts a consumer would pay. The relevant question is whether personal information is being used to charge an individual more than they otherwise would have been charged, not whether the business extracted the maximum possible amount from that consumer.

4. Clarify where surveillance pricing is and is not reasonably expected

The FTC should provide additional guidance on its proposed standard concerning products that Americans reasonably expect will not cost them differently than their "friends or neighbors." Consumer expectations vary considerably across markets, and an expectation that prices may change does not necessarily mean consumers expect those prices to be personalized based on information about them.

For many everyday goods and services, including groceries, retail products, and food delivery, consumers generally expect a posted price to apply equally to similarly situated consumers. In other markets, such as air travel, hotels, and rideshare, consumers are accustomed to prices fluctuating based on factors such as demand, availability, location, or timing. But acceptance of those forms of dynamic pricing should not be interpreted as an expectation that two consumers purchasing the same product or service under the same market conditions may receive different prices because of their individual characteristics, behavior, or inferred willingness to pay. Consumer necessities such as food and transportation should generally be subject to even greater enforcement scrutiny than nonessentials, as defined by the FTC.

The FTC should therefore provide examples or factors that distinguish the cases in which consumers can reasonably expect price variation from individualized surveillance pricing. In particular, the commission should make clear that a history of dynamic pricing within a market does not, on its own, establish a reasonable expectation that businesses may use personal information to determine the price offered to an individual consumer.

5. Preserve legitimate loyalty and rewards programs

The FTC's 2026 policy statement appropriately recognizes that consumer expectations around price variation differ across markets. In applying that distinction, the commission should distinguish opaque surveillance pricing from voluntary loyalty, rewards, coupons, subscribe-and-save, and promotional programs that offer consumers discounts—including those for broad categories of consumers, such as seniors and veterans. Recent state laws (see text box) addressing surveillance pricing have similarly recognized the need to preserve legitimate consumer discount programs and created exemptions for them. These programs should remain permissible where consumers knowingly participate, the terms are clear, and the data used are reasonably related to providing the benefit.

At the same time, the modern loyalty program can extend well beyond the direct relationship a consumer reasonably understands themselves to have with a retailer. Information generated through a loyalty program, including detailed purchase histories and shopping behavior, can be shared or sold to third parties, combined with information obtained from other sources, and used to create increasingly granular profiles of individual consumers. A consumer who provides information to a grocery store in exchange for discounts should not be presumed to have agreed to that information being sold or combined with unrelated data to infer their income, health, family circumstances, vulnerabilities, or willingness to pay.

The FTC should therefore distinguish between the use of data that are reasonably necessary to operate a loyalty or rewards program and the secondary sale, sharing, or repurposing of that information for individualized price-setting or broader consumer profiling. Loyalty programs should not become a loophole through which companies can engage in surveillance pricing that would otherwise raise consumer protection concerns. The commission should use its existing authority to address unfair or deceptive practices involving these secondary uses where applicable, while Congress should address the broader gap through comprehensive federal privacy legislation that establishes meaningful limits on the collection, sale, sharing, and secondary use of personal information. Such protections can preserve legitimate loyalty and rewards programs while preventing participation in those programs from becoming a gateway to a substantially broader system of commercial surveillance.

Recent state actions to protect consumers

Several states have already passed laws to protect consumers from the potential harms of surveillance pricing, and others are currently weighing proposals. These primarily have been focused on food and grocery delivery, which many households depend on and for which they need affordable options, and include exemptions for existing consumer discount programs. The FTC should assess the impact of the various state policies discussed below and consider how these can serve as models for further action.

- A Maryland law, which will take effect on October 1, 2026, prohibits grocery stores of at least 15,000 square feet and third-party food delivery services from using personal data to set a price for a specific shopper for most groceries. It does, however, permit loyalty programs, subscription prices, and differences based on supply, location, or operating costs. Businesses also have 45 days to correct a violation before the state can bring an enforcement action.

- A 2026 Connecticut law broadly prohibits retailers and third-party delivery services from using surveillance pricing. It includes exceptions for discounts and certain price differences unrelated to a shopper's personal data.

- A 2026 New Jersey law prohibits retailers from using personal data to set individualized prices for groceries and places a one-year moratorium on the new use of new electronic shelf labels while the state studies their effects.

- New York's legislature passed the One Fair Price Act in June 2026, and the bill is awaiting the signature of Gov. Kathy Hochul (D). This legislation, if enacted, would ban surveillance pricing but allow for discount and loyalty programs. Companies may also still use dynamic pricing algorithms, as long as the algorithm does not use an individual's personal data to set prices. The One Fair Price Act also gives the Office of the Attorney General the authority to bring civil cases for penalties and restitution against companies or retailers found to be in violation of the law.

Conclusion

As AI makes it cheaper and easier for businesses to analyze vast amounts of consumer data and tailor prices at an increasingly individual level, policymakers should establish guardrails before these practices become widespread. Not every use of algorithms to set prices raises the same concerns, but there is an important difference between adjusting prices in response to market conditions and using detailed, potentially sensitive information about an individual consumer to determine how much more that person can be made to pay.

The FTC's proposed policy statement is an important step toward establishing that distinction, but disclosure alone cannot carry the full weight of consumer protection. Americans should also have meaningful choice over whether their information is used for that purpose and be protected from practices that exploit sensitive information or moments of vulnerability. At the same time, regulators should preserve legitimate dynamic pricing, discounts, and loyalty programs that do not depend on exploiting individualized information.

The FTC has an important role to play in setting these guardrails, enforcing existing protections, and continuing to build the evidence base around how surveillance pricing affects consumers. But the commission should not have to act alone. States are already testing stronger substantive protections, and Congress should ultimately establish durable federal safeguards. As AI transforms what businesses can know about individual consumers and how precisely they can price goods and services to them, consumer protection rules must ensure that greater technological sophistication does not simply grant companies greater power to extract value from Americans based on what they know about their lives.

Acknowledgments

The authors would like to thank Veronica Goodman, Cristina Tello-Trillo, Emily Gee, Ben Olinsky, Adam Conner, Nicole Alvarez, and Sara Partridge for their contributions to this product.