September 25, 2026

Chairman Andrew N. Ferguson
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington DC, 20580

**Re: Federal Trade Commission's Proposed Enforcement Policy Statement Regarding Personalized Pricing**

The undersigned civil rights advocacy and civil society organizations appreciate the opportunity to submit comments in response to the Federal Trade Commission's August 19, 2026 Request for Comment (RFC) on Personalized Pricing[1]. We commend the Commission for seeking input on this important topic and hope our comments below will help inform the Commission's views.

We share the Commission's concerns around surveillance pricing[2] particularly on the grounds of unfairness, deception, and anticompetitive behavior. Like the Commission, our organizations have also expressed significant concern over the data collection and use practices of the technology industry. Because of their potential for harm, we urge the Commission to consider prohibiting or greatly limiting the practice altogether.

Despite the Commission's insistence otherwise in the proposed enforcement policy, the Commission already has the authority clearly mandated in Section 5 of the FTC Act to prohibit surveillance pricing outright through Unfairness authority and by vigorous enforcement of unlawful discriminatory pricing outcomes through the Equal Credit Opportunity Act (ECOA) rather than relying solely on disclosure-based remedies.[3] The Commission's proposed policy recognizes that using personal data to set "personalized"

---

[1] Federal Trade Commission's Proposed Enforcement Policy Statement Regarding Personalized Pricing
[2] Note: these comments refer to the use of people's personal data collected oftentimes without their knowledge or consent, as "surveillance pricing" rather than "personal pricing" as it may more appropriately describe the practice.
[3] https://www.govinfo.gov/content/pkg/USCODE-2024-title15/pdf/USCODE-2024-title15-chap2-subchapI-sec41.pdf

(surveillance) pricing without adequate disclosure may violate Section 5's prohibition on unfair or deceptive practices. Likewise, surveillance pricing may be unfair even if disclosed. As the Commission itself notes, charging more to homebound individuals, families with children, or people going to funerals can cause harm.[4] As such, Section 5 authority remains available for the Commission to take action to prohibit those unfair practices, even if it chooses not to exercise that authority. At the same time, we think it is important to flag the tension between the Commission's stated interest in addressing surveillance pricing harms and its recent retreat from discriminatory pricing outcomes that the FTC has traditionally enforced through ECOA. These are some of the most effective mechanisms for actually reaching those harms, and they result in remedial practices that result in fairer prices for all consumers, not just consumers of a specific race or ethnicity.

## I. The FTC should prohibit surveillance pricing outright

We urge the Commission to consider using its authority to prohibit surveillance pricing as the practice is deceptive, harms consumers directly, and carries compounding risks across civil rights, privacy, competition, and economic policy. It risks discrimination because the personal data used to set individualized prices often correlates closely with protected characteristics. It creates privacy harms, rewarding firms that collect and retain as much data on consumers as they can obtain. It is anticompetitive, advantaging firms with the most sophisticated surveillance tools and enabling them to extract more data from every transaction, further pushing out competitors. And it reduces consumer surplus, transferring value in the form of profit from households to sellers.

Advances in artificial intelligence (AI) and data collection are accelerating each of these harms, making surveillance pricing more precise and harder for consumers and regulators alike to detect. States have recognized the threat and are taking action. New Jersey,[5] Maryland,[6] Connecticut,[7] and New York[8] have already enacted prohibitions or

[4] Page 6 of FTC Enforcement Statement on Personalized Pricing "Some personalized pricing practices may also be unfair under Section 5. The higher price paid by a consumer due to personalized pricing may be a substantial injury. Consumers may not reasonably be able to avoid that higher price if the fact or nature of personalization of the price has been concealed by the retailer. For example, consumers may not be able to avoid paying the higher personalized price if they lack the information or tools necessary to, among other things, modify their behavior to avoid triggering higher prices, dispute or correct inaccurate information collected about them that is leading to higher prices, or avoid the collection of that data in the first place."
[5] https://www.nj.gov/governor/news/2026/20260723a.shtml
[6] https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0895?ys=2026RS
[7] https://cga.ct.gov/2026/ACT/PA/PDF/2026PA-00130-R00HB-05563-PA.PDF
[8] https://www.nysenate.gov/legislation/bills/2025/S8623/amendment/B

disclosure requirements, with bills proposed in states such as California[9] and Colorado.[10] The Commission has also recognized these harms and thus should use its authority to act to protect consumers.[11]

**Surveillance pricing is growing across industries.** The Commission's own report on surveillance pricing indicates that surveillance pricing is becoming more ubiquitous, appearing in grocery stores, apparel retailers, home goods and furnishing stores, convenience stores, building and hardware stores, and other retailers.[12] Across industries, companies are using the massive amounts of personal data they collect from individuals and families to set prices for goods and services based on people's behaviors and vulnerabilities.[13] The findings suggest that surveillance pricing, enabled by continued massive data-collection efforts combined with the computing power of AI, is often used not to provide lower costs to individuals; instead surveillance pricing is being used to charge the highest price an individual is willing to pay based on their circumstances.

The implications of the data collected, amassed, combined, and in some cases used to make predictions, has wide impact. Like surveillance pricing, companies are using data about their workers to use AI to set their employees' wages. And like surveillance pricing, using AI to set wages can lead to harm – suppressing those wages and leading to unpredictable pay and worker manipulation.

**Surveillance pricing leads to discrimination.** The Commission's statement correctly identifies surveillance pricing as an unfair and deceptive act and correctly warns that data revealing consumers' identities, locations, credit histories, medical conditions, sexual interests, and religious and political views may be used to set individualized prices. In many cases the harm will not announce itself that way; rather, it will occur via a proxy. Because the data feeding personalized pricing correlates closely with protected characteristics and with financial precarity, these systems can reproduce and widen existing disparities without ever indexing a prohibited category directly. Companies already collect sensitive data that can be used as proxies for protected categories, including location, demographic data, biometric data, and personal device data.

---

[9] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB2564
[10] https://leg.colorado.gov/bills/HB26-1210
[11] Page 6 of FTC Enforcement Statement on Personalized Pricing
[12] Page 7 of FTC Enforcement Statement on Personalized Pricing
[13] Fed. Trade Comm'n, FTC Surveillance Pricing 6(b) Study: Research Summaries – A Staff Perspective (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf [Hereinafter FTC Report].

Charging one consumer more than another because of a protected characteristic such as race or sex is plainly discriminatory under ECOA. In the case of credit, this can occur when two consumers of different races have equivalent creditworthiness profiles but are charged different prices without justification. Notably, the FTC has recently abandoned existing cases where this has been found.[14] While the FTC has asserted that these matters relied solely on disparate impact theory, review of the cases reveals that they actually articulate both disparate treatment and disparate impact as potential legal theories, and fall squarely within traditional disparate treatment-based pricing discrimination enforcement. The remedies in these cases benefit consumers of all races through the improved compliance policies and fairer pricing structures implemented, not just consumers of a specific race or ethnicity.

Vulnerable communities may be the most impacted by surveillance pricing**.** This may be due to a combination of economic, social, and technological factors that result in furthering existing inequalities. A report by AI Now and others supports the conclusion that surveillance prices and wages can exacerbate systemic discrimination. In making the case for prohibiting surveillance pricing and wages outright, AI Now notes that "algorithms often rely on data that reflect historical and ongoing biases, embedding these prejudices into wage- and price-setting systems and perpetuating them."[15] AI Now is not alone: Consumer Reports, has also advocated for bans on surveillance pricing, citing abuses and the need to protect individuals and families from opaque, data-driven price discrimination.[16]

- **Racial Discrimination**. Algorithms can reflect social, economic, and other patterns that could result in higher prices for marginalized populations. For example, women, the elderly, and communities of color might pay more for identical products or services based solely on consumer data patterns like zip codes, purchasing history, or other factors that can act as proxies for race or social/economic status and lead to unfair pricing. This result creates a form of digital redlining, a type of like past discriminatory practices that was banned years ago. A study of 100 million ridehailing samples from the city of Chicago found that fare pricing of neighborhoods with larger non-white populations were

---

[14] https://www.ftc.gov/news-events/news/press-releases/2026/08/ftc-ditches-disparate-impact
[15] AI Now report, Prohibiting Surveillance Prices and Wages, Feb. 2025, Surveillance Prices and Wages Report
[16] CR-Positions-Surveillance-pricing.pdf

significantly higher.[17]Surveillance pricing algorithms designed to determine an individual's willingness to pay using detailed personal data, like income, location, spending patterns, and the like, may assume that some households may be able to tolerate slightly higher prices for essential goods and services.

- **Discrimination against low-income households:** Consumer Reports has found that surveillance pricing can increase costs for consumers without benefit and undermines transparency in pricing thus restricting an individual's ability to make informed choices. The impact of surveillance pricing on vulnerable communities leads to the conclusion that the use of these tools is not about market efficiency, but rather about optimizing for a company's bottom line in ways that result in predatory behavior that exploits people's vulnerabilities, socioeconomic status, and technological capabilities:
- **Discrimination against working families.** The AFL-CIO found that "for working families, already stretched thin, [surveillance pricing] can mean paying hundreds or even thousands more each year for the same products and services as someone else."[18] They noted that surveillance pricing both "penalizes urgency" and "deepens inequality."[19] If someone  needs a flight to help a sick loved one, or if a parent is shopping late at night for items for their newborn, an algorithm "may interpret that behavior as desperation – and increase the cost."[20] Likewise, working families may not have time to "comparison shop, use privacy protections, and navigate around price manipulation" like wealthier consumers.[21]

**Personalized pricing carries competitive risk.** We urge the Commission to acknowledge the role that AI plays in the increased sophistication of surveillance pricing.The Commission's statement observes that perfect personalized pricing, absent competition, would allow a monopolist to capture the entire consumer surplus, and the research the statement  cites notes that access to data for personalized pricing can raise entry barriers and give rise to abuse-of-dominance concerns.[22] AI is making  these theoretical concerns a reality: firms with the most sophisticated AI tools will be best positioned to use surveillance pricing to capture profit. The result risks a self-reinforcing dynamic in which market success accrues to the firms most adept at extracting consumer data and using it to extract consumer surplus, rewarding data accumulation

---

[17] https://dl.acm.org/doi/10.1145/3461702.3462561
[18] Surveillance Pricing Is Costing Working Families Thousands — and It Needs to Be Stopped | Union Label and Service Trades Department, AFL-CIO
[19] See reference 18
[20] See reference 18
[21] See reference 18
[22] Page 3 of FTC Enforcement Statement on Personalized Pricing

rather than better products, lower prices, or genuine innovation. As the Commission's own sources find, consumers can be worse off when only some firms in a market can personalize than when all or none do.

## II. Transparency is necessary but more enforceable protections are needed.

While the Commission is right to look to a transparency requirement as a safeguard, disclosures alone — telling an individual that surveillance pricing is occurring — fail to address the underlying mechanisms and harms caused by the practice. AI often operates in “black boxes,” so even if there is awareness that an individual’s data may drive different pricing, the company itself may not fully understand or appreciate the parameters of how a price was set. This fundamental lack of information prevents individuals from being able to contest unfair outcomes or control inputs that may trigger higher costs. In other words, there may be insufficient information for an individual to challenge a decision or interrogate the factors used to make price determinations. Moreover, transparency alone will not empower an individual to negotiate or opt-out of an exploitive surveillance pricing scheme. Those belonging to marginalized communities lacking resources or who are less digitally savvy are particularly at risk of discrimination in surveillance pricing.

The most effective safeguard the Commission can take is to prohibit surveillance pricing altogether. Short of a ban, to protect individuals the Commission must adopt safeguards beyond transparency. There must be regulatory oversight, accountability mechanisms, and prohibitions against discriminatory pricing. In addition, any transparency requirement must be robust, going beyond simply disclosing that surveillance pricing is taking place. Like with insurance and credit decisions,[23] individuals must be provided with reasons why a price was set, including the data points or other factors, predictions, or comparisons that were used. Individuals should also be provided with a mechanism to challenge a price. Unfortunately, even these safeguards will likely fall short because they place the burden on individuals to assess, question, or challenge decisions made by opaque algorithms run by some of the largest companies in the world.

## III. The Commission's retreat from enforcement of rules preventing pricing discrimination undercuts its own stated goals.

[23] We note that insurance and credit are highly regulated industries in which risk-based price determinations have been vetted as a matter of public policy and are highly scrutinized and challenged. Those are distinguishable from surveillance pricing where decisions on the cost of a product or service are driven by a determination of how much an individual is willing to pay based on the personal data collected and analysed about that individual.

On August 7, 2026, the Commission announced that it would no longer pursue disparate-impact claims under the FTC Act, and repudiated its prior position that the unfairness prong of Section 5 independently supports discrimination claims.[24] In the same month, the Commission issued this proposed Statement, whose own illustrative examples describe pricing that turns on factors pertaining to protected classes such as identity, religious views, and sexual orientation. We urge the Commission to consider the usefulness of discriminatory pricing enforcement  as a tool for addressing surveillance pricing and other consumer harms. Discrimination satisfies the statutory definition of unfairness on its own terms. A practice is unfair under Section 5(n) of the FTC Act if it causes or is likely to cause substantial injury to consumers, the injury is not reasonably avoidable, and the injury is not outweighed by countervailing benefits to consumers or competition.[25] Surveillance pricing meets each element. The injury is monetary and concrete, consumers pay a higher price. Addressing surveillance pricing mechanisms is not a narrow intervention on behalf of a few; it is a useful tool for challenging unfair practices and ensuring the same price for everyone. Even if the Commission does not wish to utilize Unfairness authority to reach discriminatory pricing, its traditional enforcement of pricing discrimination through ECOA could achieve the same result.

At a moment when AI is making pricing systems more granular and more opaque, the Commission should be expanding the scope of its enforcement capacity, not narrowing it.

## IV. Loyalty and rewards programs are a major, under-addressed vector for surveillance pricing.

Loyalty and rewards programs are a primary channel for extracting exorbitant amounts of personal data from customers and to engage in surveillance pricing. A recent report from Vanderbilt and UC Berkeley describes the result as the "wholesale transfer of wealth from consumers to corporations, with companies collecting ever-more data while offering ever-diminishing savings." A WIRED reporter received a 515-page file from McDonald's loyalty program containing algorithmic predictions of how often he would visit, how much he would spend per order, and how likely he was to stop being a

[24] https://www.ftc.gov/news-events/news/press-releases/2026/08/ftc-ditches-disparate-impact
[25] https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness

customer.[26] The Statement's own examples rest on inferences of exactly this kind: conclusions about a consumer's household, movements, and urgency drawn from data and converted into a prediction about what that consumer will pay. Pricing strategies that would raise concerns regarding Section 5 of the FTC Act at the point of sale should not fall outside the Commission's notice because the data was gathered and applied within a rewards program.

We urge the Commission to clarify that enrollment in a loyalty program does not constitute consent to surveillance pricing, and that the disclosure obligation attaches at both moments: at enrollment, that program data may be used to set the prices that loyalty program member personally pays, and at the point of sale, that the resulting price is personalized. The concern is not with discounts offered to all members on publicly disclosed terms, which consumers understand and can evaluate —it is with individualized pricing that a loyalty program makes possible and a membership card makes invisible.

Loyalty programs also create privacy harms that surface later as costs consumers never connect to enrollment. The data these programs generate does not stay with the retailer, it is often sold for profit to data brokers, and once it reaches parties with no role in delivering any program benefit, the consumer has no practical way to trace it or contest how it is used. The Texas Attorney General alleges that Allstate's subsidiary Arity embedded tracking software in mobile applications including the Fuel Rewards and GasBuddy rewards apps, collected and sold data on roughly 45 million Americans, and that insurers used it to justify raising premiums, denying coverage, and dropping coverage.[27] A consumer who enrolls in a gas rewards program to save a few cents per gallon cannot anticipate that the resulting data may raise their auto insurance premium, cannot learn that the loyalty program was a cause of the harm, and cannot contest it. This bears directly on whether such injuries are reasonably avoidable under Section 5(n) of the FTC Act. It also raises deception concerns, since a consumer who enrolls to receive discounts is not told that the resulting data may travel to firms that will use it to set unrelated prices.

The Commission's authority under Section 5 of the FTC Act also examines impacts to competition. Loyalty programs let incumbents accumulate proprietary behavioral data

---

[26] https://www.wired.com/story/mcdonalds-built-a-515-page-dossier-on-me-it-says-ill-never-leave/

[27] https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

and locked-in customers that smaller competitors cannot replicate, raising entry barriers, facilitating greater consumer surveillance, and dampening rivalry among competitors. The Australian Competition and Consumer Commission's review of customer loyalty schemes found that rewards programs designed to make exit costly reduce competition and over the long run such schemes can yield higher prices or lower quality, regardless of discounts they deliver in the meantime.[28] Economic modeling reaches a similar conclusion: because these programs make stealing a rival's customers less profitable, they facilitate tacit collusion and firms become less likely to price competitively.[29] The resulting higher prices are an injury consumers are unable to perceive because the relevant comparison is the price that would have prevailed in a market without loyalty programs, a price no member can observe.

The Commission should make clear that personalized pricing within loyalty and rewards programs are subject to the same disclosure requirements as any other form of personalized pricing, and that enrollment in such a program is not consent to the practice. Moreover, the Commission should note that loyalty programs may cause consumer injury cognizable under Section 5 of the FTC Act, and that where such programs foreclose competition, that conduct may warrant scrutiny under the Commission's competition authority as well.

## V. The Commission should address personalized pricing through false "discounts."

The Commission should also confirm that personalization delivered as discounts, not only as price increases, can raise concerns regarding compliance with Section 5 of the FTC Act. The Statement's illustrative examples describe personalization as charging a consumer a higher price, but they do not identify the baseline against which "higher" is measured. A seller can deliver fully individualized pricing while maintaining that no consumer is charged above its posted price, and that therefore no harm is done and no disclosure is owed. The Statement should foreclose that reading.

The Commission has already recognized the problem elsewhere in the Statement, observing that consumers may be deceived when a personalized price presented as a discount is in fact a higher price derived from other data. We urge the Commission to carry that recognition into its examples and its unfairness analysis by stating that the relevant comparison is the net price a consumer pays relative to what other consumers pay for the same product at the same time, not the seller's own list price. Within this framing, a consumer who pays more than others for the same product or service as a

[28] https://www.accc.gov.au/about-us/publications/customer-loyalty-schemes-final-report
[29] https://insight.kellogg.northwestern.edu/article/membership_has_its_punishments

result of personalized pricing may suffer substantial injury, whether that difference is imposed as an increased price or delivered as a purported discount offered to some consumers and withheld from others based on their personal information.

Finally, the Commission should note that a reference price maintained for the purpose of making personalized discounts appear larger than the savings they deliver is deceptive under its Guides Against Deceptive Pricing, 16 C.F.R. Part 233, which prohibits claims that create a false impression of savings.[30]

## VI. Insurance, housing, and rental markets deserve specific attention as high-risk areas.

Personalized pricing in regulated industries (e.g. housing, insurance, etc.) should be based on actual risk, not willingness to pay. There have been reports and settlements indicating insurers are improperly using WTP (Willingness to Pay) in their pricing.[31,32] Additionally, in the rental housing market, where the factors that go into establishing rent pricing are largely kept from public view, dynamic pricing systems based on AI have become a widespread feature. Rent prices can change weekly, daily, or more frequently, based on any number of factors that are hidden from consumers, making it profoundly difficult for prospective tenants to understand why they are being charged a certain rate. ProPublica has reported that the company that produces the leading rental pricing software (RealPage) uses its clients' leasing data in pricing formation, which is believed to effectively cause rents to increase. Following this revelation, the U.S. Government Accountability Office reported that rental rates had increased 24% in the last three years and the U.S. Department of Justice filed a Statement of Interest in the anti-trust litigation against RealPage.[33] This finding illustrates why disclosure alone does not address the harms of surveillance pricing, particularly in essential markets where higher prices have downstream effects on all consumers, not only a few.

## VII. The Commission should require disclosures that consumers can act on.

As set out above, we do not believe disclosure is an adequate remedy. The recommendations in this and the following sections address how the Commission's disclosure standard should be improved if it proceeds on that basis. We support the

---

[30] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-B/part-233
[31] Suckers List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders – The Markup
[32] Allstate Price Optimization – Consumer Watchdog
[33] https://www.banking.senate.gov/hearings/artificial-intelligence-and-housing-exploring-promise-and-peril

Commission's articulation of what a personalized pricing disclosure should contain: the fact that the price is personalized, the basis of that personalization, and the type(s) of data used. We likewise support the Commission's recognition that a disclosure must include all relevant information and must give the consumer enough to identify potentially incorrect information, take measures to avoid the personalized price, or avoid future collection of data for that purpose. We urge the Commission to elaborate on what those requirements demand in practice in the Statement. Additionally, disclosure must also occur at the point of collection, prior to any action or decision on the part of the individual. Consumers who enroll in a loyalty program, make a purchase, or click through terms of service are almost never told that the data they are handing over may later determine the price they personally pay. Collection-time disclosure alerts consumers and provides them with the right to decline. It is not a substitute for pricing-time disclosure, and the standard should require both.

The following data elements would allow consumers to understand how their data is used and whether it is worth taking any of the steps the Commission describes

1. A disclosure should also allow a consumer access to the sources of the data used, and in particular whether it includes data obtained from third parties.
2. A disclosure should identify the inferences drawn about the consumer that contributed to the price, not only the categories of data collected.

A disclosure should indicate how the personalized price relates to what other consumers pay. A disclosure that omits sources, inferences, and comparison leaves the consumer aware of the practice but unable to effectively act on it. The Statement's reliance on the Fair Credit Reporting Act (FCRA) supports this reading. FCRA does more than announce that a decision was individualized: it entitles the consumer to the underlying report and to dispute what is inaccurate.[34]

## Conclusion

The Commission must take action to address the harms of surveillance pricing beyond merely a simple, undefined, transparency requirement and instead prohibit the practice. By issuing a ban on surveillance pricing, the Commission will protect the most at-risk populations and ensure fairness in the marketplace.

[34] Title IV of the Consumer Credit Protection Act

Thank you for considering our views,

Sincerely,

National Fair Housing Alliance

The Leadership Conference on Civil and Human Rights

TechEquity Action

Consumer Federation of America

League of United Latin American Citizens (LULAC)

Autistic Women & Nonbinary Network

JustLeadershipUSA

Oakland Privacy

Kapor Center Advocacy

Courage California

Feminist Majority Foundation

California Partnership to End Domestic Violence

Consumer Action

TechTonic Justice

Common Cause

Economic Security California

National Association of Consumer Advocates

MPower Change

United Church of Christ Media Justice Ministry

The Greenlining Institute

Fair Housing Advocates of Northern California

Electronic Frontier Foundation (EFF)

Asian Americans Advancing Justice | AAJC

Dream.org

UnidosUS

Service Employees International Union

Interfaith Center on Corporate Responsibility