Insights, News & Events

# FEDS PROPOSE NEW DISCLOSURE RULES FOR PERSONALIZED "SURVEILLANCE" PRICING; BUSINESSES CAN COMMENT BY SEPT 18

Insights
Aug 24, 2026

## Feds Propose New Disclosure Rules for Personalized "Surveillance" Pricing; Businesses Can Comment by Sept 18

The Federal Trade Commission just proposed a new policy that would require businesses to tell customers when they're being charged a different price than someone else for the same product based on that customer's personal data. The proposal, released August 19, targets what the FTC calls personalized pricing (the same practice often referred to as "surveillance" pricing), and gives the public until September 18 to weigh in before it's finalized. For businesses in retail, delivery, hospitality, and e-commerce that already use dynamic or algorithm-driven pricing, the proposal explains exactly what FTC agents will look for during any investigation. What do you need to know – and do?

### What the FTC is Proposing

The Commission's August 19 announcement acknowledges it lacks authority to prohibit personalized pricing across the board. Companies often offer varied pricing by consumer for legitimate reasons. These include insurance premiums that reflect individual risk, loan rates that reflect creditworthiness, and rideshare fares that shift with local supply and demand. But the FTC says the sheer volume of data companies now collect on individuals allows them to change the price on the shelf or the screen based on other factors unique to each consumer.

## Related People



**Risa B. Boerner, CIPP/US, CIPM**
Partner

610.230.2132



**Usama Kahf, CIPP/US**
Partner

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

The FTC's position is that businesses using personalized pricing should clearly and conspicuously disclose three things:

- that the price is personalized
- the basis for the personalization, and
- the types of data used to set it

The Commission says that failing to do so likely constitutes an unfair or deceptive practice under Section 5 of the FTC Act.

**FTC: "Special Price" Language Won't Be Enough**

The proposed statement says you can't just tell a shopper they've received a "specially selected" or "personalized" price and nothing more without running afoul of the law. The agency said it would treat that as likely misleading because it omits the information a consumer would need to act on it.

By contrast, the FTC offers an example of adequate disclosure. If you accurately and completely tell a consumer that a price is based on their purchase history with your business, that would pass the agency's muster.

**2 Legal Theories**

The FTC says it will pursue personalized pricing issues under both of its core Section 5 theories:

- **Deception.** Representing or implying that a price is static or generally available when it's actually personalized, or misleading consumers about the basis or effect of that personalization, can support a deception claim.
- **Unfairness.** Even without an affirmative misrepresentation, concealing that a price is personalized can be unfair if it prevents consumers from taking steps to avoid a higher price, such as comparison shopping, using a different browser or device, or correcting inaccurate data being used against them.

The statement also notes that certain data handling practices related to personalized pricing could be within the FTC's sights for another reason. If you collect, use, or share consumer data to help fuel a personalized pricing model

949.798.2118



**Danielle Kays**

Partner

312.260.4751

## Service Focus

Consumer Privacy Team

Government Relations

Privacy and Cyber

## Industry Focus

Hospitality

Retail

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

without adequate disclosure or consent, you could be separately violating the FTC Act's Section 5.

**Examples of Potential Violations**

The FTC's proposal includes a list of illustrative scenarios that would raise Section 5 concerns. Among the examples:

- a **food delivery company** charging more to consumers it believes are less able to leave their homes;
- a **grocery chain** charging more for delivered milk because data shows children live in the household;
- a **hotel** charging more because it infers a guest is traveling for a funeral; and
- a **retailer** raising a price when data shows the shopper is currently browsing from inside one of its own physical stores.

**What Should You Do?**

If your business is in retail, hospitality, delivery, ride-hailing, or e-commerce generally and you use dynamic, algorithmic, or data-driven pricing, consider taking these steps now:

**1. Inventory your pricing models.** Identify every place where price, discount, or fee amounts can vary based on data tied to an individual consumer, rather than a broad segment or a neutral factor like time or location.

**2. Audit your disclosures.** Compare existing consumer-facing language against the FTC's three-part standard: does it say the price is personalized, why, and what data was used? Generic "prices may vary" language probably won't be enough.

**3. Trace your data consent chain.** Confirm that any personal data feeding a pricing model was collected with sufficient disclosure and consent.

**4. Watch how this interacts with your CIPA and surveillance pricing exposure.** The data collection practices that power personalized pricing are the same practices driving the wave of digital wiretapping and surveillance pricing litigation we've been tracking.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

**5. Monitor federal and state legislative activity.** We recently created an overview about legislative proposals across the country related to surveillance pricing. Take a look here and make sure you are tracking any laws that could impact your business.

**6. Submit a comment before September 18.** The FTC is accepting public comment on the proposed statement, and this is your opportunity to shape a finalized disclosure standard. Reach out to your Fisher Phillips attorney or our FP Gov Team for guidance on participating in the process.

**Conclusion**

Fisher Phillips will continue to monitor developments in this area. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or anyone on our Privacy and Cyber Team.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.