

Senate Judiciary Committee
Subcommittee on Crime and Counterterrorism
Hearing on “Your Data, Their Profit: The Consumer Cost of AI Surveillance Pricing”
August 4, 2026
Questions for the Record
Senator Amy Klobuchar

For Bob Hedges, Digital Fellow at MIT’s Initiative on the Digital Economy

1. Surveillance pricing is possible because of the vast amounts of personal data collected about consumers, from browsing histories to location data.

- **Do consumers typically consent for this data to be used to set personalized prices?**

No. Consumer consent requests do not explicitly ask for permission to use the consumer’s data for “personalized pricing” or “pricing setting.” To inform this assessment, we reviewed five leading brands’ consent and data privacy policies. We also examined the five companies’ approach to data use permissions as well as the variety of mechanisms across which permission is commonly sought. Our findings are summarized below.

Companies’ data use consent requests are generally broad and non-specific because there is no obligation to be specific about their planned data uses. As a result, companies generally do not provide consumers with detailed information regarding how the collected data might be used.

While consumers routinely consent to the collection and sharing of data, the consent requests rarely or never refer to “personalized pricing” as a planned use of the data. The consent request may refer to “personalization,” but “personalization” is generally meant to imply (a) shopping recommendations, (b) greater marketing message relevance, (c) targeted advertising, or (d) greater check-out convenience. We found no examples of a company disclosing that consumer data was being collected to inform or infer a consumer’s “willingness to pay.”

We reviewed the publicly available data privacy and consent documents of Instacart (delivery service), Uber (ride-hail), Amazon (digital marketplace), Ticketmaster (ticketing), and Kroger (grocery). From this policy review, we can make the following observations:

- Across the five companies, only one company’s data permission documents explicitly called out “pricing” as a use of personal data – Uber. In [Uber’s rider notice](#), the document lists “price” and “fare calculation” as a data use and limits the inputs to location and trip data. The use of personal data for “pricing” is defined, however, as a contractual

necessity rather than consent. Under Uber's framing, a rider cannot withdraw from the pricing use, because it is a term of the contract rather than a permission.

- [Ticketmaster's policy](#) does not mention pricing anywhere, yet its own California disclosure table reports selling or sharing transaction information and consumer preferences and attributes with data brokers. A policy that never mentions pricing can still provide the data to inform willingness to pay signals.
- [Instacart's privacy policy](#) does not mention pricing either, and the company's clearest commitment, that it will never use personal information to set prices, appears in a [corporate update page](#) rather than in any privacy disclosure document.
- [Amazon's notice](#) is the best example of how limited consent requirements can be. The Amazon notice states that by using Amazon Services you are consenting to their data practices – no explicit click, signature, or account is required. Amazon's list of data uses is otherwise granular, naming generative AI model development, voice and image services, and credit risk scoring. "Pricing" is not on their list of data uses. The state-specific disclosures that would carry any profiling opt-outs are in a separate document that the formal notice links to.
- [Kroger's notice](#) is the only one that addresses the "consent for pricing" question directly and actually answers it in the negative twice. The Kroger notice explains how, pursuant to state consumer privacy laws, Kroger does not profile in a manner that would result in legal or similarly significant effects and therefore does not offer the profiling opt-out right. Its non-discrimination provision then says Kroger will not charge different prices or provide a different level of service unless those differences are related to the value of a consumer's personal data. "Pricing" is never named as a specific use case. "Providing discounts," however, is named as a purpose for nearly every data category Kroger collects, including browsing and search history, characteristics of protected classifications, and inferences.

From this review of these five leading brands, there is no example where a consumer is asked to consent to have their personal data shared for the purpose of pricing. While Uber does explicitly raise the use of personal data for pricing, it is a contractual term of service, not a consented or permissioned use.

Silence on "pricing" does not imply that they do not use personal data for pricing. To be clear, current regulation does not require obtaining explicit consumer consent for each defined data use. Silence, or the omission of a request for explicit consent to use personal data for pricing, is fully acceptable under current federal law.

It is hard to imagine an informed consumer ever consenting to have their personal data used to inform a company's price optimization engine. We should not be surprised that companies do not explicitly ask for consumers' permission to do so.

In reviewing current industry practices and regulations around obtaining consumers' consent for using personal data for pricing, there is a pattern in the approaches of how today's consent practices and regulations fall short of obtaining consumers' explicit consent for using personal data for personalized pricing. Three approaches are evident:

- 1. The consent request for pricing is simply never made:** While consent may be requested for "collection and sharing," "pricing" is not indicated as one of the approved use cases. The company is not explicit and transparent about their intentions for the "pricing" data use.
- 2. Consent covers only the collection of the data, not how the data might be used:** No consumer is asked to agree to be assigned an estimated "willingness to pay" score based on their personal data. Permission may be granted for the collection of data for what consumers may believe is "benign" use case. The consumer is not aware, or informed, that the data can be used in behavioral modeling. As a result, the resulting analytical output (e.g., a consumers' willingness to pay score) can be developed and applied outside the scope of the notice-and-choice frameworks built around categories of information the consumer supplied.
- 3. Consumers have no relationship with, or even knowledge of, the third party doing the behavioral profiling for pricing:** The data broker or pricing intermediary providing "pricing" signals to a retailer usually has no direct dealings with the consumer. No communication occurs, no permission is obtained, and no such permission is required. Consider and compare how the ordinary rule for lost property works – where a person who finds a stranger's wallet owes that stranger a duty to safeguard it and return it, and the duty arises from possession alone without any prior relationship. A data broker holding the same consumer's purchase history owes no comparable duty, because the purpose limitation that does exist under state privacy law is a contract term between the disclosing business and the recipient, which leaves the consumer unable to enforce the restriction meant to protect them.

In reviewing companies' data use disclosures, the use case of "pricing" is generally absent – the disclosures neither seek consent nor pre-emptively waive the right to use personal data for "pricing" purposes.

The policy review does reconfirm and spotlight one key issue – for a consumer, even if you read every word of the corporate disclosures, it is still not clear whether or not your personal data is being used for pricing. There is a significant opportunity to make the consent language simpler,

clearer, and more concrete on the very basic question of whether or not personal data is being used to inform pricing.

Beyond the clarity of the data use policy, another challenge in securing clear and appropriate consent to use personal data for pricing is the variety of different and overlapping mechanisms through which a consumer's consent for using their personal data might be sought. To successfully deploy a consent scheme to manage the use of personal data for pricing purposes, the full set of different channels or mechanisms through which consent can be obtained must be addressed.

There are six different mechanisms that companies commonly use to capture consumers' consent for use of consumers' personal data. The mechanisms vary in (a) the breadth of the consent requested, (b) the nature of the data elements covered, and (c) the level of detail of the data use cases for which consent is applicable. Only one mechanism – loyalty and rewards enrollment – is used to request and obtain permission to capture consent to use a consumer's data for explicitly economic reasons. Consider each of the individual channels or mechanisms for capturing consent:

- 1. Terms of service and privacy policy acceptance:** “Terms of service” is the all-purpose corporate workhorse for capturing consumers' consent for data use. For the consumer, clicking through the terms of service screen, creating an account, or in some formulations continuing to browse on a website constitutes the formal agreement and documentation by the consumer to permit the collection and sharing of behavioral data for broadly-worded purposes such as “personalization,” “service improvement,” and “analytics.” “Pricing” is almost never explicitly named. All the additional mechanisms that are used to capture consent (and are discussed below) trace back to a company's foundational terms of service and privacy policy. Cookie banners, app permissions, and onward data transfer policies all operate within the scope of the terms of service and privacy policy acceptance documents rather than granting authority of their own.
- 2. Cookie banners and consent management platforms:** In the United States, cookie banners and consent permissions are predominantly structured as “opt-out” requests. If the consumer declines or fails to object, it is deemed that the consumer has provided the necessary permission for the requested data use. Cookie banners are usually used to obtain permission to track a consumers' browser and shopping behavior. It is not explained that the consumer web tracking data can be used to inform pricing decisions.
- 3. Mobile application permissions:** Consumers' consent to collect location, contacts, and notification permissions are usually granted for a functional reason – usually the delivery or pick-up of a product. The software development kits embedded in a retailer's applications, however, can then route the same signals elsewhere for whatever purpose. The resulting permission granted, and the use the data is put to, are separated by several

steps and the initial consent request does not describe the specific uses. It is not explained that the location data can be used to inform pricing decisions.

4. **Biometric and in-store sensing consent:** Facial recognition and comparable systems generally require affirmative informed consent under state biometric statutes. Biometrics is the one category where the notice reliably appears at the moment of collecting the consent. The permitted uses are generally correspondingly narrow. Kroger's facial recognition notice, for example, names security, customer and associate safety, and the prevention of shoplifting and fraud, but nothing else.
5. **Downstream transfer under an original consent:** The granting of permission to "data share" is an important mechanism to providers in the digital/data ecosystem, but not very visible to consumers. A consumer consents to the specific company that they are dealing with and to that company's policy allowing the sharing of the consumers' data with partners and service providers. The consumer's data can then be transferred to other companies that the consumer has never heard of, for purposes that have not been disclosed to the consumer. In its [January 2025 staff perspective](#), the Federal Trade Commission reported that the data brokers it examined worked with at least 250 corporate clients selling goods and services ranging from grocery stores to apparel retailers.
6. **Loyalty and rewards enrollment:** Generally speaking, loyalty and rewards programs go the farthest in seeking clear and informed consent from consumers to use personal data to inform pricing decisions. Some of this is "best practice" and some of it is state regulation. California, for example, regulates loyalty programs as "financial incentives," which requires a written notice, opt-in consent to the material terms, revocability, and a good-faith estimate of the value of the consumer data involved. Colorado uses a parallel construct for bona fide loyalty programs.

Only in the domain of loyalty and rewards programs do we see regulatory requirements to obtain the consumers' informed and explicit permission to opt-in to share their data. Unfortunately, the loyalty and rewards space is precisely the domain that every state-enacted surveillance pricing law carves out.

In conclusion, consumers are rarely asked to consent for their personal data to be used for the purposes of "pricing." As a result, there is a significant opportunity with federal regulation to both (1) strengthen the required clarity around the company's data use disclosures to ensure consumers understand how their data is being used and (2) require explicit disclosure of how personal data is used, or not used, to inform pricing. To be successful, the disclosure and consent must be (1) concrete and use case-specific and (2) consistently deployed across the various channels and mechanisms through which companies seek and receive permission to use consumers' data.

2. It is nearly impossible for consumers or enforcers at the Federal Trade Commission to know whether a seller is using personal data to set prices.

- **How would mandatory disclosures by sellers that engage in surveillance pricing affect the incentive to engage in this practice?**

Mandatory disclosure would reduce the incentive to engage in surveillance pricing.

Today, it is generally acknowledged that “reputational risk” is the major constraint on how companies use or share personal data. Mandatory disclosure would ensure public awareness of the practice and bring forward the reputational and brand risk that most companies seek to minimize. Mandatory disclosure of the practice of using consumers’ personal data to inform pricing would be good public policy. In the below response, the evidence around the benefits of mandatory disclosure practices is shared. How to make the disclosure requirement fully effective is also discussed.

There is good evidence that mandatory disclosure works as a deterrent. Consider three examples of mandatory disclosure regarding public health considerations:

- Under California Proposition 65, [research published in Environmental Science and Technology](#) found that companies commonly replaced warning-triggering ingredients altogether rather than use them with a required disclosure or label, partly to avoid litigation.
- A companion Silent Spring Institute biomonitoring analysis, [reported in Scientific American](#), found measured declines in eleven of the listed chemicals for which before-and-after data exist, in California residents and nationally. This comes from cases where firms changed the product rather than make the mandatory disclosure. The prospect of disclosing the ingredients was a sufficient deterrent to change the practice.
- Los Angeles County restaurant hygiene grade cards produced the same pattern. [Jin and Leslie](#) reported mean restaurant hygiene scores rising from roughly 77 to roughly 90 after posting became mandatory, and foodborne illness hospitalizations falling by about twenty percent.

The New York’s Algorithmic Pricing Disclosure, in effect since November 2025, is designed specifically to achieve this effect. The required sentence, that “THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA,” is stigmatizing rather than merely informative, and it appears at the point of transaction. A retailer that does not want to display it has one reliable way to avoid it, which is not to employ surveillance pricing tactics. This mandatory disclosure deterrent is very real.

There are two high-profile examples of how public disclosure of the use of personal data to inform pricing, and the accompanying reputational and brand risk, can change companies' pricing practices:

- Amazon [abandoned differential pricing in 2000](#) after customers discovered a DVD price test, and [industry analysts still cite that episode](#) as the reason large retailers hold back. The pattern repeated recently and without any disclosure law doing the work.
- Instacart ended randomized retailer price tests in December 2025 following a [letter from Senator Klobuchar to the FTC chair](#), an [information demand from the New York Attorney General](#) on January 8, 2026, and a [House Oversight letter](#) on March 5, 2026, and then [published a public commitment](#) in July 2026 not to use personal information to set prices. Growing public awareness of their surveillance pricing tactics, and the immediate impact of Instacart's corporate reputation, ended the practice.

Mandatory disclosure would have impact because it ensures public awareness of a practice for which most companies are not prepared to carry the brand or reputational risk.

Mandatory disclosure will also dramatically increase consumer awareness of corporate practices. One of the biggest challenges with the companies' use of consumers' personal data for pricing is that consumers cannot easily detect or recognize the practice. Academic research has proven how challenging it is to detect companies' application of personalized pricing programs. A [leading academic research project examining](#) price discrimination and steering required roughly three hundred real user accounts, plus matched synthetic controls, across sixteen corporate websites, to collect evidence of personalized pricing at corporate websites. Consumers cannot be expected to undertake such efforts to protect themselves against their personal data being used against their interests

Mandatory disclosure converts a complex research inquiry – is personal data being used to inform pricing – into a straightforward question – does the company, yes or no, use personal data to inform pricing. For the consumer, the mandatory disclosure replaces the need to do personal research and due diligence by simply providing clarity on the corporate practice. The Federal Trade Commission's [proposed enforcement policy statement](#) of August 19, 2026, somewhat adopts this approach in defining the failure to disclose the use of personal data in pricing as a “deceptive practice” under Section 5 for the FTC Act.

Of course, a mandatory disclosure requirement is vulnerable to how companies practice “self-classification.” Companies will need to assess and decide whether their own conduct triggers the need for disclosure. Current corporate disclosure documents around the use of personal data suggest that companies might answer the question in a careful and calculated manner to avoid having to make the disclosure. Great care will be needed in drafting the regulation and disclosure

requirements to minimize companies' ability to use nuanced definitions to avoid being subject to the disclosure requirement.¹

At the same time, the disclosure requirement will probably do little to reduce the collection, brokerage, and inferential use of the consumer behavior data. Data practices that fall into the “gray area” of being “sort of questionable but not prohibited” will probably continue. We should also anticipate the continuing evolution of the personalized pricing from “consumer-specific pricing” to the greater use of personalized discounts. Future regulation should address these real issues.

In conclusion, mandatory disclosure will meaningfully deter surveillance pricing at branded, consumer-facing merchants, because those firms are reputationally exposed and the label of “engaging in surveillance pricing” is stigmatizing. As a result of mandatory disclosure requirements, we should see a reduction in this consumer-harming practice.

In addition to the mandatory disclosure of the use of personal data for pricing, federal legislation should consider three additional obligations/design features that would further strengthen consumer rights protection around the collection and use of personal data for pricing:

- 1. Require companies to retain and periodically report the data inputs to their pricing models inputs to the relevant regulator.** A mandatory consumer-facing disclosure label alone leaves non-disclosure undetectable, because nobody outside the company can audit their pricing practices. Corporate reporting would address this issue.
- 2. Extend the public disclosure requirement, not just to retailers and marketplaces, but also to data brokers and intermediaries.** If data brokers or intermediaries are creating or providing “willingness to pay” signals or inputs, that practice itself should be publicly disclosed. New York's pending [One Fair Price Act](#) goes further, prohibiting the use or transfer of personal data for the purpose of facilitating surveillance pricing.
- 3. Attach the disclosure duty symmetrically to the offering of personalized discounts.** This approach is what the [failed California surveillance pricing bill](#) would have required. Without it, the exemption every state legislature has written for loyalty programs and personalized discounts becomes an efficient compliance path rather than the edge case to be explicitly addressed.

Mandatory disclosure would be a powerful first step to deter and curtail the practice of surveillance pricing. We need to acknowledge, however, that it is just a first step. We also need to (1) ensure the disclosure requirement applies to a broad enough set of the players in the data

¹ Ticketmaster states that it does not typically carry out automated decision making. Uber classifies price calculation as contract performance. Kroger goes the furthest, stating in writing that it does not profile in a manner producing legal or similarly significant effects, which is the statutory trigger, and declining to offer the profiling opt-out on that basis.

ecosystem, (2) make self-reporting of the use of consumer data as an input to pricing part of regulatory obligations, and (3) monitor ongoing evolution of pricing analytics and strategy so that consumer-harming price discrimination does not simply get reinvented in another format.