AMERICAN ECONOMIC LIBERTIES PROJECT

Minding the Gaps in Surveillance Pricing Reform

How to ensure pricing protections work as intended, and are not undermined by loopholes

Stephanie T. Nguyen, Senior Fellow, Center for Law and the Economy
Lee Hepner, Senior Counsel, American Economic Liberties Project

Surveillance pricing — the practice where corporations use vast troves of personal data including search history, past purchases, location information and more to tailor prices to individual customers — has become inescapable. This is despite the fact that recent polling shows most people — across party lines — don't like it. Among the major retailers facing public scrutiny and, in some cases, legal challenges, are Instacart, Delta, JetBlue, The Washington Post, Uber, Lyft, Amazon, and Google.

In response, lawmakers across federal, state, and local jurisdictions have introduced a growing number of surveillance pricing bills aimed at banning the discriminatory practice. Yet, across these jurisdictions, the same opposition arguments and industry-motivated carveouts keep popping up, leading to laws that purport to solve a problem when in fact they grant permission for pricing abuses.

Banning surveillance pricing relies on a simple premise: Companies should not be able to weaponize granular consumer data to make inferences and profiles, for the purpose of setting targeted prices for the same products. They include carefully considered exemptions aimed at preserving, for instance, benign and accepted forms of discounting based on personal information, like senior or student discounts. Unless narrowly defined, the exemptions become the rule by which ubiquitous price discrimination continues.[1] Maryland's recently signed law presents a cautionary tale. The final version included gaping loopholes for discriminatory loyalty programs, individually-targeted "promotional offers," and undefined "temporary discounts," among other provisions that grant sweeping permission for surveillance pricing to continue. The biggest threat to effective surveillance pricing legislation is this quiet flourishing of carveouts and exceptions, which can weaken and undermine true reform.

This memo aims to build upon a prior analysis, showing the most common problematic carveouts for surveillance pricing legislation. The goal is to help lawmakers and regulators anticipate and avoid such loopholes, which risk neutering a prohibition and allowing surveillance pricing legislation to become a permission slip rather than a restriction on ubiquitous price discrimination. Below are some of the most common loopholes that weaken and derail reform.

—

The Surveillance Pricing Bill Loopholes

1. The "Loyalty Programs" Trap

The loophole: Exempting "loyalty programs" from surveillance pricing.

Loyalty programs can offer pro-competitive, non-discriminatory benefits to consumers when they are offered to all consumers, pursuant to consistent terms, and implemented equitably across all participants. Among the most common talking points against surveillance pricing legislation is that banning surveillance pricing will prohibit companies from using loyalty programs to offer consumer benefits; such as freebies, points, perks, exclusive or first access to products, promotional events, and more.

Depending on how they are defined, "loyalty programs" may encompass a range of common retail practices. Sandwich punchcards are a form of loyalty program where

[1] Distinguishing between unfair surveillance pricing and widely accepted discounts that nevertheless rely on the exchange of personal information is both necessary and possible. For example, senior or student discounts can fall under a broad definition of price discrimination, but are not "surveillance pricing" to the extent they are tethered to widely recognized and broad customer segments, are standardized so that all eligible consumers can avail themselves of the same offer, and facilitate a knowing and consensual exchange of information. Happy hours, end-of-season clearances, and matinee movie prices are outside even the broadest definition of surveillance pricing, inasmuch as they do not require any vetting of eligibility based on personal information.

benefits are clearly advertised and accruable by all participants. Credit card rewards programs offer points or tokens, redeemable against the purchase of products or services from retail partners. Loyalty programs also involve the exchange of voluminous personal information, including purchase histories that may be exploited to discriminate between program participants. In the broadest sense, “loyalty programs” might also include mailing list subscriptions, which are ubiquitous if not obligatory in many online shopping contexts, and where the exchange of personal information for targeted offers is least explicit.

The purpose is not to ban loyalty programs, but to protect them from becoming vectors for abuse. Participation in a loyalty program should be based on meaningful consent and should honor consumer expectations that terms and conditions will be standardized across all program participants. When one consumer’s “rewards points” are valued differently than another consumer’s, for instance, loyalty programs become a bait-and-switch tactic for surveillance-based price discrimination.

A recent study by one of the authors of this piece illustrates how consumers may be lured, or “hooked,” into a loyalty program, only for the provider of that program to “hack” the participants’ personal data and “hike” the price of goods. This “hook-hack-hike” methodology chafes against the notion that all loyalty programs are designed to offer consistent and real benefits to program participants.

Why it’s a problem: Surveillance pricing bans rightfully exempt loyalty programs that depend on some exchange of personal information for true benefits. But protecting loyalty programs from abuse is obligatory and can be done by mandating that terms be publicly available and consistently applied across all program participants. Otherwise, loyalty programs can function as a Trojan horse: generous to consumers at the gate, but once they’re enrolled, laden with hidden fees, intrusive data extraction, and discriminatory pricing.

How to avoid the loophole: States should ensure that “bona fide” loyalty programs are based on publicly advertised and consistently applied terms across a market and are not weaponized as a broad carveout for abusive surveillance practices.

2. The “Personalized Discounts” Trap

The loophole: Exempting “personalized discounts.”

Opponents of surveillance pricing legislation argue that “targeting and personalization are what make many modern discounts viable.” Opponents levy this criticism even where proposed legislation contains explicit carveouts for discounts that are offered to broadly recognized groups — like seniors, students, or veterans — or offered to the general public pursuant to eligibility criteria that are consistently applied to all consumers.

Opponents have argued that coupons, for example, have long been a form of price discrimination, one which consumers and the broader public understand and accept as beneficial. But coupons are not “personalized” in the sense that they are targeted to individual consumers. Rather, the traditional understanding of a coupon is a discount that is available to all consumers willing to seek out a deal.

Why it’s a problem: Setting a discount is setting the price. A personalized discount is functionally indistinguishable from a personalized price because consumers cannot know whether they are receiving a discount or simply being charged what an algorithm predicts they will pay. We contend that the distinction is in name only. A “personalized discount” is not a “discount” in the sense of a verifiable good deal, but simply a prediction of an individual consumer’s willingness to pay the offered price. No consumer will have any way of knowing whether the price they’re being offered is one or the other. The effect is the same as with any other form of surveillance pricing: eroded consumer price sensitivity, an obscured standard price, discrimination, and diminished price competition.

How is a marketplace flooded with “personalized discounts” any different than one flooded with personalized prices? It is not.

How to avoid the loophole: Preserve exemptions for standardized, publicly available discounts while avoiding exemptions for individualized discounts based on personal information. Exemptions for standardized, public-facing discounts protect all of the benefits of robust price competition, but “personalized discounts” constitute a loophole that undermines the entirety of the rule.

3. The “Subscriptions” Trap

The loophole: Exempting subscription pricing.

Subscription-based pricing is a rapidly expanding market segment. For retailers, they provide a more stable method of forecasting baseline revenue. For consumers, subscriptions reduce the friction of repurchasing goods — and, critically, suppress the need for consumers to continually reckon with whether the price of a good or service justifies its worth. Subscription-based pricing is expanding rapidly across consumer sectors: In 2023, the subscription economy was valued at $492 billion globally and was expected to grow to $1.5 trillion by 2033, encompassing everything from streaming platforms to gym memberships to cat litter.

Why it’s a problem: Exemptions for subscriptions are not justified by either their rapid growth or the reduction in price frictions, which already erode consumer price sensitivity and suppress consumer awareness of price increases. In other policy contexts, like “click-to-cancel,” lawmakers recognize the behavioral harms of rollover subscriptions by ensuring that consumers can cancel subscriptions with the same ease as they enroll in them. That same scrutiny is warranted in the context of surveillance pricing legislation, where a wealth of consumer pricing information may be exchanged to exploit consumer ignorance of changes in price and discriminate between subscribers.

A recent lawsuit against The Washington Post further illustrates how consumer retention discounts can be exploited to discriminate between consumers. That lawsuit alleges that The Post extracted consumers’ personal information, including “engagement patterns, behaviors, preferences, demographic data, income, users’ preferences and characteristics, internet and browsing activity, location data, device information” — even browsing and purchase behaviors across parent company Amazon — to compile comprehensive profiles of subscribers and discriminate on price. When subscribers sought to cancel their subscriptions, they were offered nonsensical, differential retention rates — allegedly based on a valuation of their personal willingness to pay the offered renewal price.

How to avoid the loophole: Despite growing concern about the exploitation of subscription-based pricing to deceive and discriminate against consumers, some jurisdictions have been persuaded that subscription-based pricing should be exempt from surveillance pricing bans. These exemptions are unwarranted and adequately captured by the exemption for standardized discounts that are available to all consumers, pursuant to publicly accessible terms and equitably applied across all eligible or participating subscribers.

4. The "Consumer Segmentation" Trap

The carveout: Surveillance pricing is typically described as the use of personal information to offer prices that are unique to each individual consumer. But defining surveillance pricing at the individual consumer level mistakes how surveillance pricing may also be used to discriminate between consumer groups or consumer segments. Even where prices are targeted at consumer segments, the effect is the same: discriminatory pricing based on a prediction of that consumer group's willingness to pay a higher price.

Why it's a problem: The ability to target prices to consumer segments is readily observable on major advertising platforms like Google Ads and Meta. Social media and tech platforms more broadly have long been understood to facilitate targeted advertising based on inferences about user interests. But last year, Google Ads unveiled new features that allow for personalized pricing aimed at specified consumer segments, including based on predicted household income. Couched as the ability to offer "loyalty features," Google's ad platform supports the ability to target users based on "audience signals," including "long-term life facts," habits, interests, and "lookalike segments," to group consumers based on similar online behaviors and characteristics, and to customize product prices accordingly. The next evolution of such ad targeting involves integration with Google's "Universal Commerce Protocol," in which chatbot agents will personalize the shopping experience, coordinate and personalize prices, and facilitate purchases without the consumer ever leaving the Gemini interface.[2]

How to avoid the loophole: Targeting a price at a small group, segment, or "band" of consumers does not warrant inadvertent exemption by a too-narrow definition of surveillance pricing that only restricts truly individualized prices. Otherwise, surveillance pricing prohibitions can be too-easily circumvented by ensuring that at least two consumers are targeted with a discriminatory price.

[2] Matthew Stoller, "Will Google Become Our AI-Powered Central Planner?," The Big Newsletter, Jan. 16, 2026, https://www.thebignewsletter.com/p/will-google-organize-the-worlds-prices.

Accordingly, surveillance pricing legislation should encompass price discrimination based on inferences about "groups, bands, classes, or tiers" of consumers.[3]

5. The "Higher Prices as a Focal Point" Trap

The carveout: Prohibiting surveillance pricing only when it results in a "higher price" is unenforceable in the absence of a prevailing price.

Why it's a problem: There is an understandable political salience to banning surveillance pricing only where it would result in higher prices to consumers. But doing so misdiagnoses both the nature and effect of surveillance pricing. By its nature, and excluding bona fide discounts, surveillance pricing technologies are designed to match the offered price to the maximum amount any given consumer is willing to pay. Surveillance pricing is inherently a price-*maximizing* force, and the fact that this may result in some consumers paying lower prices than other consumers does not alter that basic intent.

The effect of surveillance pricing is not to lower prices, but to maximize prices. Opponents of surveillance pricing bills have argued that the effect of surveillance pricing is to lower prices and bring more consumers into the marketplace. But prevailing research says otherwise: In real world markets, the effect of surveillance pricing is expanded corporate profits, reduced consumer welfare, and market "segmentation" – meaning that more people are being left out of the store altogether.

Regulators who consider limiting surveillance pricing bans to "higher prices" are faced with an immediate challenge: Higher than what baseline? Retail prices are rarely fixed; they fluctuate due to opaque variables, and the number of those variables has grown immeasurably with the arrival of surveillance technology. As a result, legislation that predicates enforcement on the determination of a "higher price" distracts from the real source of harm: the unrestricted use of personal data to determine different prices for the same product.

How to avoid the loophole: The affordable aims of surveillance pricing law are served by preserving the concept of a prevailing price, and by protecting bona fide discounts and loyalty programs.

---

[3] Colorado HB26-1210 (2026) (*see* Sec. 6-1-1901, definition of "individualized.") https://leg.colorado.gov/bill_files/117019/download.

Looking forward

Industry representatives are quick to argue that surveillance pricing will lead to greater affordability, while glossing over how the underlying technology is designed to maximize corporate profits and extract more from every consumer in the market. When consumers can no longer discern the fair market price of a product or service, the consequence is reduced price sensitivity, reduced incentive and ability to engage in comparison shopping, and the inability to financially plan for daily expenses.

As of August 2026, three states (Maryland, Connecticut, and New Jersey) have passed legislation targeting surveillance and algorithmic personalized pricing. Colorado's strong-in-nation bill faced a veto by outgoing Democratic Governor Jared Polis.[4] Maryland successfully passed a surveillance pricing law, but it codified several of the very same carveouts outlined above by the time it was signed by Governor Wes Moore.[5] New York was the third state to pass a surveillance pricing ban, after Connecticut, but the bill was stripped of a provision allowing individual consumers to enforce the law.[6] Efforts are still in progress in other states,[7] from California to Illinois to Pennsylvania, and an increasing number of cities, from Seattle to New York City.

Carveouts and exceptions can hollow out a bill, preserving the very practices the legislation is meant to address. As many state legislatures wrap up their annual sessions, lawmakers must reestablish a stronger trajectory for the years ahead.

---

[4] Colorado Newsline, Surveillance Pricing Bill Vetoed, (July 1, 2025), https://coloradonewsline.com/briefs/surveillance-pricing-bill-vetoed.

[5] John S.W. MacDonald, Maryland Is First to Ban A.I.-Driven Price Increases in Grocery Stores, New York Times (May 1, 2026), https://www.nytimes.com/2026/05/01/business/surveillance-pricing-groceries-maryland.html.

[6] Electronic Privacy Information Center., New York Becomes Third State to Pass Surveillance Pricing Ban (June 4, 2026), https://epic.org/new-york-becomes-third-state-to-pass-surveillance-pricing-ban/; 2026 State of Connecticut House Bill No. 5563, Public Act No. 26-130, https://cga.ct.gov/2026/ACT/PA/PDF/2026PA-00130-R00HB-05563-PA.PDF.

[7] At least seventeen states have introduced surveillance pricing bills to restrict setting individual prices and wages based on invasive data collection. This includes CA, CO, HI, IL, LA, MI, MN, NE, NJ, NY, NM, OK, PA, UT, VT, TN, and WA.