“Surveillance Pricing”: Key Concepts, the Current Legal and Legislative Landscape, and Mounting Scrutiny

Paul L. Singer, Abigail Stempson, Alexander I. Schneider, Joseph Cahill

April 15, 2026

What Is “Surveillance Pricing?”

While proposed legislation across the country offers varying definitions of surveillance pricing (see below), it is generally thought of as the practice of using consumer data, algorithms, and artificial intelligence to set individualized prices for goods or services based on an assessment of a specific consumer’s behavior and characteristics. This can include data such as browsing behavior, purchasing history, location, device type, and inferred willingness to pay. In theory, some retailers may deploy surveillance pricing to tailor prices to individual consumers based on predications of what each consumer is likely to accept. It is also commonly referred to as personalized pricing, individualized pricing, behavioral pricing, and data-driven pricing. To fully understand surveillance pricing, it is useful to distinguish it from other pricing practices with which it is often confused.

Surveillance pricing differs from dynamic pricing which involves prices that fluctuate over time or in response to general market conditions, such as changes in supply and demand, inventory levels, time of day, or seasonality.

Surveillance pricing is also distinct from electronic shelf pricing (also known as digital shelf labels), which refers to the use of digital price displays, such as electronic shelf labels in physical stores, that allow retailers to update prices quickly and centrally across shelves and locations. Electronic shelf pricing is technology to address how prices are displayed and updated, and not how prices are determined; a retailer’s use of electronic shelf pricing does not, in and of itself, entail the use or collection of individualized consumer data in setting prices.

Finally, surveillance pricing is considered by many businesses and legislators to be distinct from offering loyalty programs or otherwise tailoring relevant discounts or coupons based on a customer’s purchase history or browsing behavior. In addition, businesses frequently offer lower pricing to certain eligible groups, such as military families, seniors, or students. Businesses dispute that using personal information to offer such discounts is “surveillance,” particularly where consumers agree to be part of a loyalty program or where such practices are performed in compliance with existing laws, such as comprehensive state privacy laws and unfair and deceptive trade practice laws.

Why Is It Controversial?

Surveillance pricing has drawn concern from consumers, legislators, state attorneys general, and

others due to transparency, fairness, and consumer trust issues. Consumers may be unaware that they are being charged a different price than others for the same product or service, or why that price was offered. Concerns have also been raised that surveillance pricing may result in discriminatory outcomes or disparate impacts, particularly where algorithms may rely on protected characteristics or are used to exploit a consumer's socioeconomic status or lack of price sensitivity at a given time to extract higher payments from certain consumers.

That being said, many of these concerns remain largely speculative, as regulators, researchers, and other interested parties continue to examine whether and to what extent businesses are actually using surveillance pricing, and if so, to assess the effects of surveillance pricing practices. These debates have also taken on added significance about how in-store technologies could, in theory, enable individualized or dynamic pricing in physical retail environments, potentially extending surveillance pricing beyond online transactions and raising new questions about disclosure, consent, and consumer expectations.

The Current Legal Landscape

The legal landscape governing this practice is rapidly evolving, marked by three distinct but overlapping bodies of state law: (1) state consumer protection laws, applicable to deceptive and unfair trade practices; (2) state consumer data privacy laws that impose obligations on how personal data can be collected and used; and (3) state antitrust laws that target algorithmic coordination among competitors. State consumer protection laws are particularly significant in this context. Although these statutes generally contain a broad prohibition against unfair or deceptive acts or practices, many states also include specific provisions addressing pricing-related conduct. For example, in certain jurisdictions it is unlawful to advertise prices in any manner calculated or tending to mislead or deceive consumers, or to make false or misleading statements of fact, knowingly or with reason to know, regarding the price of a good or service.

In addition to these generally applicable statutes, states have begun proposing legislation that specifically addresses surveillance pricing practices, with New York being the first state to actually adopt a broad algorithmic pricing disclosure law. Under New York's Algorithmic Pricing Disclosure Act, businesses are required to explicitly notify consumers when prices are set using their personal data. Specifically, N.Y. Gen. Bus. Law. § 349-A(2) provides that:

> *Any entity that sets the price of a specific good or service using personalized algorithmic pricing, and that directly or indirectly advertises, promotes, labels, or publishes a statement, display, image, offer, or announcement of such pricing to a consumer in New York using personal data specific to that consumer, must include a clear and conspicuous disclosure stating:* "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA."

As we reported previously, the law faced an early unsuccessful First Amendment challenge from the National Retail Federation. A federal judge rejected the lawsuit, finding that the disclosure requirement in the law was "reasonably related" to a legitimate government interest and not "unduly burdensome." The National Retail Federation appealed the decision to the circuit court of appeals, and the case is currently awaiting review.

Overview of Proposed Legislation

The New York statute marks a significant development in the regulation of surveillance pricing and signals a broader trend toward increased transparency and oversight of algorithmic pricing practices at the state level. This broader trend is evidenced in more than 60 bills currently pending in state

legislatures across over half of U.S. states.

Surveillance pricing and related legislation generally falls along a spectrum from outright prohibitions to disclosure-based requirements.

At one end are bills that broadly prohibit businesses from engaging in surveillance or personalized pricing, often defined as offering individualized prices based on personal data collected through electronic surveillance, automated decision systems, or artificial intelligence. These measures may apply to all businesses or be limited to specific sectors, most commonly grocery and food retail, and frequently include exceptions for cost-justified price differences, uniformly available discounts, opt-in loyalty programs, or regulated industries such as insurance and financial services. Variations of these bills also target dynamic pricing more broadly, restrict the use of specific technologies or data inputs (such as biometric data, device-level signals, or precise geolocation), or focus on essential goods, SNAP- or WIC-eligible foods, or large retail establishments. Enforcement mechanisms include enforcement by state attorneys general and private rights of action.

Other bills take a more transparency-oriented or hybrid approach, permitting certain forms of algorithmic or personalized pricing but requiring clear consumer disclosures, often mandating language such as "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA," and, in some cases, opt-out rights or access to a non-personalized baseline price. These measures may apply broadly to any business advertising personalized prices or be limited to online sellers or entities above a revenue threshold, and violations are commonly treated as unfair or deceptive trade practices under existing consumer protection laws. A subset of proposals also pair pricing restrictions with bans or moratoria on electronic shelf labels, limits on the use of minors' or protected-class data, recordkeeping obligations, or extensions of similar concepts to wage-setting. Across jurisdictions, the bills vary significantly in scope, sectoral focus, permitted exceptions, and enforcement mechanisms, but collectively reflect a growing legislative effort to constrain or regulate the use of consumer data and automation in price determination.

Attorney General Investigations

We're also starting to see AGs take an interest in surveillance pricing issues. In January, California Attorney General Rob Bonta initiated an investigative sweep focused on surveillance pricing practices. According to the Office's press release, Attorney General Bonta sent letters to businesses in the retail, grocery, and hotel sectors with "significant online presence," and that the letters requested information regarding if and how these businesses use consumer data to set prices of goods and services, as well as information on companies' disclosures regarding personalized pricing, pricing experiments, and measures taken to comply with "algorithmic pricing, competition, and civil rights laws." No enforcement actions have been announced yet stemming from this investigative sweep.

Practical Takeaways for Business

As legislative and enforcement activity picks up, businesses can expect renewed scrutiny of their pricing and discount advertising practices, including the potential for investigative subpoenas or civil investigative demands related to how they collect data about consumers and use this data to help set or inform prices, or how they determine to whom to extend discount offers.

For businesses that use, or are contemplating the adoption of surveillance pricing practices, consider the following:

- Understand how prices are set (and not just the technology used),
- Inventory and assess data inputs used in pricing models,
- Evaluate transparency and disclosure practices,
- Consider structure and deployment of discount advertising practices,
- Assess potential consumer protection and discrimination risks, and
- Monitor state and federal legal developments.