States Take Aim at Algorithmic and Surveillance Pricing: Maryland Becomes the Latest Warning Sign for Data-Driven Pricing Practices

May 6, 2026

By: Alfred Brunetti

An increasing number of states are scrutinizing how businesses use personal data, algorithms, pricing software, and related technologies to set or influence consumer prices. Once viewed mainly as a revenue management, e-commerce, or marketing function, data-driven pricing is now attracting attention from an increasing number of privacy, consumer protection, and competition law regulators. Maryland is now the latest state to turn this focus into legislation.

What Happened?

On April 28, 2026, Maryland Governor Wes Moore signed the "Protection From Predatory Pricing Act" into law. The law takes effect on October 1, 2026, and regulates certain uses of personal data by food retailers and third-party food delivery service providers when setting prices.

Although this new law places only on a specific sector of the food industry in scope, businesses outside the grocery or food delivery industries – and outside Maryland – should not ignore it. Maryland's enactment is just the most recent manifestation of a broader domestic legislative trend aimed at practices often described as algorithmic, personalized, predatory, or surveillance pricing.

Other states have recently enacted similar statutes. New York's algorithmic pricing disclosure law requires companies to notify consumers when prices are set by algorithms using personal data. California's antitrust statute has been amended to address certain common pricing algorithms that rely on competitor data or facilitate coordinated pricing.

Viewed collectively, these developments signal an important shift: *regulators are increasingly focused not only on how businesses collect personal data, but also on whether they use that data to shape the terms, opportunities, prices, and commercial experiences offered to individual consumers.*

What Do We Need to Know?

Businesses often use the term "dynamic pricing" to refer to a range of pricing strategies. In some contexts, it simply means adjusting prices based on supply, demand, inventory, timing, market conditions, or other business factors. That type of pricing is not new, but what is new is the increasing regulatory attention to pricing practices that use personal data or algorithmic tools to personalize, influence, or potentially increase prices for specific consumers.

That distinction matters because changing prices due to inventory levels, seasonal demand, or general market conditions does not implicate identifiable consumer-specific data points, which can be processed to determine what price a *particular person* is likely to accept.

Maryland's new law highlights this distinction. It generally prohibits covered food retailers and third-party food delivery service providers from engaging in "dynamic pricing" to set a higher price for food *for a specific consumer*; using personal data (as defined by the Maryland Online Data Privacy Act) to set a higher price for food for a single consumer; or using protected class data to offer, advertise, or sell a good or service in a manner that disadvantages the consumer. In this context, the definition of "dynamic pricing" is narrower than the phrase might otherwise suggest because it targets only individualized pricing practices tied to consumer-specific data, not ordinary or bulk price changes.

Maryland's law is important because of what it prohibits, but it is noteworthy because of what it represents: a growing distaste among lawmakers for business models that use consumer data to personalize prices in ways consumers may not see, understand, or expect.

New York has approached the same broader issue through transparency. Its Algorithmic Pricing Disclosure Act, which took effect on November 10, 2025, requires companies that set prices using an algorithm based on consumers' personal data to display a form disclosure stating: "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA." Taking a slightly different path, California has focused on competition and antitrust concerns. By amending its antitrust act in January, the Golden State now prohibits the use or distribution of "common pricing algorithms" in anticompetitive agreements and creates liability for coercing others to adopt algorithm-recommended prices or commercial terms.

These laws are not identical, but their intentions are clear: a purposeful examination of whether pricing technologies are fair, transparent, non-discriminatory, and consistent with consumer expectations.

What Do We Need to Do?

Given this evolving environment, rather than asking where they do business, companies may be better served by asking "How do we use personal data, algorithms, and consumer-specific signals to influence pricing, offers, fees, and commercial terms?" To gain and utilize such insights, businesses should consider taking the following steps:

1. **Inventory Pricing Tools and Pricing Logic**
   Identify the software, platforms, algorithms, vendor tools, internal models, analytics systems, and business rules used to recommend, personalize, adjust, or set prices. This review should include tools used for dynamic pricing, promotional offers, discounts, delivery fees, subscription pricing, loyalty benefits, and other consumer-facing commercial terms.

2. **Identify the Data Inputs Used to Influence Price**
   Determine whether pricing tools rely on personal data, consumer profiles, purchase history, browsing behavior, geolocation, device identifiers, loyalty program data, app usage data, demographic inferences, protected class data, or other consumer-specific signals.

3. **Distinguish Market-Based Pricing From Consumer-Specific Pricing**
   Businesses should be precise in distinguishing ordinary market-based pricing from individualized pricing. A pricing change based on inventory or general demand may raise different issues than a price increase targeted at a specific consumer based on personal data or inferred willingness to pay.

4. **Review Loyalty, Rewards, Membership, and Promotional Programs**
   Maryland's law contains exceptions for certain loyalty program benefits, promotional offers, temporary discounts, and related practices. But those exceptions should not be assumed without analysis. Businesses should evaluate whether such programs are open to consumers on consistent terms and whether pricing differences are properly tied to the program structure rather than undisclosed, individualized data use.

5. **Evaluate Vendor and Platform Arrangements**
   Many companies rely on third-party pricing vendors, delivery platforms, advertising technologies, analytics providers,

revenue-management tools, or e-commerce platforms. Contracts and diligence processes should be reviewed to understand what data those vendors use, how recommendations are generated, whether competitor data or personal data is involved, and whether pricing outputs are explainable and auditable.

6. **Assess Consumer Notices and Disclosures**
   Companies should review whether their privacy notices, loyalty disclosures, terms of use, and consumer-facing explanations accurately describe how personal data is used in connection with pricing, discounts, offers, personalization, or automated decision-making.

7. **Coordinate Across Legal, Privacy, Marketing, Revenue, Product, and Technology Teams**
   The relevant facts for complex determinations often sit outside the legal department. Pricing practices often involve diverse groups of stakeholders and management teams. As such, a cross-functional review is important because legal significance may turn on technical details that are not apparent from a high-level business description.

8. **Monitor State-by-State Developments**
   Maryland, New York, and California have taken different approaches, and additional states will likely follow with their own efforts or versions. Businesses operating across jurisdictions should avoid the temptation of assuming that compliance with one state's law will satisfy another state's requirements.

Because pricing is now clearly becoming a data governance issue within an already crowded environment where privacy law, consumer protection, antitrust, and algorithmic accountability increasingly overlap, businesses will be best served by knowing not only what prices they charge, but how — and why — those prices are being set.