

**DRAFT**  
**California Retail Association**  
**DRAFT Principles for Artificial Intelligence (AI) Legislation**

Retail AI Landscape

The retail sector is an active user of systems with AI capabilities and tools to support a wide variety of business objectives. Retailers use AI tools to better serve their customers, improve the shopping experience and increase the efficiency of their operations. Retailers use AI capabilities in a variety of ways, including demand forecasting, inventory planning, customer service management, warehouse operations, fraud prevention, streamlining workflow, producing summaries of internal reports and drafting product descriptions and summaries of customer reviews highlighting similar opinions. None of these common retail uses of AI implicates the broader concerns about AI systems impacting criminal justice, education, employment, financial services, essential government services, health care, housing, insurance or legal services.

AI Legislative Principles

The California Retailers Association believes and encourages that AI legislation should be adopted at the federal level rather than a patchwork of bills state by state. AI systems are global in nature and in the long run, a patchwork of AI regulations stemming from conflicting state laws will only create market confusion and chaos, impacting consumers as well as the developers and deployers (users) of AI systems. However, if state-level policy on AI is to be made, it should be narrow in scope and thoughtfully nuanced, with an eye toward promoting consistent regulations across states by adhering to the following principles:

- **Focus on the Developers of AI, Not the Deployers.** The European Union (EU) already adopted comprehensive, well-scoped legislation ([the EU's AI Act](#)) on the development and use of AI that properly places the most significant regulatory requirements on the developers, not the deployers, of AI systems. Similarly, any AI legislation passed in the United States on the state or federal level should follow that model. This is because developers of every type of AI systems are, by virtue of being the creators of those systems, in the best position to address the potential risks of their AI systems at the design and development stages before placing them on the market for other businesses to use. Deployers, on the other hand, are not able to determine or address the potential risks from the use of the systems that are designed by AI developers who can foresee and mitigate these risks in the design and development stage.
- **Follow a Risk-Based Model that Does Not Interfere with the Retail Industry's Current Low-Risk Uses of AI.** AI legislation should follow a risk-based model that narrowly focuses on high-risk AI systems that, when deployed, could unlawfully discriminate against an individual. Accordingly, AI legislation should not impact a retailer's use of AI for innumerable routine, mundane, no-risk or low-risk processes, such as demand forecasting, inventory management and determining the products to place on the shelves for purchase by any customers.
- **Promote Transparency.** Promote transparency when AI is being used in high-risk systems that may potentially have an unlawful discriminatory impact on consumers.

- **Appropriately Define Key Terms Setting the Scope of Applicability.**
  - Any legislation defining “**deployers**” as users of AI systems should be narrowly scoped to include only those deploying high-risk AI systems.
  - An “**intentional and significant modification**” to an AI system should be defined as a modification that was neither planned nor foreseen by the AI developer as a potential use of the system by the deployer who purchases it. A deployer should have the flexibility to tailor an AI system it purchases to fit its own business model without being considered a “developer” under the law for having made any change to it, especially when the opportunity to “tailor” the AI system was designed into the system by the developer. Ensuring these anticipated uses are not captured as an “intentional and substantial modification” of the AI system will avoid a situation where a deployer who uses a system as it was intended risks being considered a “developer” itself under the law and then responsible for the original AI developer’s obligations to comply with the law.
  - Traditionally, the use of the term “**consequential decision**” in AI legislation defines a high-risk system whose outcomes create unlawful discrimination against protected classes of individuals, such as with respect to an individual’s eligibility to obtain education, employment, financial services, essential government services, health care, housing, insurance or legal services. Because the scope of a high-risk AI system turns on the definition of “consequential decision,” it should not unintentionally capture low-risk retail uses of AI as described above, as this would unnecessarily and unreasonably expand what constitutes a high-risk AI system to include tools enabling a score of everyday retail products to be offered for sale to the public by thousands of large and small retailers.
  
- **Implementation and Enforcement of AI Regulatory Framework.** Any state regulatory framework covering the use of AI could impact a wide range of businesses from the smallest to the largest. For this reason, it is imperative the law include appropriate implementation and enforcement provisions like those in nearly all state privacy laws:
  - **2-Year Implementation for Deployers:** Given the compliance costs for even the smallest businesses that may be deemed “deployers,” a minimum 2-year implementation time frame before enforcement of the regulations will be important after a law becomes effective. This will give businesses sufficient time to budget for and acquire the necessary technical, operational and legal experts and resources to develop a compliance plan. This is also consistent with the time frame of the EU’s AI Act for deployers to implement compliance plans considering the wide-reaching regulatory impact on all business that may use AI systems.
  - **State AG Enforcement with 60-Day Notice-and-Cure Period:** As with the first data privacy laws, a prototype AI regulatory framework with new definitions having uncertain applications will necessarily require compliance guidance from the office of the Attorney General. The new law should be exclusively enforced by the AG to ensure that it is applied and interpreted consistently and predictably. Enforcement through private rights of action would lead to disparate and potentially inconsistent interpretations, which would confuse consumers and businesses alike, and threaten the development and deployment of AI systems. The AG is in the best position to drive a consistent and uniform interpretation of a new state-wide regulation. Further, to promote beneficial dialogue between the office of the AG and businesses complying with the AI framework, instituting a 60-day notice-and-cure period similar to state privacy laws would be an effective tool to ensure companies understand how to comply with the new state regulatory framework.