ECOMMERCE INNOVATION ALLIANCE

David Carter, President & CEO
303 W. Broad Street
Richmond, Virginia 23220
david@ecomm-alliance.org
202.240.7890

August 1, 2025

VIA EMAIL
Cari Fais, Acting Director
New Jersey Division of Consumer Affairs
124 Halsey Street
PO Box 45027
Newark, NJ 07101
DCAProposal@dca.lps.state.nj.us

Subject: Comments on Proposed New Jersey Privacy Rules

To the New Jersey Division of Consumer Affairs:

The Ecommerce Innovation Alliance (EIA) is a non-profit trade association dedicated to fostering a predictable and fair legal environment for the ecommerce industry, advocating for common-sense policies that strengthen the ecommerce ecosystem while protecting consumer privacy. We represent a diverse membership, including ecommerce retailers, technology solution providers, and supporting businesses, with a particular focus on small and mid-size businesses that foster job growth in New Jersey and nationwide. Our expertise spans critical areas like data privacy and consumer protection, and we actively educate policymakers on the real-world impact of laws and regulations.

We commend the New Jersey Division of Consumer Affairs' stated intent to protect consumer privacy, which is a shared goal of the ecommerce industry. However, the proposed new privacy regulations, released on June 2nd, 2025, raise significant concerns for ecommerce brands nationwide, particularly smaller businesses operating across state lines. These proposed rules appear to go "significantly beyond" the existing New Jersey Data Privacy Act (NJDPA) and introduce requirements that diverge substantially from other comprehensive state privacy laws, such as the California Consumer Privacy Act (CCPA) and the Colorado Privacy Act (CPA).

Unique Burdens on Smaller Ecommerce Companies Operating Nationwide

As an initial matter, EIA is concerned that the proposed regulations fail to provide clear and meaningful guidance on how a business will know whether it is actually subject to the NJDPA and these proposed regulations. As the Division is aware, the NJDPA only applies to a business doing business in New Jersey or produces products or services targeted to New Jersey residents; and during a calendar year either (a) controls or processes the personal data of at least 100,000 consumers, or (b) controls or processes the personal data of at least 25,000 consumers and makes money from the sale of personal data.

The Division has not explained how a small business can determine if it meets these threshold requirements. For example, the regulations would define “person data” to include telephone numbers, apparently without regard to whether or not the person can be identified with other data in the company’s possession – the regulation only requires that it be linked based on “other data.” Thus, an ecommerce company may possess mobile phone numbers but, because of nationwide number portability and the frequency with which consumers maintain their mobile number despite moving across state lines, have no practical way of determining whether those phone numbers belong to a New Jersey resident. As such, the regulation’s expansive and imprecise definition of “personal data” will have the practical effect of making it impossible for smaller businesses to know whether they are or are not subject to the proposed regulations.

The proposed regulations are likely to impose unique and onerous burdens on smaller ecommerce companies that operate on a nationwide basis for several key reasons:

1. **Broad Extraterritorial Reach:** The rules will apply to any business that conducts business in New Jersey or targets New Jersey residents, if they meet certain thresholds for processing personal data. This broad applicability means that ecommerce businesses located anywhere in the U.S. that interact with New Jersey consumers will be subject to these detailed regulations, regardless of their physical presence in the state. Smaller businesses, by their nature, often lack the dedicated legal and compliance teams necessary to monitor and understand a fragmented and ever-changing landscape of state-specific privacy laws.

2. **Patchwork of Conflicting Regulations:** The proposed rules introduce numerous compliance obligations that appear to conflict with, or substantially expand upon, existing state privacy laws from other jurisdictions. This creates a complex and costly "patchwork" of privacy regulations across different states. For a small ecommerce

company striving for nationwide reach, developing and maintaining separate compliance frameworks for each state is immensely challenging and resource-intensive. This contrasts with the EIA's advocacy for common-sense policies that foster innovation and job growth.

3. **Specific Onerous Compliance Requirements:** The proposed rules introduce several detailed requirements that are particularly burdensome for smaller businesses:

    - **Expanded Data Definitions:** The proposed regulations include an expanded definition of "personal data" and categorize financial information, health data, and biometric data as "sensitive data" requiring heightened consent. Complying with varying definitions and consent requirements for different data types across multiple states significantly complicates data mapping, collection, and processing practices.

    - **Heightened Consent and Dark Patterns:** The proposed rules establish detailed requirements for obtaining consumer consent and explicitly prohibit "dark patterns" or manipulative language/visuals designed to coerce or steer consumer choice. Businesses must "test" their consent and data rights request methods to ensure they are functional and do not undermine consumer choices. While we appreciate the concern regarding dark patterns, the lack of specificity of what constitutes a dark pattern has the potential to lead to increased "shakedown" style litigation against ecommerce companies. For that reason, we would recommend clarifying that only actions that have been previously recognized as dark patterns by the United States Federal Trade Commission or the International Consumer Protection and Enforcement Network's (ICPEN) would be actionable.[1] This change would ensure that businesses have fair notice of what conduct is actionable, rather than potentially allowing recovery for conduct that no governing body has previously recognized to constitute a dark pattern.

    - **Data Minimization and Retention:** The rules require controllers to limit the collection of personal data to what is "reasonably necessary" for disclosed purposes and mandate periodic review of data retention to ensure data is not kept longer than necessary. Differing interpretations of "reasonably necessary"

---

[1] https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy

and varied data retention periods across states create substantial challenges for businesses trying to manage their data lifecycle uniformly and efficiently.

- **Data Protection Assessments (DPAs):** Controllers must conduct and document DPAs for processing activities that present a "heightened risk of harm" to consumers, with requirements for periodic updates. Performing comprehensive DPAs requires specialized expertise and significant resources, which are often beyond the capacity of smaller businesses. The subjectivity in defining "heightened risk" across different state laws further exacerbates this burden.

- **AI Regulations:** The proposed rules introduce new obligations concerning artificial intelligence (AI), including the requirement to assess and mitigate risks related to AI systems that process personal data. For many businesses, the AI that they will leverage are included in platforms that they rely upon to meet their consumers' demands. A requirement requiring every customer to assess these systems imposes undue burden on both the ecommerce retailers and the platforms. Further, given the rapidly evolving and largely unregulated nature of AI nationally, differing state-specific AI regulations could stifle innovation and create substantial compliance hurdles for businesses developing or using AI, particularly for those whose operations rely on it.

- **Loyalty Programs:** Specific rules apply to loyalty programs, requiring notice to consumers about their participation and the benefits tied to data processing. These rules aim to prevent businesses from penalizing consumers for exercising privacy rights, which adds a layer of complexity for managing customer loyalty programs uniformly across different jurisdictions.

- **Children's Data Protection:** The rules include enhanced protections for children under 13, requiring verifiable parental consent for processing sensitive personal data and prohibiting certain uses of such data. Ecommerce businesses serving diverse age groups must implement robust age-gating and consent mechanisms, which adds significant development and compliance costs, especially for smaller entities without dedicated resources.

- **Data Subject Rights Fulfillment:** The rules require controllers to provide consumers with specific rights, including access, correction, deletion, and data portability. Fulfilling these requests in a "portable format" and within specified timeframes, while ensuring proper verification, demands sophisticated technical

and administrative infrastructure that smaller businesses may struggle to afford or implement effectively across all applicable state laws.

The Onerous Burden of Differing Requirements

The burden of complying with these differing and often conflicting requirements becomes particularly onerous for smaller ecommerce businesses due to:

- **Resource Constraints:** Unlike large enterprises with dedicated legal, privacy, and IT departments, small businesses typically lack the financial and human resources to constantly adapt their data processing activities, privacy notices, and technical infrastructure to meet a divergent set of state-specific regulations.

- **Increased Costs:** The cost of legal counsel to interpret complex state-specific nuances, coupled with the expense of developing and maintaining separate technical solutions for each state's unique requirements (e.g., different opt-out mechanisms, consent flows, data retention schedules), can be prohibitive. This detracts from resources that could otherwise be invested in innovation, product development, or job creation.

- **Operational Complexity:** Managing a multitude of privacy compliance frameworks creates immense operational complexity. Training staff, auditing data practices, and responding to consumer requests become exponentially more challenging when each state has its own definitions, rights, and technical specifications for implementation.

- **Disproportionate Impact:** The cumulative effect of these burdens disproportionately impacts smaller ecommerce businesses, making it difficult for them to compete effectively with larger, more resourced companies. This ultimately stifles growth and innovation within the ecommerce sector.

Recommendations

To alleviate these burdens and foster a thriving ecommerce ecosystem while protecting consumer privacy, the Ecommerce Innovation Alliance respectfully offers the following recommendations:

1. **Align with Existing Comprehensive State Laws:** If federal legislation is not immediately feasible, we recommend that New Jersey align its proposed rules more closely with existing comprehensive state privacy laws, such as the CCPA and CPA, wherever possible. Adopting widely accepted best practices and definitions would

significantly reduce the compliance burden for businesses already operating under similar frameworks.

2. **Provide a Sufficient Implementation Period:** Given the significant changes proposed, we urge the Division to provide a substantial implementation period with regard to any rules it may adopt. This extended timeframe would allow businesses, particularly smaller ones, adequate time to understand, prepare for, and implement the necessary operational and technical changes without facing immediate penalties.

3. **Issue Clear Guidance and FAQs:** Provide clear, practical, and well-reasoned guidance, including FAQs, on how businesses can comply with the new rules. This should specifically address common scenarios faced by ecommerce businesses and clarify ambiguities to reduce uncertainty and potential for "shakedown" litigation.

In closing, the Ecommerce Innovation Alliance supports robust consumer privacy protections. However, the proposed rules, in their current form, pose significant challenges to smaller ecommerce businesses operating nationwide, threatening to stifle innovation and growth. We believe that a balanced approach, prioritizing federal harmonization or, at minimum, greater alignment with existing state laws, coupled with practical implementation support, is crucial for achieving both effective consumer protection and a thriving ecommerce industry.

Thank you for your consideration of these comments.

Sincerely,

G. David Carter
President & CEO
Ecommerce Innovation Alliance