U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

September 2, 2025

New Jersey Division of Consumer Affairs
Attn: Office of Consumer Protection
124 Halsey Street
PO Box 45027
Newark, NJ 07101

VIA ELECTRONIC SUBMISSION

Re: Public Comment on the Rule Proposal on Data Privacy, N.J.A.C 13:45L

The U.S. Chamber of Commerce ("Chamber") respectfully submits the following comments in response to the New Jersey Division of Consumer Affair's ("Division") June 2 Notice of Rule Proposal on Data Privacy ("Proposed Rule").[1] The Chamber supports privacy protections for all Americans. We believe the Proposed Rules,[2] however, would harm economic growth and innovation, and will be especially burdensome for small businesses. This is due to overly broad definitions, stringent data processing restrictions, and compliance requirements that fail to align with the Consensus Privacy Approach utilized in many other states.

I. Introduction and Burden on Interstate Commerce

The Chamber is the world's largest business organization, representing businesses of all sizes across the country. We are concerned that the Proposed Rule on Data Privacy imposes an undue burden on interstate commerce. The Chamber's recent report, *Empowering Small Business,* reveals that most small businesses are concerned with having to comply with different state laws on privacy and technology that exposes them to higher compliance and litigation costs[3]. Consistency, uniformity, and workability are critical to ensuring small businesses are not disproportionately harmed by data protection laws.

---

[1] New Jersey Division of Consumer Affairs—Notice of Modified Proposed Rulemaking (June 2, 2025) *available at* https://www.njconsumeraffairs.gov/Proposals/Pages/default.aspx.
[2] New Jersey Division of Consumer Affairs – Proposed Text of Regulations (June 2025) *available at* https://www.njconsumeraffairs.gov/ProposalPDF/ocp-06022025-proposal.pdf.
[3] U.S. Chamber of Commerce, "Empowering Small Business: The Impact of Technology on U.S. Small Business," (August 2025) at 30 *available at* https://www.uschamber.com/assets/documents/20251621-CTEC-Empowering-Small-Business-Report-2025-v1-r10-Digital-FINAL.pdf.

There are better approaches than the Proposed Rule. For example, more than 100 million Americans in states like Texas, Colorado, Indiana, and Virginia enjoy privacy protections under the "Consensus Privacy Approach." This framework gives consumers the right to delete, access, and correct data as well as opt out of targeted advertising, sales, and certain automated profiling.[4] This strikes an appropriate balance between empowering citizens over their privacy while fostering innovation.

We also believe the costs of the Proposed Rules outweigh the benefits for small businesses and shifts New Jersey away from the Consensus Privacy Approach the state opted for in originally passing the New Jersey Data Privacy Act (NJDPA). A lack of harmonization will place New Jersey businesses at a disadvantage while making it more difficult for out of state companies, particularly small businesses, to operate and sell products across state lines.

II. Definitions

A. Biometric Data

The proposed definition of "biometric data" includes any data generated from photos that "relates to" a specific individual, regardless of whether it's used for identification. The draft regulation text as written would meaningfully complicate the consent requirement for processing sensitive data and could potentially prohibit certain generative AI use cases, such as the generating of a photo or a video based on an uploaded image that includes people other than the user. For this reason, we encourage the Division to strike the last sentence in the exclusion provision or revise it to provide clarity that such data is only considered biometric if it is used to identify a "known person."

B. Data Broker

The proposed definition of "data broker" includes entities that merely "collect" or "purchase" data without a direct consumer relationship. This overly encompassing definition would label a vast sum of companies, that collect data but do not sell data, as data brokers. For this reason, we would suggest the Division strike the terms 'collect' and "purchases" from the definition.

C. Essential Goods and Services

[4]Jordan Crenshaw, "What Congress Can Learn from the States on Data Privacy," (January 2024) *available at* https://www.realclearpolicy.com/2024/01/30/what_congress_can_learn_from_the_states_on_data_privacy_1008521.html

The proposed definition of "essential goods and services" includes "any objects, wares, goods, commodities, services, or anything that is consumed or used to preserve, protect, or sustain the life, health, safety, or comfort of persons or their property." This definition is much too broad and could incorporate a variety of services that are not considered essential by other states. We suggest the definition be struck or significantly narrowed to more appropriately scope what is considered an essential good or service.

Such an overly broad definition could also cause consumers to accidentally opt out of automated profiling that they would not have expected. Under the definition of profiling, it is possible a broad interpretation of "essential goods and services" could lead consumers to inadvertently opt out of applications like ride share and grocery delivery which are assigned through software.

An overly broad definition of essential goods and services could effectively render data impact assessments purposeless as effectively the impact assessments could cover all effectively most activity in the digital economy. This would not focus companies on mitigating high-risk harms.

D. Share

Lastly, the Chamber is concerned about the use of the term "share" throughout the Proposed Rule as it is not defined. We suggest the term be defined in the draft regulation text or removed to provide further clarity.

III. Data Processing Restrictions

A. Sale Exception

Most state laws that have adopted the Consensus Privacy Approach exclude disclosures to a third party to provide a service to a consumer within the definition of "sale." The Proposed Rule would disallow this exception if there were a disclosure of personal data to a third party that uses the data for "its own purposes" and consider it a data sale. This may be incompatible with many use cases, and we suggest striking "for its own purposes" from this provision. SB 332 does not specifically provide a prohibition on third parties using data for their own purposes under the sale exception.

B. Internal Research Exception

The internal research exception within Section 1.3(d)(1)(i-ii) in the Proposed Rule goes further than necessary in nullifying the ability to use the exception if "the data or resulting research is shared with a third party, unless it is de-identified" as controllers often share non-de-identified data with third parties for purposes of industry benchmarking and research. This unnecessary limitation will burden research and could prevent the publication of research by requiring contractual obligations for de-identification for all shared research.

Additionally, the loss of the exception in cases when the "data or resulting research is used to train artificial intelligence, unless the consumer has affirmatively consented to such use" goes too far. Losing the ability to leverage the internal research exception in data collection will unfairly disadvantage small business and startups seeking to compete with larger, more resources competitors. Additionally, we believe the AI training requirement defeats the purpose of the exemption and goes beyond the Attorney General's authority. The authorizing statute does not address artificial intelligence. We suggest striking this language entirely.

IV. Strictly Necessary Standard

The inclusion of "strictly necessary" in the requirements related to user interface design, choice architecture, and dark patterns within Section 1.5(a)(9)(ii) is problematic and may be leveraged as a backdoor strict data minimization standard. We suggest this language be replaced with a "reasonably necessary" standard to better align with other states within the Consensus Privacy Approach.

V. Burdensome Compliance Requirements

A. Obligation to Delete User Data in Response to Opt-Out Requests

In Section 3.4(a)(2), the Proposed Rule states that when a consumer exercises their right to opt out, the controller shall "cease processing the consumer's personal data for the opt-out purpose, or purposes, as soon as possible, but no later than 15 days from the date the controller receives the request, and delete any of the consumer's personal data processes for the opt-out purpose, or purposes, after the consumer choice to opt out."

If a consumer has only opted out, there is no need to delete data unless it is requested as a data may be needed for other purposes of importance to a consumer. Requiring controllers to delete data to process opt-out requests is an onerous exercise

that does not provide any additional benefit and may result in an inconvenience for consumers.

B. Notice at Collection Requirement

The Proposed Rule includes a notice at collection requirement. This stipulation found in Section 2.1(e) entails providing consumers, before or at the point of the collection of data, a privacy notice with a comprehensive description of a controller's online and offline information practices and informing consumers about the rights they have regarding their personal data and any information necessary for them to exercise those rights. This requirement is unworkable for businesses without addressing situations where data is collected by a third party and it impossible for the controller to provide direct notice to a consumer. We suggest adopting language that addresses how to provide a notice of collection in instances where a third-party is collecting data on behalf of a controller.

C. Privacy Notice Content Retention Period

The Proposed Rule requires that the privacy notice disclose the "length of time" the controller intends to retain each category of personal data as opposed to allowing for specific criteria to determine retention. This is a complex undertaking that is unfeasible for many businesses. Most state laws allow for the disclosure of criteria for retention instead of specific time frames. We suggest replacing this language.

D. Data Inventory

The Proposed Rule mandates additional documentation requirements including that controllers maintain a data inventory documenting the types of data that the controller possesses, where the data is stored, and who has access to the data. The expected level of granularity of such a data inventory would be extremely burdensome, in particular to small businesses that do not fall outside the scope of the statute and aligns more to a data map as opposed to a data inventory. The Chamber encourages the Division to remove this provision to come into line with other states' approach.

E. Expanded Data Protection Assessments

The Proposed Rule adds significant requirements for data protection assessments that are not required by other states that have adopted the Consensus Privacy Approach. Providing information such as "relevant internal actors and external parties contributing to the data protection assessment, any internal or external audit

conducted in relation to the data protection assessment, including the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process, and when the data protection assessment was reviewed and approved, and the names, positions, and signatures of the individuals responsible for the review and approval" would add unnecessary burden and cost to the compliance process without providing significant consumer benefit

VI. Effective Date

The proposed changes to the existing regulations include some significant additional requirements that will necessitate technology solutions that will take time and resources to develop. We urge you to give businesses at least 12 months to come into compliance with the amendments to the existing regulations.

If you have any questions, please contact Jordan Crenshaw at jcrenshaw@uschamber.com.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce