S.9008-A/A.10008-A, TEDE Part AA

STAFF CONTACT : Chelsea Lemon | Senior Director of Government Affairs | 518.694.4462

BILL **S.9008-A/A.10008-A, TEDE Part AA**
SUBJECT **New York Data Broker Accountability Act**
DATE **March 23, 2026**
OPPOSE

The Business Council opposes the **New York Data Broker Accountability Act** (S.9008-A/A.10008-A, TEDE Part AA) which creates a data broker deletion regime without the comprehensive consumer privacy framework that makes such a tool safe, equitable, and effective. While the proposed language is similar to California's Delete Act, it was layered on top of an existing comprehensive privacy law, which New York does not have. The Business Council believes that New York should enact a comprehensive privacy law first, as 20 other states have, and model it after privacy laws enacted in Colorado, Connecticut, New Jersey and Virginia.

The Business Council does not oppose efforts to require data brokers operating in New York to register with the Department of Financial Services. However, for the below reasons, BCNYS is opposed to efforts to create a data broker deletion regime.

New York Is Skipping the Foundation Every Other State Built First

- 20 states have enacted comprehensive consumer privacy laws before or alongside any data broker registration or deletion mechanism.
- Those laws establish baseline rights (access, correction, deletion, portability, opt-out), identity verification standards, and risk-based exemptions that make a deletion portal operable and safe.
- New York has none of that infrastructure. Part AA attempts to build the roof without the walls.
- California's Delete Act — the model for this bill — was expressly designed to layer on top of the CCPA/CPRA. New York has no equivalent baseline.

The "One-Click Delete Everything" Portal Harms the Consumers It Intends to Help

- A single portal request covers 500+ registered companies with no explanation of consequences or public education awareness. Consumers are

not told they may lose:

- Fraud-prevention signals that protect against identity theft
- Identity verification services used in credit applications
- Motor vehicle recall notifications
- Healthcare payment processing records
- Business credit data essential for small business access to capital

- This is a blunt instrument, not a meaningful consumer choice. A one-click deletion option may seem straightforward, but without clear explanations of what deletion truly means, consumers are left in the dark about the real-world consequences of removing or suppressing data that supports fraud prevention, identity verification, eligibility determinations, and service continuity. The bill should require plain-language disclosures alongside any deletion mechanism and offer more granular choices so consumers can act with full understanding.
  - For instance, a consumer may wish to erase data used for certain purposes while still allowing data brokers to retain information used exclusively for fraud prevention and identity theft protection.

The Bill Creates Serious Fraud and Impersonation Risks

- No standards exist to verify that a deletion request comes from the actual consumer rather than a bad actor.
- Anyone can claim to be an "authorized agent" — the bill provides no credentialing or verification requirements for authorized agents.
- Unauthorized deletions could suppress the identity signals that detect ongoing fraud, prolonging harm to victims.
- If a request cannot be verified, it converts to a blanket opt-out — a single "Mary Williams" request could trigger opt-outs for every Mary Williams in New York.
- Household-level deletions could remove data for people who never requested deletion.

The 'Data Broker' Definition Is Both Overbroad and Under-Inclusive

- The definition sweeps in fraud prevention, identity verification, data hygiene, analytics, and business credit services — entities that provide distinct, risk-mitigating benefits to consumers.
- There is no service provider/processor exemption. While it does not appear to be the intent of the legislation, cloud providers, payment processors, and adtech platforms acting purely under client instruction/contractual obligations could be captured as data brokers. The definition should be amended to include:

- §1800 (11)(b)***(vi) an entity to the extent that the entity is acting as a service provider.***
- The definition relies on consumer "intent and expectations" — a subjective, unverifiable standard that cannot be applied consistently at scale.

"Consumer" Definition Should Exclude Individuals Operating in Employment or Commercial Contexts

- To align with the consensus definition of "sale" in other states privacy laws, the definition must be amended to read:
  - "Consumer" means a natural person who is an individual who is in New York state for other than a temporary or transitory purpose, and every individual who is domiciled in New York state who is outside the state for a temporary or transitory purpose. ***Consumer does not include a natural person acting in a commercial or employment context.***

The Bill's Definition of Sell/Sale is Not In Alignment With Other States' Privacy Laws

- To align with the consensus definition of "sale" in other states privacy laws, the definition must be amended to read:
  - 34(a). "Sell", "selling", "sale", or "sold" means ***the exchange of*** **[**selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means,**]** a consumer's personal information by a business to a third party for monetary **[**or other valuable**]** consideration.
- Without this amendment, the reference to "other valuable consideration" will introduce confusion as it has no common meaning and could be interpreted to mean nearly any benefit of any kind. This could inadvertently scope in entities as "data brokers" that merely share data with each other as part of everyday, routine business-to-business interactions.

The Bill Lacks an Opportunity to Cure & Uncertain Costs

- Legislation lacks any cure period before enforcement actions. We recommend inserting a 30-day right to cure to allow data brokers to correct an oversight or issue before facing enforcement action and suggest the following new language:
  - ***Prior to initiating any action for violation of this Act, the Superintendent of Financial Services shall provide a business thirty (30) days' written notice identifying the specific provisions of this Act the Superintendent of Financial Services alleges have been or are being violated. If within the thirty (30) days the controller or processor cures the noticed violation and provides the Superintendent of Financial***

Services an express written statement that the alleged violations have been cured and that no further violations shall occur, no action for damages under subsection (3) of this section shall be initiated against the business.

- Additionally, this bill would charge registrants an undefined pro rata share of the operating costs associated with administering the obligations of the bill. This creates significant uncertainty for businesses and could result in unreasonably high registration fees. Any fee assessment should be limited to the reasonable, documented cost of operating the registry and deletion mechanism, with a transparent allocation methodology and an opportunity to challenge erroneous assessments. The fee provisions should be amended to specify an amount that will be charged. The following amendment is suggested:
  - In registering with the office, a data broker shall do all of the following: (a) pay the ***registration fee*** **[**pro rata share assessed by the office**]**;

For these reasons, The Business Council is opposed to S.9008-A/A.10008-A TEDE Part AA and respectfully requests it be rejected in the FY2026-27 Final Executive Budget. Rather than proposing multiple different pieces of legislation that only target portions of consumer data rights and institute significant and costly compliance burdens on businesses, we must engage in meaningful conversation amongst stakeholders in New York on adopting an interoperable comprehensive consumer data privacy law.