February 25, 2025

Chair Liz Krueger
Senate Finance Committee
Chair J. Larry Pretlow
Assembly Ways and Means Committee
New York State Legislature
Legislative Office Building
Albany, NY 12248

Re: FY 2027 Joint Legislative Budget Hearing — Economic Development, Part AA (Regulation of Data Brokers) — *SUPPORT WITH AMENDMENTS*

Dear Chairs Krueger and Pretlow,

Consumer Reports writes to support Part AA of the FY 2027 Economic Development Budget proposal, which seeks to enable consumers to request the deletion of their personal information from all of the state's registered data brokers' records in a single action. Part AA would also require data brokers to report what information they collect on consumers and would impose civil penalties and fines on data brokers who fail to comply with the registration or deletion requirements. Part AA will provide a straightforward, powerful, and critically important tool for protecting the privacy and security of New Yorkers' personal information.

Data brokerage is a multi-billion-dollar industry centered on collecting and selling people's personal data, typically without their knowledge or explicit consent. It poses a host of significant risks to New York residents. Data brokers amass personal dossiers on virtually every American that include thousands of data points, including extremely granular information about people's behavior online and offline, religious practices and beliefs, physical and mental health conditions, finances, political affiliations, precise geolocation derived from cellphones and connected devices, as well as their inferences about individuals based on this existing data.[1] Some data brokers even collect and sell

[1] See, e.g., Joseph Cox, The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15, 404 Media (Aug. 22, 2023), https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/;
Douglas MacMillan, Data Brokers are Selling Your Secrets. How States are Trying to Stop Them, Wash. Post (Jun. 24, 2019). https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-yoursecrets-how-states-are-trying-stop-them/.

information about children. This information is then sold and resold, often for marketing but for a variety of other purposes as well, eroding consumers' basic expectation of privacy in the process.[2]

A few examples of data broker-driven harms include:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use data brokers to target vulnerable individuals for scams, or otherwise use personal information to cause harm. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It," "Retiring on Empty: Single," and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products.[3] Data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.[4]

- *Predatory use of consumer data.* Data brokers sell data about people who rarely even know the companies even exist—and who have rarely ever affirmatively, expressly consented to this data collection and sale. In some instances, this can result in financially disastrous consequences for consumers. A recent case brought by the Texas Attorney General alleged that Arity, a data broker owned by the insurance company Allstate, secretly harvested information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.[5] They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

- *Enhanced risks of data breaches.* Data brokers collect trillions of data points on Americans, so they are unsurprisingly a top target for hackers and cyber criminals. Recently, National Public Data, a data broker that specializes in online background checks and fraud prevention services, saw its own data breached, compromising the privacy and security of 2.9 billion consumers whose personal information they trade in, with particular concern for the 170 million individuals across the US, UK and Canada whose sensitive information,

---

[2] Big Data, A Big Disappointment for Scoring Consumer Credit Risk, Nat'l Consumer Law Ctr. at 15-16 (Mar. 2014), https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

[3] Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule; request for public comment, (December 3, 2024), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

[4] Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs

[5] Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

including social security number, was exposed.[6] And location data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones every day,[7] reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.[8] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[9]

Part AA will make it simple for consumers who do not want their information collected, sold, or retained by data brokers to express this preference. First, the bill will require data brokers to register with the Department of Financial Services, pay a nominal registration fee, and share basic information about what types of personal information they collect and sell. Then, the Department of Financial Services is required to create a website providing access to a "universal deletion mechanism" that allows consumers, via single request, to delete their personal information from *every* data broker that has collected it.

This ability to take control of your data with a single click is critical; there are hundreds of data brokers—virtually all unknown to consumers—making the task of deleting one's information from each broker on a one-by-one basis daunting, if not impossible. Previous Consumer Reports (CR) testing has shown that when privacy laws lack universal ways to manage privacy choices, consumers struggle to use them. For example, in researching the effectiveness of California's privacy law, CR found examples of data brokers utilizing onerous opt-out requirements that prevented consumers from stopping the sale of their information.[10] For 42.5% of sites tested, at least one of three testers could not even find the broker's do not sell link.[11] About 46% of the time, consumers were left waiting or unsure about the status of their do not sell request, and 52% of the time, the tester was "somewhat dissatisfied" or "very dissatisfied" with the opt-out process.[12]

Based on registration patterns in states with similar laws, New York's data broker registry will likely include at least 200 registrations, with the potential for 500 or more, similar to California's

---

[6] National Public Data breach: What you need to know, (January 31, 2025), https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535

[7] Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf

[8] Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/

[9] Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S.Military Personnel, (November 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf

[10] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Rights Protected, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf

[11] *Id.*

[12] *Id.*

experience.[13] A consumer attempting to exercise deletion rights individually would face extreme burdens searching for registered data brokers, navigating complex websites and privacy policies, and managing follow-up communications.[14] During this lengthy process, data brokers continue to buy and sell the consumer's personal information—potentially even to brokers that previously complied with a deletion request. Today, this is an impossible, Sisyphean challenge for New York consumers; but that changes with Part AA.

That said, there are several provisions in Part AA that should be rewritten to enhance clarity or to strengthen consumer protections. The text of Part AA appears to largely pull from California's Delete Act, legislation that first passed in 2023 and was updated in 2025. Notably, the California Delete Act was drafted as an amendment to the CCPA, and therefore uses CCPA's underlying definitions and exemptions. While this approach works in the California context for the most part, New York does not currently have an underlying consumer privacy law, which makes the process of replicating the California Delete Act word-for-word unwieldy in a few different ways.

We therefore suggest the following amendments. We have compiled a more detailed redline that implements these and other changes, but by way of example:

- *Remove exemptions from Section 1804(4) that do not apply to data brokers and simplify terminology.* Several of the exemptions currently provided in the legislation do not map onto data broker activities and therefore create unnecessary ambiguities that could be exploited as loopholes. For instance, Section 1804(4)(a)(i) provides that data brokers shall not be required to complete a deletion request if the personal data is reasonably necessary to "complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer…" By definition, data brokers are those that collect and sell to third parties the personal information of consumers with which they have no direct relationship. Therefore, data brokers would not be collecting personal data to fulfill warranties, issue product recalls, or providing goods or services requested by consumers. This is a CCPA exemption primarily meant to apply to covered first-party businesses and not data brokers. It should be stricken. The same principle applies for Section 1804(4)(a)(iii) and Section 1804(4)(a)(vi).

  Relatedly, many of the exemptions in Section 1804(4) don't actually refer to data brokers, but instead to "businesses" (a separate CCPA concept) which creates ambiguity. And more generally, this bill unnecessarily employs several CCPA concepts, such as "service providers," "contractors," and "business purposes" that have all been blurred together in confusing ways. The proposal should be simplified to ensure that obligations and exemptions only accrue to the appropriate stakeholders.

---

[13] Privacy Rights Clearinghouse, Registered Data Brokers (as of November 2024), (December 12, 2024), https://public.tableau.com/app/profile/privacy.rights.clearinghouse/viz/RegisteredDataBrokers2024_17340798229480/DataBrokerDatabaseShowingMissing

[14] McDonald, Aleecia M. and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies." (2009). https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

- *Reduce the overall number of exemptions.* Apart from our technical recommendations regarding exemptions described above, we also recommend reducing the overall number of exemptions on consumer protection grounds. Data brokers are incentivized to avail themselves of any possible exemption and to adopt expansive interpretations of exemptions; after all, their business model depends on retaining as much consumer data as possible. As such, the bill's exemptions should be narrowly tailored and should only exclude activities clearly in the public interest or otherwise protected by existing law. For example, it is reasonable for the bill to create narrow exemptions for data brokers solely acting as processors or carrying out legal obligations on behalf of other businesses, or to facilitate fraud prevention or Know Your Customer-type requirements for others. Any exemptions should be paired with strict purpose limitation language that clarifies that exempted data should be separated or segregated from data used for any other purpose, deleted immediately upon the expiration of the legal or contractual requirement, and only be used for purposes directly related to such exceptions and shall not be used or disclosed for any other purpose.

  In particular, the drafters should narrow the bill's blanket Fair Credit Reporting Act (FCRA) and remove the Gramm-Leach-Bliley Act (GLBA) exemption entirely. Many data brokers are hybrid entities, sometimes acting as credit reporting agencies under the FCRA and sometimes acting as marketing data brokers. While it is reasonable for the law to exclude personal information that is actually being used to furnish a credit report under FCRA, when a hybrid entity receives a deletion request, they should be responsible for deleting their marketing data about consumers. The existing text would exempt such entities wholesale, leaving much consumer data unprotected. Likewise, if financial institutions collect and sell information about non-customers without their awareness, they are engaging in the practice of data brokerage and should be regulated as such. By definition, data collected *directly* from consumers by financial institutions is not within the scope of this legislation and therefore a blanket carveout is unnecessary.

- *Clarify References to privacy rights that do not exist under current New York law.* The proposal currently references certain rights that New Yorkers don't actually have due to the lack of an underlying comprehensive privacy law. For example, Section 1804(3)(b) references the right to have deletion requests treated as an opt-out request if the deletion request cannot be verified. Such a right to opt-out should either be defined, or the proposal should provide an alternate remedy when consumer deletion requests are denied.

Assuming these issues are addressed, this bill's approach will massively reduce friction for New Yorkers seeking to take back control over their personal information. For the above reasons, we are proud to support Part AA and urge the Legislature to approve it.

Sincerely,

Matt Schwartz
Senior Policy Analyst
Consumer Reports