October 14, 2025

NY Asm. Standing Committees on Consumer Affairs & Protection and on Science & Technology
Hearing Room C
Legislative Office Building
Albany, NY 12210

RE: "Data Privacy and Consumer Protections"

Dear Chairs Rozic and Otis, and Members of the Assembly Standing Committee on Consumer Affairs and Protection and Assembly Standing Committee on Science and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I am pleased to respond to the Consumer Affairs and Science and Technology Committees' notice of public hearing on data privacy and consumer protections. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the provision of digital services therefore can have a significant impact on CCIA members.

CCIA supports comprehensive privacy legislation that ensures that consumers' personal information is handled responsibly no matter where it is collected or who is processing it. This framework should set consistent transparency requirements, consumer controls, and accountability measures for data controllers. Such a framework should be risk-focused, technology-neutral, and provide safe harbors and flexibility for organizations to make adjustments according to individuals' needs and evolving technology.

Developing comprehensive and durable privacy legislation requires balance. Such legislation should encourage innovation and unlock the incredible social value of data without infringing on related rights such as freedom of speech. Overly prescriptive or onerous regulation risks creating high barriers to entry for new companies and may even prohibit the creation of beneficial new technologies and privacy protection techniques and services. To achieve these objectives, CCIA recommends the following:

I. Roles and Responsibilities

A comprehensive privacy framework should define separate roles and responsibilities for data controllers (who determine the manner and purpose of data processing) and data processors (who process data on controllers' behalf). Controllers and processors should jointly decide on the technical means of collecting data. However, because controllers determine the purpose of data processing, they should carry all responsibilities for fulfilling direct obligations to data subjects, such as rights to access, correct, and delete data.

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

II. Personal Information, Transparency, and Consumer Rights

A comprehensive privacy framework should limit its regulations to consumers' personal data, rather than all data. Furthermore, such a framework should specifically exclude individuals acting in a commercial or employee capacity. Employee privacy and commercial privacy can be jeopardized in different ways than consumer privacy, and should therefore be regulated separately.

The framework should define categories of "sensitive data" that receive heightened protections such as requiring data protection assessments for controllers or revocable consent to process a subject's sensitive information. Such categories should include "consumer health data," i.e. data that a controller uses to identify health conditions (excluding data processed by entities covered under the Health Insurance Portability and Accountability Act (HIPAA)). To facilitate compliance, controllers should not have separate obligations for particular health conditions. "Sensitive data" should also include precise geolocation data, defined as location data derived from technology that identifies a consumer's specific location to within 1750 feet.[2] It should also include biometric data, defined as automated measurements of an individual's biological characteristics that are used to identify a specific individual, except for "a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA" (the standard formulation in state privacy laws).

Sensitive data should also include data collected from individuals *actually known* to be children, i.e. under 13 years of age. The actual knowledge portion of this standard is essential, as it is also already well-defined under existing federal law and allows companies to maintain privacy and security safeguards to protect data and to curate content aimed towards targeted demographics.

Other potential protections for minors' privacy could be obtained by extending the following protections to all consumers:

- Data access, deletion, and correction rights;
- Data minimization requirements for minors' data, including reasonable data collection and retention limits;
- Transparency and consent requirements when collecting precise geolocation information from known children;
- Requiring services targeted at minors to conduct privacy and safety risk assessments; and
- Providing privacy and safety notices that are phrased in a manner appropriate to the age of the business's target audience.

Age-appropriate design code ("AADC") measures should not be included. Such laws set dangerous precedents by regulating content that is ambiguously "harmful to minors," without providing guidelines or clarifications on how companies can comply or regulators should apply this standard to individual cases. Regulators of differing political and social views will likely apply this standard differently. Additionally, such laws encompass products and services used

[2] This standard is used in many state laws. *See, e.g.*, *An Omnibus Definition of "Sensitive Data" Across Comprehensive State Privacy Laws*, Future of Privacy Forum (last updated Feb. 27, 2024), https://cdn.sanity.io/files/3tzzh18d/production/eac1440d340a728f1f2c00ab6c27aff446bce67d.pdf.

by adults as well as children, thus undermining freedom of expression for all users. As the Supreme Court has long held, "Speech that is neither obscene as to youths nor subject to some other legitimate proscription cannot be suppressed solely to protect the young from ideas or images that a legislative body thinks unsuitable for them."[3] In California, for instance, a federal judge recently issued a preliminary injunction against the first state age-appropriate design code law, finding the law to be "content-based on its face"[4] and to "likely fail strict scrutiny."[5]

Importantly, New York should not enact restrictions that inhibit quality of service for consumers. Such restrictions include prohibiting the sharing of sensitive data with service providers or requiring strict limitations on algorithmic decisionmaking. Such limitations would make many digital services unworkable, including key services like online healthcare providers. The aforementioned opt-out, access, correction, and deletion rights protect consumers' data from being misused in such cases, while still allowing websites to function effectively.

While privacy laws should promote transparency, they should not be unduly complex — businesses of all sizes should be able to comply with transparency requirements. New York should require a single clear and accessible privacy notice to avoid consumer confusion and barriers to innovation. Such a notice should require controllers to disclose the following:

- Categories of personal data collected;
- Purposes for which the data will be used;
- Categories of data shared with third parties;
- Categories of third parties with whom data is shared; and
- How consumers may exercise their rights as data subjects.

Such a law should also set standards for data minimization. State data minimization standards typically follow one of two models, limiting data collection and processing to what is reasonably necessary to either (1) achieve a purpose the business discloses to the consumer, or (2) provide a specific product or service. CCIA recommends the first approach, as it is easier to evaluate whether a business has disclosed its purpose to consumers than whether it is technically feasible to provide a product or service without collecting certain data. The latter approach would require expensive technical expertise to evaluate, and most businesses would not know in advance whether they are complying with the law.

New York should avoid the American Privacy Rights Act (APRA) approach of limiting data collection and processing to specific purposes and prohibiting data collection beyond what is "reasonably necessary and proportionate" (or "strictly necessary" for sensitive data). These overly restrictive formulations would effectively prohibit businesses from acquiring third-party data, which would greatly stifle innovation.

III. Existing Privacy Frameworks & Protections

New York should avoid regulations that restrict cross-border data flows or promote data localization under the guise of protecting privacy, as such rules harm consumer welfare,

[3] *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 213-14 (1975).
[4] *NetChoice v. Bonta*, 770 F. Supp. 3d 1164, 1186 (N.D. Cal. 2025).
[5] *Id.* at 1193.

cybersecurity, and the digital economy. In addition, internet-based services are inherently, and almost universally, interstate concerns which fall within the federal government's purview.

High-quality legislation in other states should also serve as a model for New York privacy law. The Virginia Consumer Data Protection Act is a useful guide in several key areas: It allows consumers to access, correct, and delete data, and requires clear opt-outs in specified cases where the processing carries heightened risk of harm. Similarly, it allows consumers to opt out of targeted advertising based on third-party data but not first-party data (i.e. businesses can still use data they collect to build models and personalize recommendations to their own customers).

The latter distinction is critical: targeted advertising lowers consumer costs by allowing businesses to sell products more efficiently (particularly smaller businesses), and allows platforms connecting billions of people to operate without charging users. Additionally, growing a business requires leveraging first-party data collected from consumers to better evaluate their needs and reach new customers. Such advertising also benefits consumers by allowing them to more easily find the products and services they need.

Additionally, as noted above, privacy frameworks should give companies flexibility to implement safe and secure features based on the target audience's age. There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to small business sustainability.[6] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains more information regarding guiding principles for age assurance and how digital services have used such principles to develop best practices.[7] The report found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification methods, and that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[8] Such laws undermine privacy by forcing businesses to collect more sensitive information from both minors and adults.

IV. Data Security

New York should allow businesses to implement effective security measures without being constrained by rigid requirements. Instead, regulations should adapt to new threats and new technology, allowing businesses to implement the best security practices to guard against the specific threats they face. Accordingly, regulations should align with existing standards, such as those set forth by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). This will help businesses leverage the best existing security measures while avoiding duplicative compliance requirements that undermine efficiency. Such requirements should be general rather than prescriptive, requiring that businesses' security controls be reasonable and appropriate to the type, amount, and sensitivity of the information they process. This approach aligns with most existing laws and

[6] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[7] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[8] *Id.* at 10.

gives businesses the needed flexibility to combat security risks specific to their operations. Prescriptive requirements to institute specific security measures, by contrast, risk becoming obsolete as cyber threats evolve, imposing compliance burdens without enhancing security.

Security regulations should avoid forcing businesses to undermine encryption. There is broad consensus among security professionals that undermining encryption creates unnecessary risks, compromises potentially sensitive data, and opens systems to vulnerabilities. Despite potentially aiding law enforcement in addressing criminal activity, mechanisms that enable law enforcement access to encrypted data simultaneously grant access to malicious actors and creates additional complexity in network security system infrastructure. In 2013, former NSA director of research Fred Chang testified that "When it comes to security, complexity is not your friend.... as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries."[9] More recently, following the Salt Typhoon attack in 2024, FBI and Cybersecurity and Infrastructure Security Agency (CISA) officials cautioned Americans against sending text messages through unencrypted apps, noting the potential exposure to hackers.[10] Thus, businesses must be allowed to prioritize strengthening encryption and data security practices to effectively protect Americans' data.[11]

V. Accountability & Enforcement

Vesting authority solely in regulators with particular expertise in the data at issue gives the best chance of uniform interpretation, application, and enforcement of the statute. Enforcement authorities should engage with organizations that create best practices and frameworks for their members and stakeholders to follow, such as DTSP and NIST. Enforcement authority should be vested with a single regulatory agency to avoid legal uncertainty and conflicting requirements for businesses.

A comprehensive privacy framework should avoid broad private rights of action that contravene existing court precedents. Indeed, recent opinions express skepticism with legislative grants of broad statutory damages without clear showings of injury and actual damages.[12] Lawsuits prove extremely costly and time-intensive, with the costs often being passed on to individual consumers. Such a measure would disproportionately impact smaller businesses and startups. Furthermore, every state that has established a comprehensive consumer data privacy law — 19 states and counting — has enforced these laws through their state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority and allows public interest to determine which enforcement actions are brought.

Safe harbor provisions are important for fair and effective enforcement. Safe harbors (1) provide valuable predictability to both market actors and consumers, (2) enable speedier

[9] *Is Your Data on the Healthcare.gov Website Secure? Hearing before the H. Comm. on Science, Space and Technology*, 113th Cong. 2-3 (2013) (statement of Fred Chang, Chair in Cybersecurity, SMU).
[10] *See also Mobile Communications Best Practice Guidance*, CISA (Dec. 18, 2024), https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf (similarly cautioning consumers).
[11] *See also* Jesse Lieberfeld, *Why Encryption Matters*, Disruptive Competition Project (Feb. 20, 2025), https://project-disco.org/privacy/why-encryption-matters/.
[12] *See, e.g.*, *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021) (holding that plaintiffs suing for damages for misuse of credit report data under FCRA did not meet constitutional standing requirements without showing injury in fact).

compliance, and (3) deter vexatious, meritless litigation if in fact parties other than the state are authorized to enforce the statute. When a state agency alleges noncompliance with a privacy or security obligation, businesses should therefore be allowed to use compliance with an established privacy framework like NIST and ISO as an affirmative defense against such allegations. Businesses should also receive advance notice of complaints and have the opportunity to cure violations before enforcement actions are brought, both to minimize costly enforcement actions and focus agency resources on large-scale and repeat offenders.

* * * * *

We appreciate the Committees' consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association