Assembly Standing Committee on Consumer Affairs and Protection
Assembly Standing Committee on Science and Technology

October 14, 2025 Joint Public Hearing

SUBJECT: Data privacy and consumer protections

PURPOSE: To examine potential solutions for ensuring the protection and privacy of consumer data.

With ever-evolving and widespread use of technology, the volume of consumer and nonconsumer personal data being collected has grown significantly. Many digital platforms actively collect, share, and sell this data—often without the informed consent of individuals. While some companies have taken steps to update their privacy policies and practices, these efforts remain inconsistent, inadequate, and voluntary. New York State has made progress in safeguarding children's information through the passage of the New York Child Data Protection Act in 2024, which restricts the collection, processing, disclosure, and sharing of minors' data. However, these protections only apply to children and leave the broader population, including vulnerable communities, without necessary safeguards. The purpose of this hearing is to gather input from a broad range of stakeholders to explore potential solutions to safeguard consumer and personal data while enhancing transparency. The Assembly Standing Committee on Consumer Affairs and Protection, as well as the Assembly Standing Committee on Science and Technology, are particularly interested in examining approaches that create robust consumer and individual protections while also addressing the realities of data collection and use. The Committees welcome testimony on strategies and insights that can contribute to the development of a coherent and effective data privacy framework that protects the rights of New Yorkers in the digital age.

Submitted Testimonies (organized by panel order)

Panel 1: Chris D'Angelo, Chief Deputy Attorney General for Economic Justice, NYS Office of the Attorney General; Karuna Patel, Senior Counsel for the Economic Justice Division, NYS Office of the Attorney General

Panel 2: Alex Spyropoulos, Director of Government Relations, Tech: NYC; Chris Gilrein, Executive Director of the Northeast, TechNet; Kate Goodloe, Managing Director, The Business Software Alliance (virtual)

Panel 3: Justin Harrison, Senior Policy Counsel, New York Civil Liberties Union; Matt Schwartz, Policy Analyst, Consumer Reports

Panel 4: Siwei Lyu, Professor, University at Buffalo Department of Computer Science; Helen Nissenbaum, Professor, Cornell Tech (virtual); Pavan Kochar, CEO and Co-Founder, Centree; Dawn Kelly, Founder and CEO, Nourish Spot

Panel 5: Chelsea Lemon, Senior Director of Government Affairs, The Business Council of New York State (BCNYS); Brianna January, Director of State and Local Government Relations, Chamber of Progress; Chris Grimm, Policy Advisor, Connected Commerce Council

Panel 6: Andrew Kingman, President of Mariner Strategies LLC, State Privacy and Security Coalition; Steve Wimmer, Senior Technical and Policy Advisor, Transparency Coalition

Panel 7: Alicia Abramson, Civil Rights Intern, Surveillance Technology Oversight Project, (STOP); Hayley Tsukayama, Associate Director of Legislative Activism, Electronic Frontier Foundation (EFF) (virtual); Eric Null, Co-Director of Privacy and Data Program, Center for Democracy & Technology (virtual)

Panel 8: Diane Kennedy, President, NY News Publishers Association & Advertisers Services; Jeremy Newman, VP of Legislative and Regulatory Affairs, NY Credit Union Association; Niall O'Hegarty, General Counsel, NY Bankers Association

Testimony of the Office of the

New York State Attorney General Letitia James

Submitted to the New York State Assembly

Standing Committee on Consumer Affairs & Protection

Chair: Assembly Member Nily Rozic

&

Standing Committee on Science & Technology

Chair: Assembly Member Steven Otis

Joint Public Hearing: Data Privacy and Consumer Protections

Tuesday, October 14th at 10:00 a.m.

Purpose: To examine potential solutions for ensuring the protection and privacy of consumer data.

Good morning Chair Rozic and Chair Otis and esteemed committee members. My name is Christopher D'Angelo, and I am the Chief Deputy Attorney General for Economic Justice at the New York State Attorney General's Office. I am joined by my colleague, Karuna Patel, Senior Counsel for Economic Justice. We oversee the Economic Justice Division, including the Bureau of Internet and Technology, which enforces New York's privacy and data security laws. Thank you for the opportunity to provide testimony to explore potential solutions to safeguard New Yorkers' personal data, and to enhance transparency. We commend the Committees' commitment to balancing New Yorkers' rights to autonomy, privacy, and data security with digital innovation. Without appropriate guardrails, such innovation can be as dangerous as it can be beneficial and the Committees' recognition of the same brings us together today. The current digital world was unfortunately built without a number of necessary guardrails. Much of this world relies on the collection, use, sale, and manipulation of troves of consumer data that is picked apart, put back together, mined, and otherwise processed without the consent—or even awareness—of the average individual. Not only must we re-claim our rights to privacy, autonomy, and data security, now is the time to enact guardrails to ensure that future innovation appropriately accounts for those bedrock principles.

The successful enactment of the Stop Addictive Feeds Exploitation (SAFE) for Kids Act of 2024 and the Child Data Protection Act (CDPA) of 2024 reflect this Legislature's resolve to wrestle control of young people's data, time, and attention back to where it belongs—in the

hands of New Yorkers. Young New Yorkers increasingly suffer the negative mental health consequences of existing attention-grabbing technology and are being used as test subjects for technology like AI companions without regard for the risks and consequences. The SAFE for Kids Act is a first of its kind intervention returning the choice of whether young people's data is used for targeted advertising and algorithmic personalization to young people and parents. On September 15, after careful deliberation and stakeholder engagement, we published the notice of proposed rulemaking to implement the groundbreaking protections provided by the SAFE for Kids Act. The public comment period remains open until December 1 and we welcome all members of the public to submit comments.

The recent passage of CDPA is another important development, restricting the collection, processing, disclosure, and sharing of minors' data. The law prohibits processing of teen data for any purpose, including targeted advertising, that's not strictly necessary for the service being accessed by the user unless they provide informed consent. The law also includes strict deletion rules. The CDPA is a huge step forward for data protection and in many ways provides a blueprint for extending digital privacy protections for all New Yorkers.

The Science and Technology Committee also recently shepherded the passage of the Health Information Privacy Act or "New York HIPA." If enacted, New York HIPA would prohibit any processing of regulated health information unless that processing is strictly necessary, or the regulated entity gets informed consent. Consent in this context must be requested from consumers separately from any other transaction. This law, which we commend the Legislature for passing and urge the Governor to sign into law, is a huge step forward in protecting health information privacy in New York.

As the Committees recognize, New York is significantly trailing other states in enacting vital, more general, consumer privacy legislation. Twenty states have adopted comprehensive consumer privacy frameworks. The interest and commitment of the members of these Committees to provide New Yorkers this critical protection is timely and necessary. With New York's CDPA and New York HIPA laying the groundwork for a new, more comprehensive framework to protect all New Yorkers, we take this opportunity to highlight both the need for as well as what we view as important components of effective pr.

The Problem: A Pervasive Surveillance Economy and Societal Harm

While it has not always been easy to point to tangible or immediately visible harms resulting from the invasion of data privacy experienced by many users in today's digital economy, every individual participating in the digital world is now confronted with real and serious harms. They include:

1. Weaponization and targeting: Data about a user collected online can and has been weaponized for personal or political targeting. It is now a frightening reality that geolocation data, web-browsing, and applications women use to track menstrual cycles or fertility can be used to target women considering or exercising their right to receive abortion care.

2. Erosion of privacy: Consumers are often forced to surrender their information to simply participate in the public forum the internet is today, eliminating meaningful choice. Even where consent is requested, it can often feel coercive. This essential loss of privacy every time we use a device connected to the internet cannot be overstated.

3. Erosion of autonomy: In the current landscape of few and limited restrictions, data sharing is used to fuel "engagement features," which hyper-personalize online experiences to manipulate individuals and to maximize their engagement. These features often override an individual's autonomy and ability to freely enjoy but also step away from the digital

experience. It is no surprise that we commonly hear terms like screen addiction, brain rot, and compulsive use, to describe the resulting effects. Studies correlate these features with reduced productive economic and social activity and increased adverse mental health outcomes. The SAFE for Kids Act protects young people from some of the dangers of hyper-personalized online experiences. Strong privacy protections are complimentary and could help bring similar benefits to all New Yorkers.

4. Orchestrated polarization: Hyper-personalization is also radicalizing and dividing people. Personalized data is used not only to present people with widely divergent representations of the world, it also normalizes extreme and fringe viewpoints that prey on and exacerbate people's personal biases.

5. Increased risk of discrimination: Datasets used for targeted advertising and to hyper-personalize a user's experience can be used in ways that perpetuate or even amplify existing biases in areas like housing, credit, and employment.

6. Data insecurity: Every datum collected represents a liability. Overcollection increases the surface area for devastating data breaches, impacting millions of residents. When data breaches occur, they add to the troves of data floating around about each of us that, when placed in the hands of bad actors, makes us all more vulnerable to fraud and identify theft.

We believe a truly comprehensive and durable privacy law can mitigate some of these harms. To do so, the legislation must be structured upon three non-negotiable pillars: clear consumer rights, mandatory business duties, and robust enforcement.

Pillar One: Strong, Non-Waivable Consumer Rights

A comprehensive law must empower consumers with easily-exercised and enforceable rights. We urge the Committees to ensure any final bill incorporates the following:

• Universal opt-out mechanism: Critically, the law must mandate a centralized mechanism, such as a browser setting, allowing consumers to opt out of the sale, sharing, and use of their data for targeted advertising across all covered entities without prejudicing the consumer. This is referred to as a universal opt-out mechanism. By the end of this year, at least 12 states including California and Texas will require businesses that collect personal data for commercial purposes to recognize such a universal signal where available or required. It is both a more effective way for consumers to express their privacy preferences and significantly reduces the need for costly and sometimes annoying consent pop-ups. The mechanism should be easily accessible by the consumer and regulated entities should clearly indicate that they are honoring the consumer's wishes to protect their data.

• Protection for sensitive personal information: Consumers must have a right to affirmative, opt-in consent for the collection and processing of Sensitive Personal Information—which includes health, genetic, financial, and precise geolocation data. To be meaningful, such consent must be informed and be obtained separate from any other transaction and in a manner that makes clear that consent is not necessary to use the platform.

• Protection against default hyper-personalization: Requiring opt-in consent for profiling to deliver algorithmic personalization and a cool-off period for seeking consent for non-strictly necessary processing of data are important next steps in returning autonomy and control of their data back to New Yorkers.

• The right to know and access: The right for consumers to easily obtain a copy of the

specific pieces of personal information the business has or has access to and the categories of information a business has collected about them, and the sources of that information are basic privacy rights.

• The right to correct and delete: New Yorkers must have the ability to correct inaccurate information and to demand that a business or its service providers delete their personal information, with limited, specified exceptions.

Pillar Two: Mandatory Business Duties and Data Minimization

Consumer rights are meaningless if businesses are not bound by clear duties. The law must codify a duty of data minimization, mirroring the best practices already established in the CDPA and New York HIPA.

• Purpose and minimization principle: Businesses should only be permitted to collect personal information that is strictly necessary and proportionate to the stated purpose for which it is collected. They must not retain data longer than necessary for that specified purpose.

• Privacy assessments: Businesses engaging in high-risk data processing, such as processing sensitive personal information, or using the data for automated decision-making, must be required to conduct and document mandatory privacy protection assessments.

• Security and non-discrimination: Covered entities must maintain current and reasonable security procedures and cannot deny goods or services or charge a different price based on a consumer's decision to exercise their privacy rights.

Pillar Three: Robust and Dedicated Enforcement

A law is only as strong as its enforcement. For this law to be effective, we recommend requiring my office to enforce any new law. In addition:

• Funding to support enforcement: In the time since AG James took office, the legislature has been a reliable partner ensuring that any expansion of our duties is accompanied with appropriate enforcement resources. We very much appreciate this support and would ask that it continue for any new AG authority enforcing a comprehensive privacy law.

• Adequate penalty structure: The penalty structure must be significant enough to deter violations by the world's largest, most valuable technology companies. Penalties must be based on the number of violations or affected users, not just flat fines.

• Discretionary authority to promulgate regulations: Through rulemaking, the AG's office can provide guidance as needed for transparency and ease of compliance for regulated entities especially in this area where technology continues to develop at a rapid pace.

Conclusion and Call to Action

New Yorkers deserve a law that provides the necessary foundation for trust in our digital economy. By granting clear rights, imposing reasonable business duties, and ensuring effective enforcement, we can foster a regulatory environment that promotes innovation while safeguarding the civil liberties of our residents.

Testimony for 10/14 Assembly Hearing on Data Privacy

Good Morning, Chairs Rozic and Otis, and members of the Committees,

My name is Alex Spyropoulos, and I'm here today on behalf of Tech:NYC. Tech:NYC represents more than 550 technology companies operating and growing across New York, from early-stage startups to some of the world's largest technology firms.

As these committees explore the future of data privacy, we appreciate the opportunity to offer a perspective from our state's tech sector — not just the largest tech employers, but especially startups, small companies, and mission-driven organizations that increasingly rely on data to deliver services, build products, and engage with New Yorkers. I would also like to take this opportunity to thank you, Chair Rozic, for your leadership in working on this very important and complex policy area over the last few years. Tech:NYC looks forward to continuing to work with you and the rest of the Legislature on efforts to continue to adjust and pass your legislation: A.974 - the NY Data Protection Act.

In the absence of a single privacy framework at the federal level, Tech:NYC strongly believes in the importance of pursuing a state data privacy law that is sector agnostic and interoperable with the national landscape. As of today, 20 states have already adopted comprehensive data privacy frameworks—16 of which are in effect. Many of New York's neighboring states, such as New Jersey, Connecticut, Rhode Island, and New Hampshire, have taken action, and their specific state laws share several core elements: meaningful consumer rights, clear business obligations, and enforcement through the attorney general's office, not private lawsuits. Some of the common components of the New York Data Protection Act include aligning consumers' rights to control their data, requiring companies to conduct data protection assessments, and placing enforcement jurisdiction under the Attorney General's Office. Some of the outstanding recommendations for improvements to further align this bill with other states include incorporating a "Right-to-Cure" protocol to provide a cure period to fix violations before being penalized, and to align some of the bill's key definitions with other states like Connecticut - such as the terms "processing", "sale", and "third party", to name a few.

Without a federal data privacy standard, it is more important than ever for New York's approach to remain consistent with this emerging national model. Failure to align key definitions, compliance obligations, and rights across jurisdictions will result in a fragmented and burdensome environment for small and mid-sized businesses, which increasingly rely on websites to interact with their customers. These are the kinds of companies that make up the backbone of New York's innovation economy. Unlike large incumbents, however, these smaller companies can't afford a legal team in every state to advise on compliance and interpret regulations. Data privacy laws can be extremely complex and costly to comply with, and states that pass data privacy laws with even small differences will levy significant additional compliance costs on websites and platforms.

New York is home to over 2.2 million small businesses that employ over 3.7 million employees (over 45% of the state's employees), according to the most recent data from the Small Business Administration. Of the 2.2 million, 98% have less than 20 employees, and over half have no employees besides the

owner/operator. These small business operators have fixed budgets and costs, and adopting a divergent approach to data privacy would almost certainly increase their compliance costs. Small businesses are also not guaranteed to be lucrative or profitable, according to the SBA's 2024 Small Business Credit Survey, 35% of US small businesses operate at a loss, and 17% break even. Recent surveys have demonstrated that small businesses rely heavily upon leveraging online channels to sustain and grow their business, with 80% of small businesses having at least a basic e-commerce site in use to drive sales and expand customer contact, and the average small business generates half its sales via online channels. Combine these facts with a recent comprehensive study that examined the costs of a state privacy patchwork, which estimated that for NY-based businesses, there would be a cumulative compliance cost of $11.4 billion annually, a sizable addition to the operating budgets of the countless small businesses that would have to comply. This potential impact should not be underestimated as the Legislature considers what approach New York State aims to adopt in the data privacy realm.

Interoperability isn't just a business concern; it's a consumer clarity and consistency concern. People deserve the same rights and protections whether they're interacting with a company based in Connecticut, Colorado, or New York. Aligning New York's law with the architecture of other states will promote good data practices, reduce legal ambiguity, and allow innovative companies to scale ethically and efficiently.

And while this Legislature and state agencies are rightly focused on the risks and opportunities associated with artificial intelligence, it is worth emphasizing that any serious approach to AI governance must begin with a strong foundation of data privacy**.** AI represents the next generation of websites, apps, and online tools that users interact with and share data with - without a clear statewide data privacy law in place, New York lacks the core guardrails necessary to ensure AI systems operate within a responsible and rights-respecting data ecosystem. Advancing a data privacy law that defines consumer rights and obligations around data processing will serve as a strong precursor to New York's ability to regulate AI responsibly and ensure that all future policies are built on solid ground.

We appreciate the ongoing work of legislators across both chambers and encourage a continued focus on a comprehensive framework that includes clear definitions, streamlined responsibilities, and an enforcement structure that emphasizes consistency over confusion. A modern, harmonized approach to data privacy would make New York a national leader, not an outlier. While Tech:NYC has some outstanding recommendations to continue to improve A.974, this legislation contains structures that are similar enough to the data privacy laws in other states to serve as the most effective model for New York to consider. To that end, we have also shared a copy of the suggested amendments to A.974, and we look forward to discussing these and the implemented data privacy laws from other states with the legislature.

Thank you for the opportunity to testify. I welcome any questions.

TechNet Northeast Boston, MA 02108 www.technet.org

October 14, 2025

Re: Joint Assembly Consumer Protection and Science & Technology Committee Hearing Regarding Data Privacy

TechNet is the national, bipartisan network of technology companies that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

TechNet strongly supports a comprehensive data privacy law that is interoperable with the majority of existing state privacy laws in existence today.

We seek a comprehensive, risk-based framework of consumer rights over how their data is collected and used, and controller responsibilities to those consumers and the protection of that data, enforced by the state's attorney general. It's a model that has been thoroughly vetted and adopted in blue, red, and purple states, including Connecticut, New Jersey, New Hampshire, and Rhode Island.

The framework advanced in these states provides consumers with meaningful rights over how their data is used, and establishes a clear roadmap for companies to follow for compliance - including a clear limitation on what is collected in the first place. It is built upon definitions and operative provisions that have been carefully calibrated to ensure that personal information is safeguarded while allowing for the routine flow of information that is inherent in online transactions, and that more stringent measures are taken when dealing with information that is widely considered sensitive.

Chair Rozic's AB 974 is built on the foundation of such model laws, and while we would still seek some changes where certain definitions and operative provisions may deviate from those models cited above, we believe it would be an appropriate vehicle to advance a law that brings clarity to businesses operating in the state, and provides New Yorkers with protections and rights

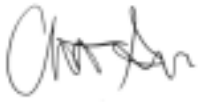
currently enjoyed by residents in nearly 20 states.

To date, New York has taken a piecemeal approach, advancing sector-specific bills to address subsets of data; namely, the Child Data Privacy Act, in effect since June of this year, and the Health Information Privacy Act that awaits Gubernatorial Action. Both policies contain outlier provisions and definitions that will require custom compliance solutions - increasing the overall cost of compliance and creating consumer confusion, while leaving significant gaps in the kinds of data covered.

An interoperable, comprehensive law would protect location information, health data - including reproductive and gender affirming care information - biometric data and all other personal data in a way that consumers understand and companies are prepared to follow. We ask that any comprehensive legislation that advances from your committees also include language to repeal or otherwise harmonize the discordant elements of the sectoral laws already passed.

TechNet looks forward to working with both of your committees as the session progresses. Please consider our members as a resource as you consider this legislation.

Sincerely,



Christopher Gilrein
Executive Director, Northeast
TechNet
cgilrein@technet.org

Testimony of Kate Goodloe

Managing Director, Policy

Business Software Alliance

Hearing on Data Privacy and Consumer Protections

New York Assembly Standing Committee on Consumer Affairs and Protection New York Assembly Standing Committee on Science and Technology

October 14, 2025

The Business Software Alliance is the leading advocate for the global enterprise software industry.[1] Our members create the business-to-business technologies used by companies across every sector of the economy. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Privacy and security are therefore core to BSA members' operations.

We appreciate your work to improve consumer privacy for New Yorkers and thank you for the opportunity to testify.

Consumers share their personal information online every day, just by using routine products and services. Whether we are shopping online, using apps to track workouts, taking rideshares, or hosting video calls with friends and family, we provide our information to a broad range of companies. Consumers deserve to know their data is used responsibly. BSA members have long advocated for a federal privacy law that protects consumers nationwide, and we recognize that states are leaders in protecting consumer privacy.

We encourage you to focus on four goals for any data privacy legislation:

- Adopt privacy protections that are interoperable with privacy laws in other states.
- Recognize the different roles of different companies that handle consumers' personal data.
- Protect the privacy of *consumers*, without sweeping in employees.
- Provide strong, exclusive enforcement to the state attorney general.

I. Adopt Privacy Protections That Are Interoperable with Existing State Privacy Laws

Twenty states have enacted comprehensive consumer privacy laws that create new rights for consumers, impose obligations on businesses that handle consumers' personal data, and create new

mechanisms to enforce those laws. As you consider how to craft a privacy law that is right for New York, we strongly recommend you look to existing privacy laws as the initial base.

Nineteen of the 20 states with consumer privacy laws start with the same structural framework. These laws take a common approach to protecting consumer privacy across state lines, even though the laws have different levels of substantive privacy protections. For example, lawmakers in 10 of those 19 states chose to require companies to honor universal opt out mechanisms, which let consumers use a standardized signal to exercise their rights to opt out of certain types of processing, but lawmakers in nine states did not. Similarly, lawmakers in 17 states chose to require companies to conduct data protection assessments, which require assessing privacy risks for activities like targeted advertising and processing sensitive data, while lawmakers in two states did not. BSA has created a resource that highlights the similar structures of these state privacy laws and we are attaching a copy for your reference.[2]

Anchoring New York's privacy law in a similar structural model — but adjusting the levels of substantive protections — supports an interoperable approach to protecting privacy that benefits both consumers and businesses in the state. When laws are interoperable, consumers can more easily understand how their rights change across jurisdictions. Interoperable laws also encourage companies to adopt strong, centralized compliance programs that serve consumers across jurisdictions. When laws are divergent, companies may need to adopt parallel compliance programs to satisfy similar requirements in different states. That requires companies to divide their funding and employees across duplicative programs, increasing the risks of errors and gaps.

We strongly recommend you take an interoperable approach to privacy, which will benefit consumers by driving investment in strong compliance programs that work across state lines.

II. Distinguishing Between Controllers and Processors Protects Consumers

Privacy laws should place meaningful limits on businesses that handle consumers' personal data and require them to handle that data responsibly.

To do this, a privacy bill must distinguish between two types of companies: *controllers*, which decide how and why to collect a consumer's personal data, and *processors*, which handle data on behalf of another company and pursuant to that company's instructions. The distinction between controllers and processors dates back more than 40 years, underpins privacy laws worldwide, and is reflected in all 20 state comprehensive consumer privacy laws.[3] Privacy laws must give clear obligations to both types of companies. To be effective, those obligations must reflect the different roles that each company has in handling consumers' data.

We strongly recommend any privacy legislation: (1) define controllers and processors, and (2) assign strong but different obligations to each type of entity, reflecting their different roles in handling consumers' personal data. This creates better protections for consumers, requiring all companies that handle their personal data to do so responsibly.

Controllers decide how and why to process a consumer's personal data — and they should be responsible for obligations related to those decisions. For example, if a law requires consent to process certain types of data, the controller should be obligated to obtain that consent. This ensures that a controller adjusts its decisions about how and why to collect personal data in light of its legal obligations.

Similarly, when laws create data minimization requirements, those obligations should fall on controllers — so that their decisions about how and why to collect consumers' data minimize the collection and use of that data. Controllers are also typically the companies interacting directly with consumers, so consumers usually expect them to carry out consumer-facing obligations like asking for consent and providing notice.

Many comprehensive state consumer privacy laws assign a common set of obligations to controllers, including:

- Responding to consumer rights requests, including requests to access, correct, delete, and port personal data.
- Honoring requests to opt out of certain processing, including targeted advertising, sale of personal data, and certain types of profiling.
- Obtaining consent to process sensitive personal data.
- Complying with data minimization obligations.
- Adopting reasonable data security measures.
- Providing privacy notices to consumers about how and why personal data is processed.
- Conducting data protection assessments, to assess potential impacts of specific activities.

Processors handle data on behalf of a controller and pursuant to its instructions — and they should be obligated to handle data confidentially and subject to contractual limitations.[4]

Many comprehensive state consumer privacy laws assign a common set of obligations to processors, including:

- Processing personal data pursuant to a contract with the controller.
- Deleting or returning personal data at the end of services.
- Providing information to the controller as necessary for the controller to conduct data protection assessments.
- Requiring any subprocessors engaged by the processor to meet the processor's obligations and to notify the controller that a subprocessor is engaged.
- Imposing a duty of confidentiality on persons processing personal data.
- Adopting reasonable data security measures.

These roles reflect the modern economy, where one company may rely on many processors to provide services to consumers. For example: A grocery store may decide to collect information from its customers and store that information in the cloud. The grocery store acts as a controller, because it decides what information to collect from consumers — and when, how, and why to use that information. The cloud storage provider acts as a processor, because it stores the data on behalf of the grocery store and processes it pursuant to the grocery store's instructions.

III. Focus on Consumers, Not Employees

As you develop comprehensive consumer privacy legislation, we urge you to focus on consumers — without sweeping in the separate privacy issues raised by employees. We strongly recommend taking the approach of 19 existing state privacy laws,[5] which focus on protecting consumer privacy. These laws exclude individuals acting in a commercial or employment context in their definition of

"consumer," and exclude data processed or maintained in employment contexts from the scope of their application.

IV. Provide Strong and Exclusive Enforcement to Attorney General

State privacy laws should create a strong, consistent enforcement mechanism by providing exclusive enforcement authority to the Attorney General. State attorneys general have a long track record of enforcing privacy-related laws in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. Promoting a consistent, clear enforcement approach helps companies understand their obligations and apply them in practice, better protecting consumers. All state privacy laws provide state attorneys general with enforcement authority,[6] and we urge you to adopt this approach in any comprehensive consumer data privacy legislation.

We appreciate the work of both Committees to protect the privacy of New York consumers. Thank you for the opportunity to testify, and I look forward to your questions.

Legislative Affairs

125 Broad Street, 19th Floor
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of the New York Civil Liberties Union

Before the Assembly Standing Committee on Consumer Affairs and Protection and the Assembly Standing Committee on Science and Technology regarding Data Privacy and Consumer Protections

October 14, 2025

The New York Civil Liberties Union (NYCLU) is grateful for the opportunity to submit the following testimony regarding Data Privacy and Consumer Protections. The NYCLU advances civil rights and civil liberties so that all New Yorkers can live with dignity, liberty, justice, and equality. Founded in 1951 as the state affiliate of the national ACLU, we deploy an expert mix of litigation, policy advocacy, field organizing, and strategic communications. Informed by the insights of our communities and coalitions and powered by 90,000 member-donors, we work across complex issues to create more justice and liberty for more people.

Our testimony for this Committee will describe the critical need for comprehensive consumer data privacy protections, as well as begin to name the complex legal considerations at stake. The NYCLU recommends that the New York Assembly extend the approach it has already taken to both young people's information and electronic health data to all consumer data. We look forward to partnering with the Assembly to ensure New Yorkers can attain the data privacy they deserve.

I. Introduction

It is no longer possible to participate in society without supplying our personal data to private companies, government agencies, and other third parties. We generally give away more data than we think, to more parties than we need, often unknowingly. We trade our data for access and convenience that might otherwise cost money, or we simply surrender it as the nonrefundable cost of doing business in the era of surveillance capitalism.

What's more, data privacy is a common thread that unites so many of us. Indeed, data privacy makes it easier for New Yorkers to enjoy their fundamental rights, like the right to free expression, the right to protest, the right to abortion, and the right to be free from discrimination, as well as secure in our physical safety.[1] Pursuing comprehensive privacy

[1] *Cf.* Ellie Quinlan Houghtaling, *Vindictive Trump Plots Ruthless Revenge Over His Legal Battles*, NEW REPUBLIC, May 30, 2024, https://newrepublic.com/post/182071/trump-revenge-lawsuits-hush-money january-6.

policies and legislation is all the more important at a moment in time when our federal administration and corporate actors are seeking to use our data to punish us and diminish our civil liberties.

II. Surveillance Capitalism: Background and Impact

Surveillance Capitalism[2]—a colloquial term for the tech industry's unregulated collection and leveraging of our personal data for profit—threatens our privacy. Companies collect every scrap of information available about our daily lives: what we buy, where we eat, who we associate with, our facial images, our fingerprints, our voices and conversations, our body shapes and gaits, our locations in real time, what routes we take to work, what music we listen to in the car, our social media and browser histories, and literally everything we click or tap on.

The more time we spend doing business with Big Tech, the less of our private lives we call our own.

Why is this a problem? A single data point, such as the purchase of one item in a drugstore, may not on its own reveal intimate details of one's life. But when aggregated with thousands of other data points and analyzed jointly with other data sets, such as one's entire purchase history, one's cellphone or car location data, the name and contact information of everyone one has spoken to in the last month, and one's entire browser history, that data provides an even deeper and more detailed profile of us than we can imagine. And along the way, the data may be sold, shared, fragmented, stolen, lost, or even used against us by corporations and the government. When that happens, the consequences are no longer simply about selling advertisements or buying and selling products. They are profound.

Here are just a few examples of what can happen:

Cambridge Analytica purportedly influenced the outcome of the 2016 presidential election by obtaining more than 50 million Facebook users' personal information from an unsavory app developer and allegedly using it to convince Americans to vote for Trump.[3]

Similarly, during the 2016 election, campaigns used personal information to target advertisements to African-Americans urging them not to vote at all, or to vote on the wrong day.[4] Reporting on these and other phenomena, the *New York Times* observed that exploitation of personal information enables "unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination."[5]

[2] Coined by Harvard Business School professor Shoshanna Zuboff, in her monumental *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.
[3] Timothy B. Lee, *Facebook's Cambridge Analytica scandal, explained [Updated]*, ARS TECHNICA, Mar. 20, 2018, https://arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal explained/
[4] Natasha Singer, *Just Don't Call It Privacy*, NYTIMES, Sept. 23, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html. [5] *Id*.

The stakes have only gotten higher since 2016 because of the impact of artificial intelligence (AI) on mass data processing. Indeed, AI has supercharged companies' ability to process images, crunch numbers, and identify complex behavioral patterns, setting up a potential revolution in behavioral engineering—not only in advertising, but in politics, medicine, employment, and elsewhere throughout our fragile democracy.

AI-powered surveillance capitalism is a significant revenue source for AI companies like Clearview AI, which amassed billions of facial images from social media sites without users' notice or consent, and used those images to engineer a vast surveillance system that law

enforcement agencies and various private parties then used to track individual people.[6]

In the meantime, "surveillance pricing" is becoming commonplace: retailers are charging different prices for the same goods and services based on customers' information (location, demographics, browsing patterns, shopping history, and other behavior), overcharging customers while perpetuating and amplifying discrimination.[7]

In the hands of an administration unmoored from the rule of law and motivated to pursue perceived political enemies, mass data collection threatens many areas of our lives. For instance, when it comes to reproductive freedom and LGBTQ rights, Trump and his allies have made clear that overturning *Roe v. Wade* was just the beginning—their ultimate aim is to eliminate access to abortion across the country and erase transgender people from public life. To do this, the Trump administration and its state government allies are using cutting-edge technologies to track and punish those they suspect of providing, receiving, or helping others to access abortion or gender-affirming care.[8]

The Trump administration has similarly promised to use online surveillance to identify and track down immigrants for draconian ends.[9] And, the administration's supporters have been identifying protesters they disagree with and submitting their names to Immigration and Customs Enforcement (ICE).[10]

In fact, the Internet, and social media in particular, has made it easy for the government and non-governmental actors to identify and retaliate against individuals who gather in public. At Columbia University, for example, pro-Palestine activists were targeted by a "doxxing truck" that displayed their names and photos on a billboard under the heading "Columbia's Leading

[6] *ACLU Sues Clearview AI.* PRESS RELEASE, May 28,2020. https://www.aclu.org/press releases/aclu-sues-clearview-ai

[7] Federal Trade Commission. *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices.* PRESS RELEASE. January 15, 2020. https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates wide-range-personal-data-used-set-individualized-consumer

[8] *E.g.* Rindala Alajaji, *She Got an Abortion. So A Texas Cop Used 83,000 Cameras to Track Her Down*, EFF, May 30, 2025, https://www.eff.org/deeplinks/2025/05/she-got-abortion-so-texas-cop-used 83000-cameras-track-her-down.

[9] Dell Cameron, *ICE Wants to Build Out a 24/7 Social Media Surveillance Team*, WIRED, Oct. 3, 2025, https://www.wired.com/story/ice-social-media-surveillance-24-7-contract/.

[10] *E.g.* Betar Worldwide (@Betar_USA), X (Jan. 29, 2025, 1:34 PM), https://x.com/Betar_USA/status/1884671352365576587.

Anti-Semites,"[11] and peaceful protestors were advised[12] to wear face coverings to avoid being doxxed. Some law firms are actively engaged in surveillance of law students to make those students unemployable.[13]

In sum, this mass data collection has enormous implications for our civil liberties and pillars of democracy.

III. New York Must Extend Privacy Protections to all Consumer Data

New York legislators have already selected a protective approach to data privacy in certain sectors, but in light of current threats, this is not far enough. For both young people[14] and commercial health data,[15] this body has opted rightly for an approach that prohibits the sale of New York data and requires a company obtain a user's affirmative consent before processing their data (unless that processing is strictly necessary for a short list of enumerated purposes). Like Washington,

Connecticut, and Nevada, this approach also provides individuals with access and deletion rights, includes data security provisions, and prohibits companies from charging people more or treating them differently because they exercise their privacy rights.

More must be done. **The Legislature should extend these protections into all areas of the surveillance economy. Even if the preferred path is a sectoral approach**, the Legislature should apply these consistent, appropriate, and measured consumer privacy protections across all sectors of the digital world.

IV. Key Components of Data Privacy and Consumer Protection Legislation

Effective privacy legislation must take the following into account, consistent with New York's past privacy-related enactments.

[11] Karam, Esha. *'Doxxing Truck' Displaying Names and Faces of Affiliates it Calls 'Antisemites' Comes to Columbia*, COLUMBIA SPECTATOR, Oct. 25, 2023, https://www.columbiaspectator.com/news/2023/10/25/doxxing-truck-displaying-names-and-faces-of affiliates-it-calls-antisemites-comes-to-columbia/.
[12] Ramirez, Isabella. *Shafik, 'Disheartened' by 'Abhorrent Rhetoric,' Reaffirms Safety in New Statement on Escalating Violence in Israel and Gaza*, COLUMBIA SPECTATOR, Oct. 18, 2023, https://www.columbiaspectator.com/news/2023/10/18/shafik-disheartened-by-abhorrent-rhetoric reaffirms-safety-in-new-statement-on-escalating-violence-in-israel-and-gaza/.
[13] Farrell, Maureen. *A Prestigious Law Firm Rescinded Job Offers for Columbia and Harvard Students, but It May Reverse Itself*, NY TIMES, Oct. 17, 2023, https://www.nytimes.com/2023/10/17/business/davis-polk-employment-columbia-harvard-israel palestine.html; Emily Flitter, *A Wall Street Law Firm Wants to Define Consequences of Israel Protests,* THE NEW YORK TIMES, July 8, 2024, https://www.nytimes.com/2024/07/08/business/sullivan-cromwell israel-protests.html?searchResultPosition=3; Joe Patrice, *Biglaw Firm's Antisemitism Fight Seems More Concerned With Anti-War Protests,* ABOVE THE LAW, June 20, 2024, https://abovethelaw.com/2024/06/sullivan-cromwell-law-school-antisemitism/.
[14] N.Y. Gen. Business. Law section 899-ee *et. seq.*
[15] S.929/A.2141, 2025-2026 Reg. Sess. (NY 2025) (awaiting Governor's signature). We encourage the committees to full-throatily urge the Governor to expediently sign this legislation.

A. Privacy Legislation Must Provide Meaningful Notice, Opt-in Consent, and Affirmative Obligations

Comprehensive and effective privacy legislation must include robust and meaningful privacy protections and accessible mechanisms for individuals to control their personal information.

Research demonstrates that it would take 76 work days for an individual to read all of the privacy policies encountered in a year.[16] This is because privacy policies that discuss companies' data collection, retention, use, sharing, and monetizing practices, are in fine-print legalese that no reasonable person reads. This practice is widespread. Countless websites, apps, services, internet-connected devices, and even brick-and-mortar stores collect, retain, use, share, and monetize our personal information—often in ways we do not understand and would not agree to if we understood.

Comprehensive privacy legislation must require meaningful notice to individuals that is concise and intelligible, clear and prominent, written in clear and plain language, and that leverages appropriate visualizations to make complex information understandable to the ordinary user.

But notice alone is insufficient. Legislation should also require individuals' affirmative, opt-in consent before covered entities collect, use, retain, share, or monetize their personal information that is not strictly necessary for a narrow list of permitted purposes. This is important, because default is often destiny. Many individuals never change a site's default settings, meaning that significantly more personal information will be processed under an opt-out regime than under an opt-in regime.[17] In addition, in order to ensure that opt-in consent is meaningful, comprehensive privacy legislation must prohibit the use of coercive site designs that manipulate individuals into granting their assent as well as pay-for-privacy regimes that risk making privacy a luxury good rather than a norm and right..

Finally, comprehensive privacy legislation must provide individuals with access, deletion, and portability rights and must include robust data security requirements; as well as limit covered entities to sharing individuals' personal information only with authorized parties that will treat that information with similar care.

B. Comprehensive Privacy Legislation Must Apply to All Personal Information

Comprehensive privacy legislation must provide meaningful protections for all personal information—that is any information that is reasonably linkable, directly or indirectly, to a specific individual, household, or device.

Too frequently, lawmakers, federally and in other states, have missed the mark by providing heightened protection for so-called "sensitive information" (like first and last name, social

[16] Alexis D. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.
[17] Lena V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PRO PUBLICA, July 27, 2016, https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world.

security numbers, and bank account numbers) and lesser protection for other personal information. This distinction is increasingly illogical in the digital age. Purportedly non sensitive information can be aggregated to reveal sensitive information, and, in fact, some non sensitive information, in isolation, may reveal sensitive information. For example, while health status is frequently considered sensitive, shopping history is not. But, if an individual is shopping at TLC Direct[18] and Headcovers Unlimited,[19] two websites that specialize in hats for chemotherapy patients, that individual's shopping history may reveal their health status.

Furthermore, sensitivity is highly subjective; different individuals are likely to perceive the sensitivity of different pieces of personal information differently. At bottom, line drawing around "sensitivity" levels is inherently arbitrary and ineffective, and comprehensive privacy legislation should protect all personal information.

C. Comprehensive Privacy Legislation Must Apply to All Types of Processing

Comprehensive privacy legislation must govern all types of personal information processing, including, but not limited to the following: collection, access, use, retention, sharing, monetization, analysis, creation, generation, derivation, decision-making, recording, alternation, organization, structuring, storage, disclosure, transmission, sale, licensing, disposal, destruction, de-identifying, or other handling of personal information.

Legislation that focuses solely or primarily on the sale of personal information misses the mark.

Many entities that profit off of personal information do not sell that information.[20] Rather, they leverage it to sell advertisements. For example, when an advertiser approaches an entity with an audience it would like to reach (say, suburban women with children who drive minivans and like the color blue), the entity often uses the personal information it maintains to match the advertisement to the desired audience.[21] The fact that the personal information does not change hands is immaterial—the entity still profits off of consumer data.

This sort of targeting is commonplace.

D. Privacy Legislation Must Provide for Standing and Redress

Comprehensive privacy legislation must include a private right of action. While the Attorney General and other state and local actors should have a role in enforcing any privacy law, a private right of action ensures accountability to those who are harmed. Importantly, it allows individuals to seek redress in cases where the government does not intervene and further incentivizes companies to adhere privacy protections in the face of private lawsuits. This is imperative, because given State budget constraints, the Attorney General will only have

[18] TLC DIRECT, https://www.tlcdirect.org (last visited Nov. 2, 2018).
[19] HEADCOVERS UNLIMITED, https://www.headcovers.com (last visited Nov. 2, 2018). [20] *E.g.* Kurt Wagner, *This is how Facebook uses your data for ad targeting*, RECODE, Apr. 11, 2018, https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg. [21] *Id*. Some entities are also set up to find look-alike audiences with similar traits to a pre-populated list an advertiser provides. Some also permit an advertiser to target particular individuals. UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

adequate resources to investigate claims, enforce violations, and assess penalties in the most egregious cases.[22]

A necessary requisite to any private right of action is ensuring that individuals have standing to bring lawsuits. Two legislative pathways exist.

The first is to make clear in the legislation that a violation of the act itself or regulations promulgated thereunder with respect to an individual's personal information constitutes an injury-in-fact to that individual. This is the approach that Illinois lawmakers took in their Biometric Information Privacy Act and that the Ninth Circuit has upheld.[23]

The second is for legislation to enumerate a fulsome list of harms[24] that arise from misuse of personal information and to confer standing on anyone who has experienced one of those harms as a result of a violation of the act or regulations promulgated thereunder. If lawmakers elect this approach, it is imperative to define harm more broadly than merely "reasonably foreseeable and material physical or financial harm" to an individual.[25] Although these harms are important, financial harm, in particular, is among the least likely to occur. That is because when financial loss arises from a data breach or misuse of data – say, where a credit card number is stolen and fraudulent purchases are made – it is often difficult to trace the stolen

[22] Letter from Calif. Attorney General Becerra to Ed Chau, California State Assembly, and Robert M. Hertzberg, California Senate, Re: California Consumer Privacy Act of 2018 (Aug. 22, 2018, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/08/ag-becerras-letter-re-california consumer-privacy-act.pdf) ("[T]he CCPA does not include a private right of action that would allow consumer to seek legal remedies for themselves to protect their privacy. . . . **The lack of a private right of action**,

which would provide a critical adjunct to governmental enforcement, **will substantially increase the AGO's need for new enforcement resources**. I urge you to provide consumer with a private right of action under the CCPA." (Emphasis added.)

[23] *See Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).

[24] A fulsome list of harms should include but not be limited to:

1. direct or indirect financial harm;
2. physical harm or threats to individuals or property, including but not limited to bias related crimes and threats, harassment, and sexual harassment;
3. discrimination in goods, services, or economic opportunity – such as housing, employment, credit, insurance, education, or health care – on the basis of an individual or class of individuals' actual or perceived age, race, national origin, sex, sexual orientation, gender identity or expression, disability, and/or membership in another protected class;
4. interference with or surveillance of First Amendment-protected activities by state actors; 5. interference with the right to vote or with free and fair elections;
6. interference with due process or equal protection under law;
7. loss of individual control over personal information, nonconsensual sharing of private information, and data breach;
8. the nonconsensual capture of information or communications within an individual's home or where an individual has a reasonable expectation of seclusion or access control; and 9. other effects on an individual that may not be reasonably foreseeable to, contemplated by, or expected by the individual to whom the personal information relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity that alter or limit that individual's choices or predetermine results.

[25] S.5642 § 2, 2019-2020 Reg. Sess. (N.Y. 2019).

information to a particular privacy violation.[26] When it is possible to trace the financial harm back, banks often reimburse customers for fraudulent purchases, obviating any actual financial loss.[27] Physical harm, of course, can be devastating when it occurs. However, these two harms are a vanishingly small subset of the harms that can arise from the pervasive collection, sharing, monetization, use, and misuse of personal information.[28]

A best practice would be to codify a rebuttable presumption of harm to an individual where the act itself, or regulations promulgated thereunder, has been violated with respect to that individual's personal information.

In addition to ensuring that private individuals have standing to sue, legislation should provide *per se* statutory damages for violations of the act. This approach, utilized in the federal Cable Privacy Act, is beneficial because, although the harm is real, quantifying damages associated with misuse or unauthorized use of personal information is often contentious in a litigation context. Statutory damages incentivize covered entities to comply with the law and have previously been employed, with success, in the privacy context.[29]

V. Other Legal Considerations Impacting Consumer Privacy Protections

Expanding New York's existing approach to privacy legislation to address all sectors of society, of course, will pose challenges that are different in scope from the challenges in drafting the existing sectoral bills. There are a set of complex legal considerations that should be taken in to account when drafting comprehensive privacy legislation, as well as future sectoral bills. The NYCLU looks forward to the opportunity to work with the legislature to address these areas.

A. The Government Must Limit How the Government itself Gathers and Utilizes Consumer Data.

While it is imperative that New York establish strong consumer privacy protections between data collectors and brokers on one side, and individual persons on the other, industry First Amendment protections and continued technological development may make it difficult to

regulate industry. To further protect consumers, the State should limit its *own* relationship with Big Tech by assessing how the state gathers and utilizes consumer data and how various government agencies either use industry resources to directly collect data on the State's own residents or purchase that data from brokers and third-party merchants.

The First Amendment protects Americans' right to communicate and receive information anonymously and with minimal government interference. This generally makes it unlawful for

[26] *See* Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, WALL STREET J., June 26, 2016, https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases 1466985988.
[27] *Id.*
[28] *See generally* Allie Bohm, Policy Counsel, NYCLU, A Joint Public Hearing to Conduct Discussion on Online Privacy and What Role the State Legislature Should Play in Overseeing It, Testimony before the New York State Senate Committee on Consumer Protection and the New York State Senate Committee on Internet and Technology (June 4, 2019).
[29] *E.g.* 47 U.S.C. § 551 (2001) (The Cable Privacy Act).

the government to track what we read, who we talk to, what we say, and who we associate with. The surveillance economy has upended this balance because the government can now purchase (or simply demand) our personal data from companies.

Indeed, the ever-growing partnership between law enforcement and the surveillance capitalism industry is chief among today's greatest threats to personal privacy. For example, private companies collect personal data about their customers at a scale beyond that of all but the most powerful intelligence agencies—and then share it with or sell it to law enforcement, who often lack a proper warrant or even a valid subpoena.

These transactions may happen without the knowledge or consent of the person to whom the information pertains, allowing the government to learn almost anything it wants about us– circumventing the constitutional safeguards that would have shielded the same information in the analog age. Especially in today's political climate, this is untenable.

The Legislature must make sure that *all* personal data—not just "sensitive" data[30]—is off-limits to police and other government actors absent a warrant or valid subpoena *issued by a court and signed by a judge*—this means that a neutral arbiter has signed off that the data is likely to turn up evidence of a crime, an important safeguard against government over-reach and fishing expeditions.

B. The First Amendment Protects Anonymous Speech

People of all ages rely on the internet and social media not only for news, information, commentary and entertainment, but also community, companionship, advice and support. For people—especially young people—who cannot find those things locally, or who are afraid to discuss personal issues with parents or nearby adults, the internet can be a lifesaver. For those who wish to seek community or support anonymous, however, age-verification protocols and other online identification requirements burden users who may want to participate, but who do not have a government ID, or who are otherwise concerned about their privacy and security.[31] They force users to "relinquish their anonymity to access protected speech, and . . . create a potentially permanent electronic record" of the sites users choose to visit.[32] That "constitutes an encroachment into the personal lives of those who use the internet precisely because it affords anonymity."[33]

Fortunately, courts across the country are beginning to understand the scope of the surveillance ecosystem, and have begun enjoining age verification and other invasive laws on privacy-related

grounds, recognizing that such practices can burden the First Amendment rights of who wish to use social media anonymously;[34] deter *lawful* users who can't or won't turn over personal

[30] *Supra B. Comprehensive Privacy Legislation Must Apply to All Personal Information.* [31] *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 99 (2d Cir. 2003).
[32] *ACLU v. Mukasey*, 534 F.3d 181, 197 (3d Cir. 2008).
[33] *State v. Weidner*, 235 Wis. 2d 306, 320 (2000).
[34] *See*, *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998) (holding that mandatory age verification "violates the First and Fourteenth Amendments of the United States Constitution because it

information;[35] burden the First Amendment rights of young people, even assuming those rights are not coextensive with those of adults;[36] and, generally raise significant privacy concerns.[37] This is not a surprising trend, as requiring users to submit personal information to social media platforms or third-party authenticators carries significant risks the data will be either misused or leaked, a problem made worse if biometric or other sensitive information is involved.[38] The Legislature must resist the growing trend of putting some content behind privacy-destroying age assurance or identity-proving mechanisms.

C. *The First Amendment Also Protects Companies' Data Processing*

While protecting anonymous expression from government infringement, the First Amendment also protects the distribution and flow of information among private parties, including personal information that has already been shared or otherwise made public. This means that in crafting privacy laws, the Legislature must tread carefully when telling private entities how they may process or distribute the data they collect.

While jurisprudence in this area is still developing, the U.S. Supreme Court has articulated a few clear principles by the Legislature should abide. Most critically, any comprehensive privacy law may not restrict the processing of personal information based on the purpose of the processing or the identity of the processor.

This barrier to the government's ability to restrict information-sharing played out most prominently in *Sorrell v. IMS Health Inc.* There, the U.S. Supreme Court overturned a Vermont statute that prohibited regulated entities from "selling or disseminating prescriber-identifying information for marketing," subjecting content- and speaker-based restrictions "on the sale,

prevents people from communicating and accessing information anonymously"), *aff'd*, 194 F.3d 1142 (10th Cir. 1999).
[35] *See*, *e.g.*, *PSINet, Inc. v. Chapman*, 362 F.3d 227, 236-37 (4th Cir. 2004) (age-verification using credit card numbers "creates First Amendment problems of its own" because "many adults may be unwilling to provide their credit card number online" and "[s]uch a restriction would also serve as a complete block to adults who wish to access adult material but do not own a credit card"); *Se. Booksellers Ass'n v. McMaster*, 371 F. Supp. 2d 773, 782 (D.S.C. 2005) (holding that age verification creates a "First Amendment problem" because "age verification deters lawful users from accessing speech they are entitled to receive").
[36] *See*, *NetChoice, LLC v. Reyes*, No. 2:23-CV-00911-RJS-CMR, 2024 WL 4135626, at *14 (D. Utah **Sept. 10, 2024**) (emphasis ours, decided **post** SAFE Act enactment)
[37] *See NetChoice, LLC v. Bonta*, No. 22-CV-08861-BLF, 2023 WL 6135551, at *12 (N.D. Cal. Sept. 18, 2023) (noting the California Age Appropriate Design Code's age verification provision was "actually likely to exacerbate the problem by inducing covered businesses to require consumers, including children, to divulge additional personal information."); *PSINet*, *supra* (adults may be unwilling to submit credit card numbers online).
[38] Requiring adult users to produce state-approved documentation to prove their age and/or submit to biometric age-verification testing **imposes significant burdens on adult access to constitutionally protected speech and "discourage[s] users from accessing [the regulated] sites**." *Reno v. American*

Civil Liberties Union, 521 U.S. 844, 856 (1997). Age-verification schemes […] "are not only an additional hassle," but "**they also require that website visitors forgo the anonymity otherwise available on the internet**." *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 99 (2d Cir. 2003); *see also ACLU v. Mukasey*, 534 F.3d 181, 197 (3d Cir. 2008) (finding age-verification requirements force users to 'relinquish their anonymity to access protected speech').

disclosure, and use of" personal information to heightened scrutiny.[39] Any comprehensive privacy law that totally proscribes the collection, use, retention, sharing, or monetization of personal information based on the purpose for the leveraging or the identity of the entity doing the leveraging is likely suspect under *Sorrell*.

A *Sorrell* problem could materialize in legislation in multiple ways, from bills that cover only a subset of entities that leverage the same types of personal information to bills that regulate only particular uses of personal information. Perhaps the most tempting way the issue arises is when well-meaning bill drafters endeavor to create a journalism carveout to any privacy bill. In addition to raising difficult questions about who qualifies as a journalist, a journalism carveout is both an identity-based (journalist) and purpose-based (news gathering and dissemination) distinction that the Supreme Court is likely to look askance at following *Sorrell*. The same thought process would apply to carveouts for essentially non-monetary purposes like scientific research, opposition research, and opinion polling.

Fortunately, there is a constitutional way to ensure that privacy legislation does not undermine journalism—a goal we certainly share. That solution is to focus on the way personal information is collected so that legislation applies to personal information captured in exchange for any kind of consideration, including but not limited to a good or service, the placement of targeted advertisements, or a membership; as a result of an individual, household, or device's establishment or maintenance of an account with a covered entity; or as a result of an individual, household, or device's interaction with a covered entity. Although a major downside of this approach is that it would not reach data brokers that have no direct relationship with individuals, if a bill is properly drafted, it would likely ossify the data broker industry by choking off new sources of personal information.

In addition to *Sorrell*, First Amendment jurisprudence around how websites present content and drive user engagement are still developing and will take time to percolate through the courts. Indeed, while general protections for website editorial discretion and content presentation are no longer in doubt,[40] a more nuanced judicial review of the various methods of privacy protection has barely begun. For the time being, legislatures will have to navigate some uncertainty about what access- or content-limiting website features may run afoul of the First Amendment.

*****

The NYCLU thanks the committees for the opportunity to provide testimony and for your focus on this critical and timely issue. We look forward to working with you to create real and meaningful privacy protections for New Yorkers—it has never been more important.

[39] 564 U.S. 552, 562 – 65 (2011).
[40] *Moody v. NetChoice LLC*, 144 S.Ct. 2383 (2024).

October 10, 2025

Chair Nily Rozic
Committee on Consumer Affairs and Protection
Chair Steven Otis
Committee on Science and Technology
New York State Assembly Hearing
Room C
Legislative Office Building
Albany, NY 12210

Re: Joint Public Hearing on Data Privacy and Consumer Protections

Dear Chair Rozic and Chair Otis,

Thank you for inviting me to testify today and thank you for your work on and attention to the critical issue of data privacy. My name is Matt Schwartz, and I am a policy analyst with Consumer Reports based in Washington D.C.

Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. CR has 6 million members spread across every state in the U.S., including New York.

Consumer Reports has advocated at the federal and state levels for the introduction and passage of comprehensive data privacy legislation. We have worked with lawmakers and advocates in dozens of states to advance legislation that is as workable and protective of consumers as possible. We are also currently working with lawmakers in New York to advance legislation to ensure our connected device manufacturers are transparent about their data security practices (S. 8507) and to strengthen New York's General Business Law (A.5287, (A.8427, and S.105).

As you've heard from many others, Congress has tried and failed to pass a privacy law for years now, and so it has fallen to states to step up and protect their constituents. And as you also might be aware, big tech companies have made the rounds across states to try to pass their favored model of privacy legislation in lieu of stronger protections that meaningfully change business practices to address harms faced by consumers. When they've been unable to advance their own model, they've worked tirelessly to undermine stronger efforts from being signed into law.

But over the last year or so, we've seen states increasingly reject industry lobbying and push for real privacy protections. In 2024, Maryland passed a comprehensive privacy law that broke with

national trends and instituted real limitations on when companies can collect and use personal and sensitive data. Earlier this year, states like Oregon, Connecticut, and California updated their existing privacy laws to better protect consumers. And strong privacy bills have made progress in states like Washington, New Mexico, Massachusetts, and Maine. We are hopeful that New York can join this national trend.

In our view, privacy legislation must contain three core provisions, which are reflected in our model state privacy legislation we co-created along with our partners at EPIC.

First, privacy legislation should put default limits on when companies can collect and use personal data. This concept is often called data minimization, and it is the idea that companies only collect and use data that is necessary to provide the service the consumer has asked for. So, my weather application needs my location data to give me the forecast, but it doesn't need to sell my location data to other businesses or data brokers for unrelated purposes. Privacy laws should ensure that unnecessary uses of data are blocked by default, and that they don't require the consumer to make any choices, such as opting in or opting out in order to protect themselves.

Second, privacy laws should create heightened protections for sensitive data, including an outright ban on the sale of data like our cell phone location data, religious and political beliefs, and information collected from minors. Unfortunately, there is a multi-billion-dollar industry centered on collecting and selling people's sensitive information, often collected from people's mobile devices. This information is often collected by shadowy data brokers and routinely used for purposes against consumers' interests, to stalk individuals, to set insurance rates based on information that people never even realized they were sharing, and, increasingly, to price essential products and services, like groceries, based on their individual willingness to pay. Good privacy laws should set strong standards that prevent the abuse of our most sensitive data.

Finally, we believe privacy laws need strong enforcement mechanisms in order to help incentivize companies to comply. Under the 13 active state privacy laws, which all lack a private enforcement mechanism, there have only been a handful of public enforcement actions to-date. And yet, one does not need to look hard to find obvious violations of privacy laws. Two separate privacy compliance websites recently shared that they've found that more than 70 percent of top websites are not compliant with state privacy provisions related to opt-outs. We are more than willing to be flexible about what stronger enforcement looks like in practice, including protections for frivolous lawsuits, but leaving these laws fully under the purview of AG's offices has not been a successful strategy so far.

Overall, there is much we can take from the progress being made in privacy legislation across the states. We'd love to be a resource for you to ensure that New York keeps pace. Thank you again for inviting me and I'd welcome any questions you have.

Sincerely,

Matt Schwartz
Policy Analyst

Testimony of Dr. Siwei Lyu
SUNY Distinguished Professor of Computer Science and Engineering
Director, Center for Information Integrity, University at Buffalo
Before the New York State Assembly Committees on Consumer Affairs and Protection and Science and Technology, Tuesday, 10/14/2025

The exponential rise in data collection has far outpaced the development of regulatory efforts. Almost every digital activity—whether on social media, through online shopping, or via smart devices—produces personal data that are stored and potentially exploited by third parties. Traditional data mining already exposes sensitive details about individuals' lifestyles, political leanings, and personal preferences. The growing use of personal data to train generative AI systems amplifies privacy and security risks. When personal imageries and voice recordings are collected without adequate safeguards, they can be exploited to fabricate highly realistic synthetic images, voices, and videos, with wide-ranging consequences.

These harms are no longer hypothetical and are already playing out in New York. **Financial harm** has surfaced. The New York Attorney General's office recently warned of investment scams using manipulated videos of celebrity endorsements to mislead and defraud New Yorkers[1]. AI cloned voices are used to impersonate family members and extort money in scams targeting New Yorkers[2]. A Long Island man was sentenced for creating and sharing deepfake pornographic images of underage women without their consent[3], demonstrating the **Reputational harm to individuals**. **Public harm** also looms: a case in point is the political robocalls that used an AI-generated voice of President Biden to discourage voter turnout in the 2024 New Hampshire primary.

Strong safeguards are needed to protect New Yorkers and their communities from the escalated risks posed by AI trained on unconsented personal data. **Transparency and disclosure** should be the foundation: companies must be required to clearly report in formats accessible to the public about what data is collected, how it is used, and with whom it is shared. **Data minimization** should guide collection practices, ensuring that organizations gather only what is strictly necessary for the stated purpose rather than engaging in sweeping data harvesting.

Accountability mechanisms are equally important. It is unacceptable to input personally identifiable, confidential, or sensitive information into an AI system if that system uses the data to train its model or risks disclosing it to unauthorized parties. Generative AI systems must also be held to stricter standards when generating personal specific content. No one should use unconsented personal data to create outputs aim to deceive. To prohibit the misuse or mishandling of personal information in AI systems, New York State needs to create independent AI auditing guidelines, structures, and enforcements.

At the same time, we need **practical defenses**—tools to reliably detect AI-generated media and methods to remove certain user data from models, a procedure known as unlearning, when necessary. These measures will help ensure AI serves the public interest while protecting privacy, security, and trust. Finally, investment in **public education** is critical, and New York can prepare her citizens—particularly vulnerable groups including the younger generations and older adults—to recognize and resist manipulation in digital environments.

New York has already demonstrated national leadership in AI technologies with the **Empire AI** Initiative. But we cannot underestimate risks posed by unregulated data collection and AI misuse to New Yorkers, which demand a coordinated response. And there is no better time than now to take actions.

---

[1] **New York Attorney General press release**, "Investor alert: AI-enabled deepfake investment scams targeting New Yorkers".
[2] **CBS New York**, "Voice-cloning scams are a growing threat in New York".
[3] **Fox5 NY**, "Long Island man sentenced for sharing deepfake porn of underage women".

Testimony before the NYS Assembly Committee on Science and Technology
Helen Nissenbaum
Andrew H. and Ann R. Tisch Professor, Information Science
Director, Digital Life Initiative, Cornell Tech
New York City, October 14, 2025

The frenzied demand for data to fuel Large Language Models and an explosion of interest in AI agents (agent systems) adds more reason to revisit privacy regulation. With little hope that the Federal government will act on privacy; the States have an opportunity to step up and set an example. This moment also offers an opportunity to correct a course on privacy regulation which, increasingly, has dried far from the actual threats posed by private and public actors, armed with powerful digital technologies with formidable capacities to capture and process data, conduct surveillance, generate knowledge about us, and manipulate human behavior.

I'd like to offer two key points:

I. It's time to move on from the failed project of notice-and-choice (privacy terms of service, privacy policies, notice and consent).

What may have been plausible in 1974 is utterly without merit in 2025. There is a vast literature offering incontrovertible, rigorous, scientific evidence that the approach does not, nor can it deliver privacy. (If you doubt this point, how does the approach protect privacy threats from Ring Doorbells, now armed with facial recognition, Meta Ray-Ban glasses, and more.)

While acknowledging that digital technology has produced a lot of good, thoughtful privacy regulation could have saved us from many of the harms associated with the current regime. To prevent a repeat of past mistakes, it's still worth asking why notice-and-choice has remained entrenched for so long. One clear reason is vested interests. Tech industry incumbents bemoan the complexity and cost of compliance. While the approach holds incumbents to their published terms of service, it allows them virtually free reign to determine what these terms are. To let powerful stakeholders unilaterally define terms, on such a massive scale, is negligent.

For one-hundred years, the Catholic Church clung onto a Geocentric theory of the planetary system despite overwhelming scientific evidence favoring Heliocentrism. For sound privacy protection, fifty should be the cutoff.

II. Challenging the (apparent) absence of alternatives.

I have argued that comprehensive privacy protection must begin with a baseline of substantive rules governing data flows, tailored to specific domains and relationships. Before I am heckled out of the meeting, I remind you that we've done this before. We have privacy rules for the health domain, finance, law enforcement, education, and a few more. In many of these cases, lawmakers wisely delegated rulemaking to respective agencies and experts, authorizing them to develop rules that calibrate the safety and interests of data subjects with the data flow needs of these domains – the purposes and values of healthcare, finance, etc. – subject to fundamental political and ethical values of our society. Such calibration cannot be achieved solely with a pairwise procedural mechanism of notice and choice.

Unfortunately, these sectoral rules, too, are in dire need of an overhaul, in order to mitigate the shifting contours in education, healthcare, finance, etc. brought about, largely, by a vast landscape of online digital services, devices, apps, and soon agent systems. These ships have created gaping holes. For example, in healthcare, online companies and apps that provide health services have dodged constraints, which apply to traditional healthcare settings. Why is this a problem? Because they leave users exposed and vulnerable. Similarly, I have heard school superintendents complain they don't know for sure where their students' data has flowed due to the scores of third-party educational learning and administrative tech intermediaries. Imagine when AI is admitted to classrooms! We're rightly preoccupied with what it means for learning. But what of the data about our children that these systems extract? (An article with Professors K. Strandburg (NYU Law School) and S. Viljoen (University of Michigan Law School) discusses *regulatory dodge* around HIPAA privacy rules and around GLBA privacy rules.)

Importantly, correcting these rules does not mean making them more restrictive. It might mean making them less restrictive, allowing carefully tailored data flows, previously disallowed, that promote the public interest, e.g., by furthering open scientific research or public health.

Bringing substantive privacy regulation to the vast tranches of online life that are not presently subject to privacy law means acknowledging significant differences within and among these tranches. In the past, steamrolling over these differences allowed the entry of predatorial data brokers and enabled abuses by vast tech empires which, by law, were allowed to aggregate data from wildly disparate holdings. We need distinctive sets of privacy rules that acknowledge the obvious discontinuities between incompatible social domains.

Most of us know that buying a car is not the same as reading a newspaper and should be protected as such. Socializing on Instagram is not the same as engaging professionally on LinkedIn, an avid gardener searching for a trowel is different from a victim of abuse searching for a hotline on a chatbot or a web search engine. Just because services are online and commercial does not mean the same privacy rules apply across the board. Flattening these differences flies against our values and – as our studies have demonstrated – against the privacy expectations of ordinary people. Individual consent may play a role but only within guardrails.

As with sectoral regulation, we should seek guidance on privacy rules from domain experts and wisdom borne of closely studying distinctive areas and practices of online life. Highly trained technical experts and commercial incumbents should be consulted, too, but we dare not leave it to the proverbial foxes to guard the henhouse. The mistake today? Believing that only the titans of GenAI know enough, mistaking self-serving blog posts based on nontransparent experiments for objective scientific evidence.

This is a good moment to address the resurgent interest in privacy. With the dangerous potential of personalized AI agents, we are no longer in a competition of us (data subjects) versus them (tech companies). Instead, regulation should protect data subjects while rewarding commercial actors seeking to do the right thing by their customers and society.

Selected publications relevant to testimony

K. Martin, H. Nissenbaum, V. Shmatikov (2025) "No Cookies For You! Evaluating The Promises of Big

Tech's 'Privacy-Enhancing' Techniques.," *Georgetown Law Technology Review, 9 Geo. L. Tech. Rev. 1 (2025)*

K. Strandburg, S. Viljoen, H. Nissenbaum (2024) "The Great Regulatory Dodge," *Harvard J. Law & Tech 1231 (2023)*

I. Sivan- Sevilla, H. Nissenbaum, P. Parham (2022) "Public Comment for FTC's Commercial Surveillance ANPR," *OSF Preprints*.

K. MarPn and H. Nissenbaum (2020) "What is it about LocaPon?" *Berkeley Technology Law Journal,* 35:1, 103.

K. Martin and H. Nissenbaum (2017) "Privacy Interests in Public Records: An Empirical Investigation," *Harvard Journal of Law and Technology* 31:1, 111-143.

K. Martin and H. Nissenbaum (2017) "Measuring Privacy: An Empirical Test Using Context To Expose Confounding Variables," *Columbia Science and Technology Law Review* 18, 176-218.

H. Nissenbaum (2019) "Contextual Integrity Up and Down the Data Food Chain," *TheoreGcal Inquiries in Law* 20:1, 221-256

H. Nissenbaum (2015) "Respect for Context as a Benchmark for Privacy Online: What it is and isn't," In *Social Dimensions of Privacy*, Eds. B. Roessler, D. Mokrosinska, Cambridge: Cambridge University Press.

S. Barocas and H. Nissenbaum (2014) "Big Data's End Run Around Consent and Anonymity," In *Privacy, Big Data, and the Public Good*, Eds. J. Lane, V. Stodden, S. Bender, H. Nissenbaum, Cambridge: Cambridge University Press, 44-75.

H. Nissenbaum (Fall 2011) "A Contextual Approach to Privacy Online," *Daedalus* 140:4, 32-48.

Testimony of
Pavan Kochar
CEO & Co-Founder, Certree pavan_kochar@certree.com | +1 (650) 800-8868 |
https://www.certree.com

Before the
New York State Assembly Standing Committee on Consumer Affairs and Protection New York State Assembly Standing Committee on Science and Technology

Joint Public Hearing on Data Privacy and Consumer Protections October 14, 2025

Thank you, Chair Rozic, Chair Otis, and members of the committees, for the opportunity to testify on the critical issue of data privacy and consumer protections.

My name is Pavan Kochar, and I am the CEO and Co-Founder of Certree, a California-based technology company committed to giving individuals ownership and control over their official records — such as proof of income, employment, and education credentials.

Every day, the payroll and education records of millions of New Yorkers are shared and monetized by data brokers — often without people even knowing. Life-changing decisions — applying for a loan, a mortgage, an apartment, social benefits, or a job — are being made based on data that individuals have never reviewed for accuracy and are difficult to correct. At the same time, identity thieves exploit systems that lack proper safeguards and authentication.

The workers and students most affected often have no idea this is happening, no ability to stop it, and may lose life-changing opportunities without ever knowing why.

Today's employment and education data ecosystem is dominated by a few powerful brokers who obtain information through exclusive contracts with employers, colleges, and payroll providers.

Organizations such as employers, schools and colleges routinely send payroll and student data to these brokers to handle verification requests — such as background checks by employers, income verification for mortgage companies, or eligibility verification for social benefits. The brokers then aggregate and resell this information to lenders, landlords, background check companies, data resellers, and other buyers.

This broker-driven model of verification is fundamentally broken for several reasons.

Once data ends up with a broker, consumers lose all control. The largest payroll data broker in the country markets a "360-degree consumer view," giving its corporate clients access to a person's income, employment, education, credit, bank balances, and even criminal history – something no one has truly consented to.

An FTC study found that 21% of respondents had successfully disputed at least one error in their data reports. Faulty information routinely costs workers jobs, loans, apartments, and social benefits. Because brokers bypass the individuals whose data they use, most never even know inaccurate data was the reason they were rejected. When they do discover errors, fixing them is nearly impossible: in 2021, the CFPB reported that the largest brokers provided relief in fewer than 2% of complaints. In this model, consumers are not customers — they are products.

Major brokers often do not directly authenticate the individuals whose data they release. They rely on intermediary buyers to confirm consent — a loophole that enables fraudsters to impersonate victims and commit financial identity theft without the victim's knowledge. Worse still, because many brokers also

sell credit monitoring services, they profit when fraud incidents rise.

Centralized databases of payroll and education data are enormous targets for hackers. The largest brokers in payroll and education have all suffered mass breaches — one admitted to facing 35 million cyberattacks per day. Every breach exposes millions of records, leaving consumers to deal with the aftermath.

These brokers pay for exclusive access to employer payroll data and use their dominance to eliminate competition. As a result, they have entrenched monopolies that drive up costs for everyone — lenders, consumers, and government agencies alike. Taxpayer dollars are wasted on inflated verification services, and borrowers face higher fees as costs are passed along. In effect, payroll data is auctioned to the highest bidder, while the citizens whose information fuels the system bear the ultimate cost.

In fact, an entire industry of verification companies recently filed an antitrust class action against the largest payroll data broker for this very reason.

Certree has also submitted a petition to the Federal Trade Commission calling for an investigation into the anti-competitive and privacy-violating practices of dominant data brokers.

New York can lead the nation by adopting a rights-based framework that puts individuals back in control of their personal data.

No payroll or student data should be transmitted to a third party for verification unless:

- The individual gives explicit, informed consent; and
- The individual has a reasonable opportunity to review and correct that data before it is transmitted.

This approach isn't radical — it's common sense and long overdue. We are talking about data that can shape one's life trajectory. It can block someone from a job, sink a mortgage application, deny access to social benefits, or hand over the keys to identity thieves. This is more than data; it's destiny — and it must be treated with the seriousness that it deserves.

At Certree, we've proven that a privacy-first model is possible. Our platform allows employers, schools, and agencies to issue official documents directly to individuals in a private, tamperevident vault. Only the individual can view and share their own records — Certree cannot see or sell their data. Individuals maintain full control and transparency over who can access what, ensuring that true consumer protection can be achieved through technological innovation.

New York has long been a national leader in financial integrity, civil rights, and consumer protection. This is your opportunity to close a dangerous loophole that allows corporations to traffic in personal data without consent, transparency, or accountability.

We are not asking for too much. If data brokers want to use our personal data for life-changing decisions, the least they can do is ask first — and make sure it's accurate.

By passing this legislation, New York can protect privacy, improve data quality, foster fair competition, and set a national precedent for responsible, people-first data governance.

Thank you, Chair Rozic, Chair Otis, and members, for your leadership and for giving Certree the opportunity to contribute to this important discussion. I welcome your questions.

Supporting Documentation and References

1. Certree Petition to the FTC (2022): Requests investigation into anti-competitive practices in payroll and employment data markets.
https://certree.com/assets/petition_to_ftc.pdf
2. Greystone Mortgage Inc. et al. v. Equifax Workforce Solutions LLC: Class action alleging monopolization of income and employment verification markets.
https://www.classaction.org/media/greystone-mortgage-inc-et-al-v-equifax-workforcesolutions-llc-et-al.pdf
3. St. Louis Housing Authority v. Equifax Workforce Solutions: Lawsuit alleging unfair leveraging of exclusive contracts and inflated pricing in violation of antitrust laws.
https://www.classaction.org/media/st-louis-housing-authority-v-equifax-workforcesolutions_1.pdf
4. RealClearPolicy (2022): Article describing how Equifax's Work Number system raises mortgage costs and undermines transparency.
https://www.realclearpolicy.com/articles/2022/03/21/how_the_work_number_cheats_american_consumers_822725.html
5. Duke University (2023): Study reporting data inaccuracies and the flow of student data from colleges to data brokers and credit bureaus.
https://techpolicy.sanford.duke.edu/wp-content/uploads/2023/07/Data-Brokers-and-theSale-of-Students-Data-Simmons-2023.pdf
6. ProtectBorrowers.org (2023): Analysis exposing how the National Student Clearinghouse avoids FCRA oversight, leading to data errors that harm borrowers.
https://protectborrowers.org/how-a-data-company-at-the-center-of-the-student-loansystem-is-costing-borrowers-millions/

Testimony of Dawn Kelly

Hearing on Data Privacy and Consumer Protections

October 14, 2025

My name is Dawn Kelly. I own The Nourish Spot, a juice bar and community hub in Jamaica, Queens. I write today as a small business owner deeply concerned that proposed limits on data access could make it harder for local businesses like mine to reach customers, grow, and create jobs.

After my corporate job was eliminated in 2015, I turned that setback into a new beginning. I opened The Nourish Spot with my daughter, hoping to nourish our community with healthy food and good jobs. We started out with a single storefront in Jamaica, Queens, and have since opened a second location, served as a food vendor for the U.S. Open, and expanded into JFK Airport. That growth has been powered by digital tools powered by data.

Anonymous, non-personally identifiable data is a lifeline for small businesses — powering a host of critically important tools. Data helps me send digital ads to likely customers, understand my customers and their preferences, and make informed business decisions. For example, our Google Business Profile data showed where customers were visiting from, helping us decide where to open a second location.

We're not invading anyone's privacy; we're simply using insights from aggregated data to provide quality service. Letting a customer know about a new version of a smoothie they enjoyed last week isn't prying — it's good business. Your decisions about data access will have a major impact on small businesses like mine. If digital ads become less effective because data is degraded, or if we lose access to data-powered insights and analytics, it will be much harder for us to connect with and understand our customers — hurting our bottom line.

Lastly, I am deeply concerned that a private right of action might be included in data-privacy legislation. As a member of the NYC Mayor's Small Business Advisory Council, I saw firsthand how predatory law firms use private rights of action to extract fees from well-meaning, law-abiding small businesses. We are already struggling with serious economic uncertainties, and we don't have the time, energy, or money to fight frivolous lawsuits. I strongly urge you to consider how a private right of action exposes small businesses to predatory practices.

I share your goal of protecting consumers, but we need to find a balance that also protects small businesses. Data-powered tools are essential for our success and growth. As you consider this issue, I ask that you please don't cut off the data that powers our digital tools and keeps us thriving. Instead, please continue to work with us to craft legislation that empowers small businesses to keep serving our communities, creating jobs, and succeeding in today's digital economy.

Thank you for your work on behalf of New Yorkers, and for allowing me to comment on this important issue.

Testimony to Assembly Standing Committee on Consumer Affairs and Protection & Assembly Standing Committee on Science and Technology

Public Hearing: Data Privacy and Consumer Protections

Submitted by: Chelsea Lemon, Senior Director of Government Affairs, October 14, 2025

My name is Chelsea Lemon and I am Senior Director of Government Affairs of The Business Council of New York State, Inc. We are New York's largest statewide employer association, representing 3,200 private sector employers from across New York, in all major business sectors.

We appreciate this opportunity to submit comments for inclusion in the record for today's public hearing on Data Privacy and Consumer Protections as your committees examine potential solutions for ensuring the protection and privacy of consumer data.

The Business Council has the unique perspective of advocating on behalf of New York State businesses that touch every sector of the economy. In that role we consider many voices in the business community and utilize that interaction to advocate for the best possible results for our members, and most of all, the State of New York. We support the passage of reasonable consumer data privacy laws that protect consumers in meaningful ways, but we firmly believe it must be done in a way that does not disrupt businesses' ability to improve consumer access to services and products, or that creates an unnecessary patchwork of laws across the nation that increase operational barriers and compliance costs, which ultimately increase the price of services and goods and threaten New York's economic competitiveness with other states.

In September 2025, the Public Policy Institute of New York State, an affiliate of The Business Council, released *Blueprint for New York – Creating a Roadmap for Change*, a report which analyzed New York's economic competitiveness and business climate compared to other states. It showed that New York was 50th in business friendliness, 50th in both taxation and migration, and 49th in projected working age population growth. Additionally, while our job growth over the past 10 years has grown 7.3%, it is lower than the national average (12%) and one third of growth in Florida (24.9%) or Texas (20.3%).

The report also showed that New York is the second most regulated state, with more than 300,000 regulations. While regulations may address a specific issue or safety concern, excessive regulations often have unintended economic outcomes that are far more detrimental to consumers in the state as they can drive up costs and prices, limit the number of new business opportunities, and reduce the number of jobs available. In addition to being the second most regulated state, New York leads the nation in the amount of legislation filed, with 24,195 pieces of legislation filed in the 2023-24 legislative session, averaging to about 113 bills per member. This is five times the national average (4,610 bills filed per state on average) and

nearly double the second most prolific state, Illinois. The sheer number of regulations and legislative activity makes it next to impossible for businesses to keep up, and the regulatory and legislative uncertainty stifles new investments and innovation.

In addition, qualitative feedback was solicited from businesses from every region across the state during more than 10 in-person roundtables and 12 virtual industry roundtables with more than 300 business leaders and owners participating. While there was optimism about regional collaboration, the quality of public education, and new industry opportunities', especially in life sciences, manufacturing and semiconductor, participants were grim when it came to speaking about New York's cost prohibitive regulatory and legal environment and high cost of doing business.

A statewide survey of more than 550 business leaders showed that only 3% of those polled feel that regulators and lawmakers fully understand and support their business. The poll mirrored the sentiment we heard from businesses during our roundtable meetings: excessive regulations, high taxes, and the overall cost to doing business were the primary barriers to growth.

What does our state's economic competitiveness and business climate have to do with creating a cohesive and effective data privacy framework?

We believe a comprehensive data privacy framework should be addressed in New York in a way that protects consumers but doesn't strangle businesses or expose them to unnecessary compliance or operational costs that disadvantage both businesses and New York consumers. This can be done. We can protect consumers data while at the same time protecting our state's economic competitiveness and improving our business climate.

The Business Council understands that absent a federal framework, more states are acting to implement consumer data privacy laws. We have significant concern that if New York implements a law vastly different from other states, it puts New York businesses and consumers at significant disadvantages that will harm the state's competitiveness. Implementing vastly different data privacy laws from that of other states will introduce substantial compliance and operational roadblocks that will make it even more difficult to do business in New York, thus raising the cost of doing business here. When the cost of doing business is high, the cost of goods and services increases, further impacting affordability.

When California implemented the California Consumer Privacy Act (CCPA), the California Attorney General's office performed a regulatory assessment and found that 75% of California businesses would have to comply, costing businesses $55 billion statewide. The initial cost to comply was significant:

- $50,000 for companies with <20 employees
- $100,000 for companies with 20-100 employees
- $450,000 for companies with 100-500 employees
- $2 million for companies with over 500 employees

We believe that the best way to avoid new, unnecessary compliance and operational costs is to adopt a policy framework that is consistent with the adoption of other neighboring states, like Connecticut. New Jersey also has a similar law to that of Connecticut, and so do Rhode Island and New Hampshire. While each of these states has nuances and can vary in their thresholds and scope, they operate on shared foundations. However, we have concerns about the low thresholds in RI and NH dramatically impacting small and medium sized businesses. Adopting

an approach like Connecticut's framework wouldn't disadvantage New York but would incorporate it into the existing regional framework. Our economies are intertwined; it shouldn't be harder for New York businesses to comply with data privacy laws than our neighboring states.

The Business Council is concerned that if New York pursues its own distinct comprehensive data privacy law, it will create a patchwork of data privacy laws that are inconsistent and

[1] ***Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*** (August 2019). Prepared by Berkeley Economic Advising and Research, LLC for the Attorney General's Office, California Department of Justice.

introduce new operational barriers and compliance costs. This could cut off New York from opportunities to attract growing and emerging industries, like AI.

The Business Council is also concerned by the patchwork that is being created within the state. Before passage of a comprehensive data privacy law, New York has already adopted the New York Child Data Protection Act (2024) and the New York Health Information Privacy Act passed the Legislature this session, though it awaits action of the Governor. There are other pieces of legislation that have put additional requirements on the use of personal data by companies, including the personalized algorithmic pricing law that passed in the FY2026 budget. We support reasonable consumer data privacy laws that protect consumers, especially vulnerable populations like children, but having a comprehensive framework in place prior to the adoption of these other consumer data privacy related bills would have created a foundation to further build upon. Yet, we fear that having these laws in place will complicate the smooth implementation of a comprehensive data privacy bill and will have to be contemplated as part of streamlining a cohesive and comprehensive data privacy law.

A patchwork of laws lends to the burdensome regulatory environment businesses in New York face and make it excruciatingly difficult to navigate. The adoption of a comprehensive data privacy bill should be composed with industry to ensure the most comprehensive and thoughtful outcome, and to avoid unintended (and often negative) economic consequences that would impact both businesses and consumers.

As always, we welcome and appreciate the opportunity to engage in discussions with the Assembly Standing Committees on Consumer Affairs and Protection and Science and Technology and other members of the State Legislature on this and other issues.

Chelsea Lemon
Senior Director of Government Affairs
The Business Council of New York State, Inc.
111 Washington Avenue, Albany, NY 12210
518.694.4462
Chelsea.lemon@bcnys.org

Testimony of Chris Grimm
Connected Commerce Council

Before the NY Assembly Committees on Consumer Affairs & Protection and Science & Technology
Hearing on Data Privacy and Consumer Protections

October 14, 2025

Thank you for giving me the opportunity to testify today on proposed New York data privacy regulations and how they might impact New York small businesses.

My name is Chris Grimm. I'm a policy advisor for the Connected Commerce Council, or 3C — a nonprofit organization dedicated to ensuring that small businesses have the tools they need to compete and succeed in today's digital economy. In the years since our organization was founded, we have met with hundreds of small businesses and dozens of small business consultants regarding the challenges and opportunities presented by the transition from physical to digital commerce and marketing. 3C is supported by Amazon and Google, but our mission is to support small businesses that work with all digital platforms.

Today's top-performing small businesses simultaneously operate online and offline. Restaurants, service providers, manufacturers, and retailers combine physical locations, wholesale relationships, and online platforms to maximize reach, optimize marketing dollars, and lower costs and prices in an effort to win more business and provide a little more for their families, employees, and communities.

As part of the digital small business revolution, companies rely on basic data to reach customers, make smart business decisions, and grow. When states overregulate the collection and use of basic, non-personally identifiable data, like A974 and S8524 would, it becomes much harder for small businesses to succeed.

In their current form, these bills would only allow businesses to collect and use the minimum amount of data necessary to deliver a requested product or service. This radical approach goes further than the current gold-standard privacy laws in California and the EU, which require websites to notify consumers about the data they are going to collect and the purposes for which it will be used; provide a way to opt out of the data collection and use; and limit their data collection to the minimum needed for the stated purposes. The bills also use overbroad definitions that capture far more than data that may contain personally identifiable information. This creates several issues for New York's small businesses, many of whom, such as New York-based EatOkra — an app that connects foodies to Black-owned restaurants — have data on more than 50,000 customers, the threshold for complying with the bills.

First, data allows small businesses to provide the kind of tailored services that customers value and expect. If I buy a tie from Waldorf Tuxedo, just a few blocks from this legislative office building, I'll appreciate it when the shop uses my past-purchase data to tell me that matching shirts are in stock, or that there's a sale on similar ties. There's nothing sinister about that — it's just good customer service. But that would mean using my individual customer data for purposes beyond providing my requested product or service, the purchase of the tie. This use of data, along with many other product recommendations, would be severely limited under A974 and S8524 except for specific instances where customers request this service. Similarly, Fuzi Pasta, a restaurant in Fresh Meadows, would not be able to use location data for customers who order delivery through their website to determine where to open a new location.
Second, there is no question that digital advertising has greatly benefited small businesses,

particularly compared to mass media advertising. It enables the smallest businesses with $100 advertising budgets to compete with global brands. That's because data-powered digital advertising helps small businesses reach the right audiences.

To make digital advertising work, businesses need to collect data about their customers so they can understand their audience and work with digital partners like Google or Facebook to ensure they are only paying for ads that are seen by those most likely to be interested in their products. In addition, these digital partners need to be able to collect data from consumers to ensure they deliver those ads to the right audiences. Without data, digital advertising would be more expensive and less effective, hurting small businesses' ability to compete.

Third, data-powered insights and analytics help small businesses make smarter business decisions. E-commerce engines like Shopify or marketplaces like Etsy provide data-based insights about product performance, customer habits, and more. This is all made possible by data collected and used for more than delivering a customer a requested product or service. In fact, no customer requests that their data be used for these purposes, but they are a fundamental part of what makes the modern internet possible.

Protecting consumers' privacy is important, and I appreciate your efforts to do so. But it's critical that New York balance consumer protections with policies that allow small businesses to continue to grow and succeed. As you move forward with data privacy legislation, I urge you to avoid overregulating data collection and use, overbroad definitions, and carveouts that don't Work.

Several states have passed successful, balanced data privacy laws, including California, Connecticut, Virginia, Colorado, and Oregon. New York's 2.2 million small businesses can't afford to be the canaries in the coal mine for radical, untested laws.

STATE PRIVACY & SECURITY COALITION

October 10, 2025

RE: Joint Public Hearing – Data Privacy and Consumer Protections

Dear Chair Rozic, Chair Otis, and Members of the Committees:

The State Privacy & Security Coalition (SPSC), representing over 30 companies and six trade associations across the retail, telecommunications, technology, automotive, healthcare, and payment card sectors, appreciates the opportunity to provide written testimony to the Assembly Standing Committee on Consumer Affairs and Protection and the Assembly Standing Committee on Science and Technology regarding data privacy and consumer protections in the State of New York. SPSC shares the Committees' commitment to engaging collaboratively with stakeholders to create legislation that achieves meaningful protections for New York consumers while maintaining operational workability for businesses. We are happy to be a resource for these committees given our experience working on state privacy legislation since its inception.

As the Committees continue this important work, we emphasize the critical importance of consistency and interoperability with other state privacy laws (e.g., the national consensus framework). Data privacy laws are inherently complex, and when requirements diverge too sharply across jurisdictions, businesses face significant challenges in implementation. That, in turn, risks creating unintended negative privacy consequences for consumers, including incentives for companies to collect or retain more data than necessary to demonstrate compliance – a particular concern for a state such as New York, with millions of people coming to and visiting New York City on a daily basis. A uniform approach provides clarity for both consumers and businesses and ensures that compliance efforts remain focused on safeguarding privacy rather than navigating conflicting or redundant obligations.

While some media outlets and advocates attempt to paint this issue as one that inherently involves conflict, we believe the story of state privacy legislation is the success of pragmatism and bipartisanship, and would like to take this opportunity to highlight topics of consensus which have allowed this framework to be overwhelmingly adopted, now covering over 100M consumers across 18 states of all political leanings. These include the following:

- Nearly every jurisdiction agrees on the dual principles of **data minimization and purpose limitation**. These concepts are widely accepted, almost entirely universal in their requirements, and essential to consumer trust.
- **Standardized definitions** on what constitutes:
    - Consent; Consumer; Controller; Dark Patterns; Decisions that produce legal or similarly significant effects; Deidentified Data; Personal Data; Precise Geolocation Data; Profiling; Sale of Personal Data; Sensitive Data; and Targeted Advertising.
- **Sensitive data categories** that include reproductive health care, immigration data, precise geolocation data, biometric data used to identify an individual, and racial and sexual orientation data.
- **Heightened protections for sensitive data** that include opt-in consent requirements and documented risk assessments for the type of data referenced above.
- **Consumer rights** to exercise control over personal data and the Homelines and frameworks for responding to those rights requests, including: The right to access

personal data; The right to delete personal data; The right to correct inaccurate personal data; The right to port personal data from one controller to another; The right to opt-out of: § Targeted advertising; § Sale of personal data; and § Profiling in furtherance of automated decisions that produce legal or similarly significant effects.
- **Universal Opt-Out Mechanisms** (UOOM).
- **Loyalty program** provisions.
- **Data Protection Assessments**, which require the documented consideration of risks and benefits to processing particular types of data.
- **Contractual Requirements** between Controllers and Processors that ensures responsibilities are appropriately apportioned between parties.
- **Exemptions for critical operations** such as responding to legal processes, thwarting cybersecurity and consumer fraud threats, preserving the integrity and security of systems, clinical research, warranty recalls, internal development and refinement of products and services, etc.
- **Strong limitations** on how businesses can use data for those exempt purposes.
- **Universal agreement** that the Attorney General is the appropriate enforcement mechanism for privacy violations.

As demonstrated above, the vast majority of concepts in state privacy law have been carefully vetted by work groups, stakeholder sessions, and tireless work by legislators to strike the right balance between consumer protection, consumer demand for products and services, and operational workability for businesses.

Of course, this interoperability relies on ensuring that, for example, UOOM technical requirements do not vary on a state-by-state basis and allow proper time for the technology to mature and for businesses to implement, or that a time-consuming data protection assessment process that can be used in one state can also be used in another.

Finally, as the Committees evaluate the appropriate enforcement structure for any comprehensive law, we urge caution against introducing private rights of action that could invite costly and fragmented litigation without meaningfully advancing consumer privacy. By focusing on workable, interoperable rules, New York can adopt a framework that delivers strong protections while preserving space for innovation, growth, and consumer benefit.

I. THE NATIONAL CONSENSUS ON DATA MINIMIZATION PROVIDES CLEAR LIMITS ON DATA COLLECTION

The principle of data minimization is a foundation of modern privacy protection. It requires organizations to collect and use only the personal information necessary to achieve a clearly defined and legitimate purpose—reducing the risks of overcollection, misuse, and data breaches. By requiring that companies publicly disclose the purposes of data collection, enforcement authorities have a single place to look in order to determine compliance.

Across the United States, the prevailing approach is the standard that personal data collection must be “adequate, relevant, and reasonably necessary” – or some analogous formulation[1] - for the purposes disclosed to the consumer.[2] The framework originates in the Fair Information Practice Principles of the 1970s[3], was modernized in the European Union’s General Data Protection Regulation (GDPR) [4], and has since been widely embraced both globally[5] and domestically. Except for Maryland, every state that has enacted a comprehensive privacy law has adopted this standard, which today protects hundreds of millions of consumers. By requiring a clear, purpose-driven justification for each category of data collected, the framework delivers strong and consistent protections while supporting responsible service delivery and innovation.

As noted above, Maryland recently departed from the consensus by adopting an untested data minimization standard that limits collection to what is "reasonably necessary" to provide or maintain a specific product or service requested by a consumer, or, in the case of sensitive data, what is "strictly necessary." [6] This approach appears to significantly change the scope of data minimization protections and risks undermining consumer interests. Unlike the purpose-and-disclosure-based national model, Maryland's framework is minimization to subjective judgments about what qualifies as a "specifically requested" service, creating uncertainty for routine processing such as product improvement, product recommendations, or system optimization. The law relies on determinations of necessity, which due to its novelty, is likely to result in disparate compliance interpretations.

Critically, the Maryland standard deprives the consumer of the ability to consent to collection and processing of sensitive data. We strongly believe that consent, as universally and robustly defined in the consensus framework, plays a strong part in how companies process sensitive data. Consumers should have the ability to evaluate a product or service and say "no, I don't want you to collect my biometric and precise geolocation data." The Maryland standard removes this important consumer control.

The "disclosed purpose" framework better protects consumers against overcollection. Excessive or poorly justified data collection heightens the risks of misuse and breaches, especially when sensitive data is involved. The proportionality test built into the consensus model requires companies to disclose why data is needed, even when consent has been obtained, and empowers regulators to intervene when data practices exceed legitimate purposes. Maryland's approach leaves gaps by tying minimization too narrowly to the concept of a consumer-requested service.

For these reasons, New York should align with the national consensus and adopt the "disclosed purpose" standard. That approach provides stronger and more consistent protections, clear compliance obligations, and a balanced path that safeguards privacy while enabling innovation.

II. AN INTEROPERABLE FRAMEWORK MAXIMIZES OPERATIONAL WORKABILITY AND MINIMIZES THE ECONOMIC IMPACT OF THIS COMPLEX REGULATION

Since 2021, the rapid and bipartisan enactment of comprehensive state privacy laws has led to increased alignment around the core elements of consumer data protection. Across states, lawmakers have coalesced around consistent and interoperable definitions—such as "personal data," "sale," "biometric data," "consumer health data," "targeted advertising," and "consumer"—as well as shared standards, including individual rights to access, correct, and delete personal data; data minimization obligations; universal opt out mechanisms and requirements to conduct data protection impact assessments for high-risk processing activities. This emerging national model has been shaped through extensive stakeholder collaboration across industry, civil society, and government. For example, Consumer Reports publicly praised Connecticut's comprehensive privacy law when it was enacted, commending the governor and legislature for adopting "a strong law that will extend real privacy protections to its citizens."[7]

New York should build on this national consensus by aligning with widely adopted state frameworks such as those in Connecticut, New Jersey, New Hampshire, Rhode Island, Colorado, Oregon, and Delaware. Any proposal should incorporate consistent terminology, compliance structures, and regulatory expectations already familiar to many businesses. Rather than requiring companies to navigate a patchwork of conflicting rules, adopting the national

model supports the development of interoperable privacy programs that can scale across jurisdictions.

In contrast, state laws that diverge significantly from the national trend impose considerable and well-documented economic burdens. Businesses operating across jurisdictions must adapt compliance programs to accommodate varying definitions, thresholds, and operational obligations. One study by the Information Technology & Innovation Foundation estimated that if all 50 states enacted divergent privacy laws, nationwide compliance costs could exceed $239 billion annually, with $50 billion of those costs falling on small businesses.[8] These costs are not a result of privacy protections themselves, but stem from the complexity and redundancy of meeting inconsistent legal requirements in each state.

California's privacy regime illustrates the scale of these impacts. When the California Consumer Privacy Act (CCPA) first went into effect, the California Department of Justice estimated that initial compliance costs could total up to $55 billion statewide.[9] Small businesses were projected to incur $50,000 in initial costs, while large businesses faced expenses as high as $2 million.[10] Subsequent amendments under the California Privacy Rights Act (CPRA) introduced further obligations— prompting the California Privacy Protection Agency (CPPA) to propose new regulations, including requirements to complete a cybersecurity audit, establish requirements to prepare a risk assessment, and requirements related to businesses' use of automated decision-making technology.[11] According to the CPPA's own economic analysis, first-year compliance with these regulations is expected to cost businesses $4.835 billion. For small businesses, the agency projected initial compliance costs between $6,058 and $36,950, with ongoing annual costs of $15,831. For a typical business, initial costs range from $6,058 to $63,133, with ongoing annual costs of $19,750.[12]

Indeed, small and mid-sized businesses are disproportionately impacted by fragmented privacy laws. Without in-house legal departments, engineering teams, or full-Home compliance staff, these businesses must rely on external vendors and consultants to meet emerging regulatory demands.[13] When state laws impose outlier provisions—for instance, vague and untested data minimization requirements—businesses must often overhaul core systems and processes to meet new obligations for a single jurisdiction.

To comply with diverging requirements, businesses frequently invest in a patchwork of vendor compliance tools—which may include consent management platforms to capture and log user authorizations, universal opt-out signal recognition systems that accommodate browser-based mechanisms like the Global Privacy Control (GPC), and privacy preference portals enabling consumers to modify data use seqngs.[14] Businesses oZen must obtain legal counsel and potentially renegotiate vendor and service contracts to reflect new laws' deviations relating to permissible data use, retention schedules, processing limitations, and liability provisions. [15] Each such change triggers legal review, negotiation cycles, and re-execution—consuming Home, legal resources, and operational bandwidth.[16] Smaller businesses, in particular, face mounting challenges in updating hundreds of third-party agreements while avoiding service interruptions.

By more closely aligning with the consensus framework, New York can avoid the pitfalls of fragmentation and allow businesses to leverage existing internal processes, compliance tools, and vendor contracts already designed to meet similar requirements. For vendors serving clients across multiple states, interoperable obligations reduce the need to create jurisdiction-specific products, lowering both implementation and cost. Alignment with national trends also ensures that New York-based companies are not placed at a competitive disadvantage compared to peers operating in states with clearer and more consistent laws.

Uniformity further promotes accountability and compliance. When businesses clearly understand their obligations—and can implement them without unnecessary operational disruption—they are more likely to comply, regulators can more effectively enforce, and consumers benefit from more consistent protections. By following the dominant structure of existing state laws, New York can provide meaningful safeguards while minimizing legal uncertainty. This approach ensures cost-effective compliance and protects consumers without placing undue strain on the business community, particularly small and mid-sized enterprises that form the backbone of the state's economy.

III. NATIONAL PRIVACY STANDARDS PROVIDE CLEAR, HIGH-IMPACT SAFEGUARDS FOR SENSITIVE DATA

Modern privacy laws across the country recognize that certain categories of personal information warrant heightened protection because of their sensitivity and potential for misuse. The national consensus model, therefore, establishes increased safeguards for precise geolocation data, reproductive and gender-affirming health data, and biometric data. These protections are built on strict consent requirements, prohibitions on exploitative practices, and clear consumer rights that together ensure trust, accountability, and consistency.

- ***Geolocation Data Protections***: The processing of precise geolocaHon data provides a wide range of public interest and consumer uses. It can also be used to reveal highly intimate details about where people live, work, and seek medical care. State privacy laws balance these interests by designating such information as sensitive and requiring opt-in consent before it can be collected or used, ensuring that location tracking cannot occur passively or without consumer awareness. Several states also prohibit the use of geofencing near reproductive or sexual health facilities for purposes of identifying individuals, collecting their data, or sending targeted outreach relating to such sensitive data. These measures empower consumers to control whether their movements are tracked and prevent the use of locaHon data in ways that could expose private health decisions or subject individuals to profiling and surveillance.
- ***Protections for Reproductive and Gender-Affirming Care Data***: In the post-*Dobbs* era, some states have prioritized reproductive and gender-affirming health data to receive the highest level of protection. State laws require explicit, opt-in consent before this information can be collected, transferred, or sold, and have clear definitions to regulate high-risk use of this information (i.e., use for the purpose of identifying an individual). Coupled with restrictions on geofencing around health facilities, these measures guarantee that consumers maintain control over sensitive health data.
- ***Biometric Data Protections***: Biometric data used to identify a specific individual—such as fingerprints, voiceprints, and iris scans—is consistently treated as sensitive data under the national model. Controllers must obtain explicit consent before processing such biometric data, ensuring consumers retain control over the use of these deeply personal markers. At the same time, laws avoid overregulating common technologies like photographs, audio, or video recordings to avoid conflating sensitive biometric data with these common data types. States also provide explicit exemptions allowing the use of data for cybersecurity and fraud prevention purposes, thereby preserving beneficial applications such as secure authenHcaHon and account protecHon. This dual approach balances consumer protecHon with innovaHon and security.

Importantly, these heightened protections for sensitive data work in tandem with baseline consumer rights that apply to all personal data. Individuals retain the rights to access, delete, and correct their information, as well as to transfer it between companies. When combined with explicit consent requirements and restrictions on exploitative practices, these rights ensure that consumers remain in control of their sensitive data across all contexts.

Taken together, these targeted safeguards reflect the national consensus that sensitive data requires the strongest protections. They deliver consistent standards across states, protect consumers against the most serious privacy harms, and provide regulators and businesses with workable rules.

IV. STATE ATTORNEYS GENERAL ARE BEST SUITED TO BRING ENFORCEMENT ACTIONS FOR VIOLATIONS OF STATE COMPREHENSIVE DATA PRIVACY LAWS

With respect to enforcement, every state comprehensive law vests exclusive authority in the Attorney General, authorizes civil penalties under state law, and does not create a private right of acHon (PRA). This framework provides a balanced approach to accountability without inviting unnecessary or fragmented litigation.

Attorney General enforcement promotes consistent legal interpretation, centralized expertise, and public accountability. State AGs have already demonstrated their capacity to deliver meaningful outcomes—including California's $1.2 million CCPA settlement with Sephora[17] and the first-ever enforcement action under Texas's new Data Privacy and Security Act.[18] Filed in January 2025, the case alleged that a company collected and sold sensitive geolocation and behavioral data from consumers without proper notice or consent.[19] As the latest legal action brought under a state's comprehensive privacy law, the case illustrates how AGs can act swiftly to address emerging data practices and reinforce compliance obligations. These enforcement efforts not only hold violators accountable but also help establish market-wide norms for transparency, user control, and responsible data use.

a. Early Enforcement in Peer States Highlights the Strength of AG Oversight

Connecticut and Oregon have demonstrated how centralized Attorney General enforcement provides timely, effective consumer protection under comprehensive privacy laws. In the first six months following the effective date of the Connecticut Data Privacy Act, the Office of the Attorney General received more than 30 consumer complaints, issued over a dozen notices of violaHon, and reported that most companies resolved the identified issues promptly after being contacted by the AG.[20] Oregon's Department of Justice received 110 consumer complaints during the same initial period and opened 21 formal enforcement managers.[21] Each of those matters was resolved through voluntary remediation, resulting in stronger privacy notices, improved rights mechanisms, and greater overall transparency for consumers across the state. These outcomes illustrate the effectiveness of centralized enforcement in driving rapid compliance and protecting not only the individuals who file complaints, but the broader public as well.

b. Dedicated Privacy Units and Enforcement Resources Drive Long-Term Results

Strong Attorney General enforcement depends on proper resourcing, and several states have taken meaningful steps to institutionalize privacy within their offices. Oregon, for example, created a dedicated Privacy Unit within the Department of Justice, staffed with attorneys and

policy experts focused exclusively on enforcing the state's Consumer Privacy Act. [22] Virginia established a Consumer Privacy Fund, channeling civil penalties into a dedicated account that supports enforcement and public education. [23] New York could consider similar structures to ensure its enforcement regime is rigorous, sustainable, and grounded in subject-matter expertise while remaining responsive to evolving technologies and business models.

Additionally, state regulators have formalized interstate collaboration through the *Consortium of Privacy Regulators*, which now includes the California Privacy Protection Agency and Attorneys General from states such as Colorado, Connecticut, Delaware, Indiana, New Jersey, Oregon, Minnesota, and New Hampshire.[24] This multistate consortium is designed to coordinate investigations, align enforcement priorities, and share technical expertise, strengthening both individual states' capacity and national consistency in enforcement.[25] New York could consider not only adopting internal mechanisms like a dedicated privacy unit or enforcement fund, but also joining this consortium to ensure its enforcement regime is rigorous, sustainable, and grounded in subject-maker expertise while remaining responsive to evolving technologies and business models.

c. Cure Provisions Promote Compliance and Reserve Resources for Bad Actors

Many states also provide a right to cure alleged violations. Under this model, when the Attorney General determines that a violation can be remedied, the office may issue a notice and allow a specific window for resolution. Experience in other states demonstrates that cure provisions are highly effective. In California, the Attorney General reported that 75 percent of businesses receiving cure notices came into compliance within the prescribed period, and the remainder either came into compliance shortly thereafter or became subject to a full investigation. [26] In Oregon, all 21 businesses that received cure letters corrected their practices within the cure period,[27] and Connecticut has reported similarly high rates of cooperation. [28] By promoting remediation before escalation, cure provisions deliver faster, more direct relief to consumers and ensure that enforcement resources are used efficiently. They also provide flexibility for the Attorney General, who can determine whether a violation is so serious that cure is inappropriate, or instead resolve issues quickly by requiring corrective action without the need for a full investigation.

d. Private Rights of Action Fail to Provide Consumers with Meaningful Benefits

The introduction of a PRA would significantly increase litigation, discourage beneficial uses of biometric data, and impose compliance burdens that extend beyond established national privacy standards. While strong consumer privacy protections are essential, a broad PRA goes too far, following the path of Illinois' Biometric Information Privacy Act (BIPA)—which has resulted in excessive lawsuits, heightened costs for businesses, and reduced access to consumer services.

A private right of action would create widespread exposure to class action litigation for any alleged violaHons, resulting in a broad chilling effect on the use of data to power products and services consumers rely on every day, including the potential removal of services from the state altogether. Illinois' experience with BIPA serves as a warning. Since 2018, more than 2,000 lawsuits have been filed under BIPA, with trial lawyers exploring minor technical violations rather than addressing substantive consumer harms.[29] The cost of defending these lawsuits averages $500,000 per case, forcing many businesses—regardless of compliance—to settle rather than endure protracted litigation.[30] This environment has led companies to limit or withdraw services that rely on biometric technology, depriving consumers of security-enhancing tools. Recognizing these consequences, Illinois lawmakers amended BIPA in 2024 to reduce the prospect of ruinous damage awards by limiting liability to a single violaHon per person instead of per transaction.[31]

Similar litigation has emerged in other states. In California, plaintiffs have increasingly leveraged the state's Invasion of Privacy Act (CIPA) to bring lawsuits against website operators, small businesses, non-profits and more for using routine analytics technologies—alleging wiretapping violaHons in the absence of express notice or consent.[31] In New Jersey, ongoing lawsuits under Daniel's Law have implicated hundreds of online service providers that publish *publicly available* property records and personal contact information.[32] In short, these trends highlight how unchecked private rights of action can fuel litigation abuse, undermine regulatory clarity, and discourage the availability of lawful, consumer-facing services.

Finally, class action lawsuits have repeatedly failed to deliver meaningful consumer relief. A Consumer Financial Protection Bureau study found that in 87% of resolved class acHons, absent class members received no benefit—either because the case was dismissed or the settlement compensated only named plainHffs. [33] Even when monetary awards were issued, the majority of funds went to attorneys rather than affected consumers.[34] In contrast, New York's Attorney General already has robust enforcement authority under the state's Consumer Protection Act, making a private right of action unnecessary. ***If enacted, a PRA would primarily benefit trial lawyers while offering liOle real protection to consumers. New York should, therefore, align with every other state in the country with a comprehensive privacy law, and elect to provide Attorney General enforcement over private lawsuits.***

* * * *

As stated above, SPSC appreciates the Committee's thoughtful engagement and shares its goal of advancing strong, workable privacy protections for New York consumers. We believe the national model provides the most balanced and effective path forward—delivering robust safeguards for sensitive data, a clear and flexible data minimization standard, and a proven enforcement framework grounded in Attorney General oversight. By aligning with the consensus approach adopted in other states, New York can ensure meaningful consumer protections while minimizing compliance burdens and regulatory fragmentation. We respectfully urge the Committee to align with this national model and welcome the opportunity to continue working collaboratively to refine and implement strong privacy legislation.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition

William C. Martinez
Counsel, State Privacy & Security Coalition

---

[1] California and Connec-cut both add onto the "disclosed purpose" standard a requirement that data collec-on and processing prac-ces must accord with a consumer's reasonable expecta-ons. See Cal. Code Regs. -t. 11, § 7002(c)(3) (2025), hIps://govt.westlaw.com/calregs/Document/I7C5D69409E0F11F09C6BF97E55B516E3; Conn. Pub. Act No. 25-113, § 9(a)(3)(i) (2025), hIps://www.cga.ct.gov/2025/ACT/PA/PDF/2025PA-00113-R00SB-01295PA.PDF.

[2] See *US State Comprehensive Privacy Laws Report: 2024 Legisla=ve Session*, IAPP (Oct. 2024) ("All state laws also include some kind of requirement to limit the collec-on and/or processing of data. The data minimization clauses typically require regulated en-es to ensure the collec-on, use, reten-on and sharing of a consumer's personal informa-on is limited to what is 'adequate, relevant, and reasonably necessary' and that it is propor-onate to achieving the purposes for which it was collected or processed."), hIps://iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2024_session.pdf.

[3] See Cheryl Saniuk-Heinig, *50 Years and Sell Kicking: An Examination of FIPPs in Modern Regula=on*, IAPP

(May 25, 2021), hlps://iapp.org/news/a/50-years-and-s-ll-kicking-an-examina-on-of-fipps-in-modern-regula-on.
[4] See Art. 5 GDPR, *Principles rela=ng to processing of personal data* ("Personal data shall be: adequate, relevant and limited to what is necessary in rela-on to the purposes for which they are processed."), hlps://gdprinfo.eu/art-5-gdpr/.
[5] See, e.g., Bill C-27, 1st Sess., 44th Parl., § 12(2) (Can. 2022) ("An organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances."), hlps://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading; Brazilian General Data Protec-on Law, IAPP (Oct. 2020) ("Necessity: limitation of processing to the minimum necessary to achieve its purposes, covering relevant, propor-onal, and not excessive data."), hlps://iapp.org/resources/ar-cle/braziliandata-protec-on-law-lgpd-english-transla-on/; Act on the Protec-on of Personal Informa-on, Act No. 57 of 2003, art. 16 (Japan 2003) ("A personal information handling business operator shall not handle personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve a ulization purpose specified pursuant to the provisions under the preceding Ar-cle."), hlps://www.ppc.go.jp/files/pdf/APPI_english.pdf.
[6] See S.B. 541, 2024 Gen. Assemb., Reg. Sess. § 14–4607(B)(1)(i) (Md. 2024), hlps://mgaleg.maryland.gov/2024RS/bills/sb/sb0541f.pdf.
[7] See Jus-n Brookman, *Connecticut governor signs comprehensive privacy bill into law*, CONSUMER REPORTS (May 11, 2022) ("Consumer Reports praised the governor and legislature for approving the bill."), hlps://advocacy.consumerreports.org/press_release/connec-cut-governor-signs-comprehensive-privacy-bill-intolaw/.
[8] See Ash Johnson, *The Impending Patchwork of Privacy Is Bad for Business and Consumers*, INFO. TECH. & INNOVATION FOUND. (Mar. 27, 2023), hlps://i-f.org/publica-ons/2023/03/27/the-impending-patchwork-of-privacy-is-bad-forbusiness-and-consumers/.
[9] See *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, CAL. DEP'T OF JUST. (Aug. 2019), hlps://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.
[10] *Id.*
[11] See *Standardized Regulatory Impact Assessment: California Privacy Protection Agency*, CAL. PRIVACY PROT. AGENCY (Oct. 2024), hlps://cppa.ca.gov/regula-ons/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf.
[12] See California Privacy Protection Agency, *Final Statement of Reasons: CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations* (Sept. 2025) hlps://cppa.ca.gov/regula-ons/pdf/ccpa_updates_cyber_risk_admt_fsor_and_uid.pdf.
[13] See Daniel Castro, et. al., *The Looming Cost of a Patchwork of State Privacy Laws*, INFO. TECH. & INNOVATION FOUND. (Jan. 24, 2022), hlps://i-f.org/publica-ons/2022/01/24/looming-cost-patchwork-state-privacy-laws/ ("[T]he costs associated with data privacy laws adversely affect small businesses, none more so than their larger counterparts, because the high costs represent a larger propor-on of their revenue. Larger firms are also more likely to have inhouse regulatory exper-se and to be in compliance with privacy laws outside the United States.").
[14] See, e.g., Samuel Adams, et. al., *Survey of Current Universal Opt-Out Mechanisms*, FUTURE OF PRIVACY FORUM (Oct. 12, 2023), hlps://fpf.org/blog/survey-of-current-universal-opt-out-mechanisms/.
[15] See, e.g., *IAPP-Bloomberg Law Privacy Tech Vendor Report*, IAPP & BLOOMBERG L. 2 (April 2016), hlps://iapp.org/media/pdf/resource_center/IAPP_Bloomberg_externalCounsel-finalforprint-032516.pdf ("We found that a significant percentage of corporate respondents — 76 percent — are currently using outside counsel for privacy and data security malers, with nearly two-thirds employing them as needed (63 percent), and an addi-onal 13 percent on a retainer basis."); see also *id*. at 3 ("Tasks outside lawyers are most often hired to perform are log-on, draining and reviewing contracts and vendor agreements, interacting with regulators, and assisting with trans-border data transfer transactions.")
[16] See, e.g., *Privacy Governance Report 2024*, IAPP, at 15 (Nov. 2024) (no-ng in 2023, respondent companies across industries engaged in 5,588 vendor-related privacy reviews), hlps://iapp.org/media/pdf/resource_center/IAPP_Governance_Report_2024.pdf.
[17] See *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, CAL. DEP'T OF JUST. (Aug. 24, 2022), hlps://oag.ca.gov/news/press-releases/alorney-generalbonta-announces-sellement-sephora-part-ongoing-enforc

ement.
[18] See F. Paul Pitmann, et. al., *Texas Attorney General's Landmark Privacy Lawsuit Signals New Era in Data Privacy Enforcement*, WHITE & CASE (Feb. 3, 2025), hlps://www.whitecase.com/insight-alert/texas-alorney-generalslandmark-privacy-lawsuit-signals-new-era-data-privacy.
[19] *Id*.
[20] See *Report To The General Assembly's General Law Committee*, CONN. OFF. OF ATT'Y GEN. (Feb. 1, 2024), hlps://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf.
[21] See *Enforcement Report: The Oregon Consumer Privacy Act (2024), The First Six Months*, OR. DEP'T OF JUST. (Mar. 2025), hlps://www.doj.state.or.us/wp-content/uploads/2025/03/OCPA-Six-Month-Enforcement-Report.pdf.
[22] *Id*.
[23] See Va. Code Ann. § 59.1-584(C) ("All civil penal-es, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Regulatory, Consumer Advocacy, Li-ga-on, and Enforcement Revolving Trust Fund.").
[24] See *Minnesota and New Hampshire Join Consortium of State Privacy Regulators*, CAL. PRIVACY PROT. AGENCY (Oct. 8, 2025), hlps://cppa.ca.gov/announcements/2025/20251008.html.
[25] See Skadden, Arps, Slate, Meagher & Flom LLP, *Eight-State Consortium of Privacy Regulators Marks Shi' Toward Coordinated Enforcement*, SKADDEN (May 2, 2025), hlps://www.skadden.com/insights/publica-ons/2025/05/eightstate-consor-um-of-privacy-regulators-marks-shin.
[26] See Joe Duball, *California attorney general offers CCPA enforcement update, launches repor=ng tool*, IAPP (July 20, 2021), hlps://iapp.org/news/a/california-alorney-general-offer-ccpa-enforcement-update-launches-repor-ngtool.
[27] See *Enforcement Report: The Oregon Consumer Privacy Act (2024), The First Six Months, supra.*
[28] See *Report To The General Assembly's General Law Committee*, *supra*.
[29] Lisa Burden, *Companies hit with class ac=ons under Illinois biometric data law*, LEGALDIVE (Nov. 8, 2023), LEGALDIVE (Nov. 8, 2023), hlps://www.legaldive.com/news/class-ac-on-lawsuits-illinois-biometric-data-law-privacycorporate-counsel-law-arent-fox-freeman/699258/.
[30] See, e.g., *Biometrics bill takes on a life of its own*, MAINE STATE CHAMBER OF COMMERCE (June 9, 2022), hlps://www.mainechamber.org/mscc-blog/biometrics-bill-takes-on-a-life-of-its-own; Steve Korris, *AbboX EMS sells BIPA class action for nearly $500,000*, MADISON-ST. CLAIR RECORD (Sept. 6, 2023), hlps://madisonrecord.com/stories/649508206-abbol-ems-selles-bipa-class-ac-on-for-nearly-500-000. [31] See *A'er 16 years, BIPA is amended to limit poten=al damages for viola=ons*, JDSUPRA (Aug. 30, 2024), hlps://www.jdsupra.com/legalnews/aner-16-years-bipa-is-amended-to-limit-9943997/
[31] See Michael J. Stortz, *Pen Register and Trap and Trace Claims: The Latest Wave of CIPA Litigation*, K&L GATES (March 4, 2024), hlps://www.klgates.com/Pen-Register-and-Trap-and-Trace-Claims-The-Latest-Wave-of-CIPALi-ga-on-3-4-2024.
[32] See *Daniel's Law and the Explosion of Privacy Claims Impac=ng Real Estate and Tech Platforms*, THOMPSON HINE (Mar. 12, 2024), hlps://www.thompsonhine.com/insights/daniels-law-and-the-explosion-of-privacy-claimsimpac-ng-real-estate-and-tech-platorms/.
[33] See Consumer Fin. Protection Bureau, *Arbitration Study: Report to Congress 2015*, at sec-on 6, p. 37 (2015), hlps://files.consumerfinance.gov/f/201503_cfpb_arbitra-on-study-report-to-congress-2015.pdf.
[34] *Id*.

RETAIL COUNCIL OF NEW YORK STATE
RESULTS FOR TODAY'S RETAILERS

Testimony on behalf of the Retail Council of New York State New York State Assembly Public Hearing Data Privacy and Consumer Protection

October 14, 2025

Testimony submitted by:

Kelsey Dorado Bobersky Director of State and Local Government Relations, Retail Council of New York State

Chair Rozic and honorable committee members:

Thank you for the opportunity to provide testimony related to data privacy and consumer protection.

My name is Kelsey Dorado Bobersky; I am the Director of State and Local Government Relations for the Retail Council of New York State. Our organization is the state's leading trade group for the retail industry, representing thousands of stores ranging from the smallest independent merchants to national and international brands.

Despite the rapid transformation of the retail ecosystem, retailers' core business remains straightforward: to sell products and services to customers. To do so, retailers have always sought to know their customers well in order to serve them better. Today's consumers expect a seamless experience across all channels, and while methods and technologies may have changed over the years, we are guided by one simple purpose: to better serve our customers.

Retailers have leveraged new technologies to meet customer expectations for personalization and a seamless experience between mobile, online and in-store shopping. Digital mobile technology has enabled retailers to innovate at a greater speed to meet the demands of consumers and, today, shoppers have come to expect that level of service.

The Retail Council of New York State has been constructive on the issue of consumer privacy and data protection for years. Main Street businesses take this issue seriously for a variety of reasons, and fully understand that if a customer's information is compromised, they will shop elsewhere. Legislative solutions that protect an individual's personal information should be transparent for consumers and extend obligations to all businesses that handle personal data to ensure comprehensive protection. Businesses using personal data should inform consumers of the categories of personal information they collect, how that data is used, and enable consumers to correct and delete their information. In our view, there is a way to promote consumer privacy and protection, while also maintaining the benefits and services that customers currently enjoy in their relationships with retailers.

From our perspective, there are six critical elements that are important to consider when drafting state privacy laws.

Fair enforcement and no private right of action

The retail industry is categorically opposed to private rights of action as an enforcement mechanism for state privacy laws. Instead, retailers support enforcement by the attorney general so that the interpretation and enforcement of privacy laws can be consistently applied across the state based on cases of actual harm. The attorney general has prosecutorial discretion and is not motivated by personal remuneration in the decision to bring litigation. In addition, we support provisions that will provide a reasonable opportunity for businesses to cure any deficiency in compliance before facing enforcement.

Main Street retailers are often the ones targeted by frivolous lawsuits. These businesses have neither in-house counsel nor abundant resources to acquire expert legal help to defend themselves, often leading to settlements that line the pockets of the trial lawyers with little benefit to consumers. There is a significant risk that a private right of action tied to a state privacy law will lead to a new cottage industry of "privacy trolls."

Statutory obligations for all

Retailers believe that all businesses handling personal information should have direct, statutory obligations to protect that information and honor consumers' rights with respect to it, including processing consumer rights requests. We do not support exemptions for businesses that have no other equivalent federal or state privacy obligations to protect data, such as the obligations provided by the Health Insurance Portability and Accountability Act (HIPAA) and state laws covering protected health information. For example, some industry-specific federal laws are over twenty years old and do not provide 21 st-century privacy protections, such as access, correction and deletion rights. Businesses in those sectors that are subject only to those federal laws should be subject to the same requirements as other businesses under state privacy laws, wherever the state law exceeds the standards of the federal law for the same use of data.

Sole responsibility should not fall on consumer-facing companies, like retailers, to supervise downstream data use. Retailers will often be the first point of contact for customers about their personal information, but third parties and service providers handling their personal information should have equivalent statutory responsibility for their actions and fulfilling consumer rights requests.

Preserve customer service, convenience and benefits

Retailers should not be prohibited from offering different prices, rates, levels or qualities, of goods or services in the context of a customer loyalty program. Loyalty programs should not be defined as "financial incentives" and cannot be arbitrarily valuated by state-required mechanisms. Consumers voluntarily participate in loyalty programs and provide personal information so that they may earn benefits and discounts. A 2024 Forrester research study shows that 90% of online United States adults participated in at least one loyalty program [1]. State laws should not make illegal the types of voluntary programs that consumers enjoy. Proposed privacy legislation that potentially puts loyalty plans at risk often appear as a provision called "nondiscrimination," in which the bill text prohibits treating customers who exercise privacy rights differently in terms of price or service. In legislation with a

[1] Pedini, John. "Consumers Clays More th_ay Discounts f_i-onaLovaltv Præram_s." Forrester, 24 Jan. 2025.

nondiscrimination provision, a safe harbor will be required to preserve loyalty programs, discounts, coupons, club cards and related programs used by retailers. However, as noted above, safe harbors based upon data-valuation tests do not work (e.g., "California Consumer Privacy Act" model), and the safe harbor language to protect loyalty and related programs will need to be carefully crafted based on the language used in the nondiscrimination provision of a particular state's privacy bill.

Loyalty programs are typically offered free of charge and help bolster a relationship between a customer and the brand. It also ensures that brands can personalize and offer the best products that a consumer wants and needs — and when a customer no longer desires personalized advertisements, they should be empowered to opt out.

Implement a risk-based approach

Retailers believe in a risk-based approach to privacy regulation. This begins with a core definition of sensitive personal information that is clearly linked to areas where there is a real risk of tangible harm. Creating a scope that allows companies to draw well-defined boundaries around truly sensitive personal information while enabling non-sensitive data to be used to benefit customers is vital to having a functioning privacy regulatory framework.

Legislation must not unnecessarily expand what data would be considered "personal information." It should exempt de-identified or aggregated data as well as exclude any data that would constitute employee data or business-to-business data, where the latter includes data sharing that facilitates transactions between businesses.

Consumer rights and protections

Retailers believe in providing consumers with reasonable choice, access, correction, and deletion rights over their personal information. But which controls to offer, when to offer them, and how they are offered should depend on context.

For example, a transaction that includes delivery necessarily includes the transmission of a customer's address to the third-party delivery service. The context of this transaction should not require consent because transferring address information is necessary to meet the customer's desire for delivery.

There are many more data use cases in the retail context, such as accepting payment cards for processing, or providing warranty information or other benefits associated with a purchase. The key is meeting consumers' expectations with respect to the data use. Personal information used responsibly to meet consumer expectations should not be prohibited or regulated in ways that hinder the consumer shopping experience.

A privacy approach that evaluates data use in context better addresses the business models and uses of data in the marketplace today, rather than relying on foundational consent models alone.

Flexible and secure compliance measures for customers

Retailers support privacy legislation that recognizes that the channel or medium through which customers and businesses interact with each other, including physical locations, must be considered in designing compliant consumer privacy notifications and methods for businesses' secure receipt of consumer rights requests. This would ensure that both the privacy and security

of those communications, and the timely processing of customer rights requests, are achieved in the manner most appropriate for each context.

Taking requests in-store will mean creating new verification procedures, which could pose additional security risks. Furthermore, there are challenges to maintaining ongoing additional training for in-store employees who already have significant mandatory training requirements and for whom it may be difficult to execute complicated compliance requirements because of tumover and the seasonal nature of the business. This is especially true in industry sectors like retail, which employ many seasonal or temporary employees at peak times of business for very short periods of time, making training or additional matters trying.

Requiring in-store requests also imposes disproportionate obligations on brick-and-mortar stores, whose data processing is typically of low risk compared to big tech companies and systems (other than those designed to process payment card information) and may not be designed to facilitate processing personal information.

Thank you again for the opportunity to provide testimony on this important issue. We will continue to remain constructive throughout the legislative process.

Respectfully submitted,

Kelsey Dorado Bobersky
Director of State and Local Government Relations
Retail Council of New York State
kelseydorado@rcnys.com

Testimony for the New York Assembly Standing Committee on Consumer Affairs and Protection, and Assembly Standing Committee on Science and Technology October 14, 2025

Good morning, Chair and distinguished members of the Committee. Thank you for the opportunity to speak today on an issue of fundamental importance to all New Yorkers: data privacy and protections, especially for our children.

Testimony on a New York Data Privacy Framework

In the 21st century, the digital world is no longer just a marketplace of data; it is the environment where our children live, learn, and grow. While this ecosystem powers innovation, it has been built on opaque data management, rampant data collection policies, and a near-total lack of critical oversight. Generative AI and algorithmic systems now use this data in unforeseen ways, posing unique and serious threats to the safety and developmental health of our youngest citizens. Threats such as chatbot-initiated manipulation and emotional addiction, the misuse of deepfakes to create child pornography, and the mining of data to enhance and target unsolicited products and services.

I am here today on behalf of the Transparency Coalition, a group of non-partisan extechnologists working for the public good, to advocate for targeted policies that establish data privacy and online safety as fundamental rights for all New Yorkers, with an unwavering focus on protecting our children. New York has the opportunity to lead the nation by expanding on the important work done to date, and enacting legislation that prioritizes the well-being of its most vulnerable residents, the children of New York State. We recommend focusing on these six critical areas that establish a Child-First Privacy Framework:

1. Establish a Heightened Data Fiduciary Duty

Enact legislation defining entities that control personal data as "data fiduciaries." This status must impose a statutory duty of loyalty, care, and confidentiality toward individuals, with the highest obligations applied to data from children and teens. This would legally obligate platforms to act in the best interests of young users, prohibiting the use of their data in ways that are manipulative, discriminatory, or harmful to their mental and physical well-being. The burden must be on the company to prove their data practices benefit the child, not their bottom line.

2. Make Child Safety the Default, Not an Opt-In

We must move beyond a simple consent model where children are concerned. We advocate for a "Safety by Design" mandate that establishes the highest level of privacy and safety as the default setting for any user reasonably likely to be a minor. This includes:

• Banning surveillance advertising targeted at users under 18.

• Prohibiting the use of manipulative design features such as infinite scroll and auto-play that prioritize engagement over a child’s well-being, or behaviors designed specifically to mimic real people, their emotions, and personas, and using these features to create emotional engagement and intimacy.

• Making the strong protections in the New York Child Data Protection Act (NYCDPA) the baseline for all

services, not a separate standard.

3. Create a Privacy Protection Agency with Teeth

To ensure these rights are meaningful, New York should establish a dedicated privacy protection agency, similar to California's CPPA. Crucially, this agency must include a wellfunded division specifically focused on Youth Privacy and Safety. This division would be staffed with experts in child development and technology who can investigate harms, conduct audits of platforms, and create and enforce robust, state-of-the-art rules to protect children online.

4. Empower Parents with a Targeted Private Right of Action

Allow New Yorkers—and specifically empower parents and guardians on behalf of their children—to sue companies for significant harms. This right should be triggered by data breaches of sensitive information, the illegal processing of a child's data, or a platform's intentional use of design features that cause demonstrable harm to a minor. This provides a powerful deterrent and a path to justice for families. 5. Mandate "Safety and Privacy by Design" Legislation must require companies to build safety and privacy into their products from the very beginning. This includes mandating that companies conduct and publish independent Child Safety Impact Assessments before launching new products or features likely to be accessed by minors. This should not just apply to generative AI tools such as chatbots; it should include ANY AI product or platform that interacts with, and acquires data from, a child. This includes any AI used in educational and entertainment settings. This shifts the burden from the consumer to the company to prove their platforms are safe before they can cause harm. Data collection must be strictly limited to what is justifiable and necessary for the core function of the service.

6. Demand Algorithmic and Data Transparency

Finally, true safety is impossible without transparency. The law must require platforms to provide clear, understandable explanations of how their algorithms use children's data for content recommendation, moderation, and other profiling. This transparency is essential for researchers, parents, and regulators to understand and mitigate the risks of addiction, mental health issues, and exposure to harmful content.

By taking these steps, you can create a legal framework that places meaningful controls on how platforms acquire, manage, and use our children's data. You can build on New York's important work to create a digital world built on trust, transparency, and a fundamental respect for the next generation.

ALICIA ABRAMSON
CIVIL RIGHTS INTERN, Surveillance Technology Oversight (STOP) Project

Today's digital world has created a sweeping system of data collection and exploitation that profits off of the personal data of individuals. An alarming lack of privacy protections leaves corporations and data brokers free to collect as much highly sensitive personal data as they wish without facing consequences, fueling a lucrative industry based in the eradication of digital privacy. Data has become a commodity; companies gather as much data as they can from consumers, all to monetize and sell off to the highest bidder.

Corporations are increasingly capable of extracting information from every aspect of our lives, information that is then repackaged and sold without our consent or knowledge. Every click, every swipe, every like contributes to a vast store of information. These millions of data points are sold and combined to create comprehensive and deeply invasive profiles of consumers that reveal a massive amount of personal information, from sexual orientation to religious beliefs to health status. Extensive data collection brings heightened privacy risks: security breaches, identity theft, physical harm, data-driven discrimination, law enforcement overreach.

1. Unnecessary data collection puts people seeking abortions and gender-affirming care at greater risk, as reproductive health data from period tracking apps, online searches for contraceptives, or location data from a trip to an abortion clinic can all be collected and sold to advertisers, law enforcement, or other data brokers. 2 It threatens the privacy and safety of victims of harm, making it easier for abusers to find and stalk them. It leads to discrimination in every field imaginable — health insurance companies can use data to determine healthcare rates,3 landlords can use personal data to discriminate in housing,4 governments can use data to decide who receives welfare benefits.5 Anything and everything you do online can be tracked, aggregated, misused, and potentially exposed.

Nineteen states have passed laws that aim to curb this practice, but they fail to enact meaningful privacy protections, leaving excessive data collection unchecked.

The New York Privacy Act (S.3044 Gonzalez / A.8158 Rozic) follows this model, which is why it should be rejected. It is a bill that serves corporations, not consumers. Corporations advocate for an opt-out model because they know that it allows them to continue collecting and monetizing our personal data — but we do not need to let this model become the standard. Since there is no comprehensive privacy law at the federal level, a patchwork approach has taken its place, and the opt-out framework has proliferated due to corporate lobbying and tech platforms oversized influence in privacy legislation. New York has the chance to become a national leader and set a new standard for data privacy. But if the New York Privacy Act is passed, the opt-out framework and its lack of any real protections will become entrenched; it will become the national standard and be nearly impossible to change. No one will be protected online for the foreseeable future.

The Digital Fairness Act (S.2476-2025-26 Kavanagh / A.3308-2204-25 Cruz) offers stronger protections. It operates on an opt-in model, meaning that the default assumption is that data may not be collected or processed unless a user affirmatively consents to such collection. This would be a real positive difference and lead to far less unnecessary data collection, reducing security and privacy risks. S.T.O.P. supports the Digital Fairness Act and urges the legislature to pass it.

Even so, the opt-in model is not the strongest alternative available. Think about how many different websites a person visits in just one day – do you really want to read through a privacy notice for each one and figure out if you want to consent to that data collection? Many users will be under the assumption that they have to consent to data collection in order to use the service. Just like with cookie pop-ups, most people will opt in simply because it's easier.

The onus should not be on the consumer to navigate confusing privacy terms. The majority of people do not understand how their data is being used, and they shouldn't have to develop an encyclopedic understanding of the data economy just to access baseline privacy protections. Privacy should be the default. This is why, instead of "opt-in" or "opt-out," the Surveillance Technology Oversight Projects supports a data minimization framework, the gold standard for privacy protections.8 If New York wants to raise the bar and fundamentally change the way we think about digital privacy, we need data minimization as the pillar of a state privacy law. Data minimization limits the amount of data companies are allowed to collect in the first place to what is necessary to provide the requested product or service. It makes privacy the default and places the burden on companies rather than consumers.

A privacy law based on data minimization will genuinely protect individuals online, from both a privacy and security standpoint.9 When companies collect massive amounts of data, data breaches can be devastating and reveal deeply sensitive and personal information. Similarly, the federal government can subpoena a limitless amount of information about each New Yorker, and use it against people on the basis of their healthcare decisions, religious beliefs, or political opinions. But under data minimization, data breaches and federal overreach cause less damage because there is less data to be exposed, since it was not collected in the first place. Similarly, data-driven discrimination is not possible when there is no data to base it on. And study after study has shown that consumers simply do not want corporations to know everything about them10 — it's creepy, it's invasive, and it violates a fundamental principle of privacy: the right to be left alone.

As more and more states pass privacy laws that cater to corporations and fail to protect consumers, New York has the opportunity to pave a new path towards true digital privacy. We can let the New York Privacy Act further cement the status quo that allows corporations to spy on us with impunity, or we can fundamentally transform digital privacy by enacting data minimization and making privacy the default, allowing individuals to participate in the digital world without having to worry about what is being done with their data behind closed doors.

---

1 Danielle Keats Citron and Daniel Solove, Privacy Harms, GWU Legal Studies Research Paper No. 2021-11 (Feb. 2021), https://ssrn.com/abstract=3782222.

2 Sarah Geoghegan and Dana Khabbaz, Reproductive Privacy in the Age of Surveillance Capitalism, Electronic Privacy Information Center (Jul. 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/.

3 Marshall Allen, Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates, ProPublica (Jul. 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-yourrates.

4 Katy McLaughlin, Robots Are Taking Over (the Rental Screening Process), The Wall Street Journal (Nov. 21, 2019), https://www.wsj.com/articles/robots-are-taking-over-the-rental-screening-process-11574332200.

5 Matt Burgess, Evaline Schot, and Gabriel Geiger, This Algorithm Could Ruin Your Life, Wired (Mar. 6, 2023), https://www.wired.com/story/welfare-algorithms-discrimination/.

6 Caitriona Fitzgerald, Kara Williams, R.J. Cross, and Ellen Hengesbach, The State of Privacy, Electronic Privacy Information Center and U.S. PIRG Education Fund (Jan. 2025), https://epic.org/wp-content/uploads/2025/04/EPICPIRG-State-of-Privacy-2025.pdf.

7 Tim R. Samples, Katherine Ireland, and Caroline Kraczon, TL;DR: The Law and Linguistics of Social

Platform Terms-of-Use, Berkeley Technology Law Journal (Apr. 2017), https://doi.org/10.15779/Z38HT2GC9C.

8 Kara Williams and Caitriona Fitzgerald, Data minimization is the key to a meaningful privacy law, Electronic Privacy Information Center (May 9, 2024), https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/.

9 Access Now, Data Minimization: Key to Protecting Privacy and Reducing Harm (May 2021), https://www.accessnow.org/wpcontent/uploads/2021/05/Data-Minimization-Report.pdf.

10 Pew Research Center, How Americans View Data Privacy (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-pr iv acy-laws/.

Written Testimony for October 2025 Hearing on Data Privacy and Consumer Protection

New York State Assembly Standing Committees on Consumer Affairs and Protection and Science and Technology

Submitted electronically

The Electronic Frontier Foundation[1] thanks Chairs Rozic and Otis, and distinguished members of the Committees for the opportunity to submit testimony on this critical issue. We strongly urge this body to enact comprehensive data privacy legislation that extends protections to all New Yorkers— ensuring that privacy rights are upheld, no matter a person's age, income, or background.

The Growing Threat of Data Collection

In our modern world, private companies gather vast amounts of personal data on individuals. This data includes everything from our location and communications to our online behavior, biometric data, and even sensitive health information. Unfortunately, once companies collect this data, it is often sold, shared, and used in ways that most people don't fully understand. We've seen the consequences of this unchecked data collection and sharing in real-time—data breaches at platforms like Discord and Tea Messaging exposed users' sensitive information, underscoring the vulnerability of personal data and the minimal control users have over how it's used.

These practices are pervasive and largely invisible to consumers. Data is collected and exchanged through vast networks of data brokers and sold to third parties without users' knowledge or consent. This sometimes includes include law enforcement agencies, who buy data rather than seek warrants for it, which is why it's important not to exclude government contractors from data privacy law. When companies fail to protect this data, it can end up in the hands of bad actors, putting millions of people at risk.

The Limitations of Existing Protections

New York took a significant step forward with the 2024 passage of the Child Data Protection Act. While this law is an important milestone, it only applies to minors, leaving the broader population— especially marginalized and vulnerable communities—still exposed to invasive and opaque surveillance practices. Earlier this year, New York also passed the New York Health Information

[1] The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We represent more than 30,000 active donors and members, including thousands of supporters in New York.

Privacy Act, recognizing the need to protect sensitive health data. While these efforts are important, they

cannot be enough.

It's time for New York to lead once again, by passing strong, comprehensive privacy legislation that ensures everyone is protected from invasive corporate practices. This includes creating robust protections for personal data and holding companies accountable when they violate those rights.

The Underlying Issue: Unchecked Corporate Data Collection

At the heart of many modern-day harms, including issues around child safety, health privacy, algorithmic discrimination, and government overreach, is one fundamental issue: unregulated data collection and surveillance by private companies. Companies today collect personal information on an unprecedented scale. They track where we go, what we buy, who we communicate with, and even what we believe. This data is often gathered without clear, informed consent from the individuals it concerns. It is then bought, sold, shared, and used to infer sensitive characteristics, sometimes resulting in life-altering decisions that impact employment, housing, credit, education, and healthcare.

These practices disproportionately harm already marginalized groups, including low-income people, people of color, and vulnerable communities. As such, data privacy is not just an issue of convenience or control over our digital lives—it is also a civil rights issue. A meaningful response requires a comprehensive privacy framework grounded in transparency, consent, and robust enforcement.

Components of Strong Comprehensive Data Privacy Legislation

EFF urges this body to pursue data privacy legislation that centers individual rights, is grounded in data minimization, consent, transparency rights, and has robust enforcement. Below, we outline key concepts that should guide your work in protecting New Yorkers' data.

Data Minimization by Default

First and foremost, privacy should be the default—not the exception. Companies should only collect the data strictly necessary to provide the service that a user requests. Consumers should not have to sift through complicated settings or obscure terms to opt out of unnecessary data collection. Privacy should be an automatic right, not something users have to fight for.

Strong Opt-In Consent

Data collection should be strictly prohibited unless consumers provide clear, specific, and voluntary opt-in consent. This consent must be easy to understand and revocable at any time. Additionally, companies must be banned from using manipulative design tactics—often referred to as "deceptive design"—to trick users into agreeing to data collection they don't fully understand or want.

Clear User Rights

Consumers should have robust rights over their personal data, including the ability to access, correct, port, and delete their data. These rights are essential to empowering individuals to take control of their digital identities. Many countries and regions have already recognized these basic rights, and New York must do the same.

Prohibition on Behavioral Advertising

Behavioral advertising—the practice of tracking individuals across websites and apps to serve targeted ads—is one of the primary drivers of data abuse. New York should prohibit this business model outright, as it incentivizes companies to collect and misuse personal data rather than simply providing services that respect user privacy.

Strong Enforcement and a Private Right of Action

A law without enforcement is meaningless. While government agencies like the Attorney General's office play an important role, relying solely on them to enforce privacy rights is not enough— especially when resources are limited. Therefore, individuals must have the right to bring a private action against companies that violate their privacy. Such "private rights of action" are among EFF's highest priorities in any data privacy legislation.

No Pay-for-Privacy Schemes

We must ensure that privacy is not a luxury available only to those who can afford it. Allowing companies to offer discounts in exchange for greater data collection creates a two-tiered system: those who can afford privacy, and those who cannot. This scheme undermines the concept of informed consent and exacerbates inequality, making privacy a privilege rather than a right.

Non-Discrimination Protections

Consumers who choose to exercise their privacy rights should not face discrimination. Companies must be prohibited from denying services, charging higher prices, or offering inferior service to individuals who seek to protect their privacy. Privacy rights should not be a reason to penalize or disadvantage consumers.

Transparency and Accountability for Data Brokers

Data brokers—companies that buy and sell personal data—are a particularly opaque part of the data ecosystem. As such, they must be subject to transparency and accountability requirements. Requiring data brokers to register and disclose their practices would allow consumers to better understand how their data is being collected, shared, and used, and enable them to exercise their rights accordingly.

Protections for All New Yorkers

Lastly, privacy protections must apply equally to all New Yorkers—whether or not they fall into specific vulnerable categories. Privacy protections should not be limited to children or particular types of sensitive data. They must cover all personally identifiable information, regardless of how it is inferred or where it comes from.

Conclusion: The Path Forward

The constant stream of troubling news about companies violating privacy and data protection laws makes it clear that now is the time for action. A comprehensive, rights-based privacy law will not only address the issues we face today but will also establish a strong foundation to safeguard privacy in the future. New York has the opportunity to lead the nation in this critical area, ensuring that privacy and civil liberties are protected for all citizens in the digital age.

We urge you to pass legislation that puts people's rights first, not corporate interests.

Thank you for your time and consideration.

Sincerely,

Hayley Tsukayama
Associate Director of Legislative Activism
Electronic Frontier Foundation
(415) 436-9333 x 161

Testimony Regarding Comprehensive Privacy Protections

Eric Null, Co-Director, Privacy & Data Program Center for Democracy & Technology
Washington, DC

Before the New York Assembly Standing Committees on Consumer Affairs and Protection, and Science and Technology

Tuesday, October 14, 2025
Hearing on Data Privacy and Consumer Protections

Thank you for the invite to testify today before you regarding comprehensive privacy protections. My name is Eric Null, I am the co-director of the privacy & data program at the Center for Democracy & Technology, a thirty-year-old nonpartisan, nonprofit organization based in Washington, DC, focusing on protecting individual rights, civil rights, and civil liberties in the digital age.

I will focus today on three issues: one, moving beyond the notice-and-consent regime to a data minimization regime; two, protecting civil rights; and three, ensuring strong enforcement.

First, wouldn't it be nice if people could go online, purchase the goods they want, access the services they want, talk to their friends and family, engage in research, and generally use online services *without* needing to worry about the vast overcollection and use of data about them from every corner of the internet? These people could trust that those online services are collecting only the data needed to provide the service, which then would reduce the potential harms they might experience from, for example, the sale of that data in the vast data brokerage market, or from data breaches.

The only way we achieve that goal is to move beyond the failed notice-and-consent regime, which has been dominant since the 1990s and ultimately places the privacy burden on already-overburdened individuals. This regime is based on the fiction that an individual somehow consents to any collection or use of data so long as it is buried somewhere in a dense, legalistic privacy policy. We know people don't view privacy policies as particularly effective or useful.[1] We know people don't read privacy policies.[2] And we know that if people did try to read privacy policies, it would take them hundreds of hours per year.[3][4] As a result, people have a sense of futility and feel a lack of control over privacy risks, and they often underestimate the risks of disclosing data.[5]

Instead, we should be placing the privacy burden on the companies that benefit most from the

collection and exploitation of that data — meaning, it should be the company's responsibility to justify their data collection and use. To accomplish that, legislation should require companies to collect, use, and disclose data *only* to the extent needed to provide the services that are requested by the individual. This is the real data minimization standard, as adopted in Maryland,[6] and as proposed throughout the country and at the federal level.[7]

Data minimization helps prevent privacy harms at the outset because data a company does not have cannot lead to downstream harm through misuse, unauthorized access or disclosure (particularly to law enforcement), or some other harmful action. Data breaches are essentially a part of daily life now, as thousands of breaches happen per year. Those breaches would cause significantly less harm to individuals if companies were required to limit their collection of data – and its disclosure or sale to third parties – to only what is needed to provide the service. The recent breaches of Discord data (government IDs, IP addresses) and the Tea app (drivers licenses, photos, direct messages) show just how damaging data breaches can be.[8][9]

Stronger privacy protections are also bipartisan. Consumers from both sides of the aisle have been asking for years for more government protections over company data practices.[8] And a recent Consumer Reports survey found that seventy-two percent of Republicans and seventy-nine percent of Democrats "support a law that limits companies to using only the data they need to provide their service."[10]

Second, privacy rights are civil rights. Privacy legislation should put a stop to biased data practices and protect civil rights because we have already seen data being used in a discriminatory way, particularly through the training of, and decisions made by, algorithms. For instance, credit scores and the factors used to calculate them are deeply correlated with race. According to the Brookings Institute, Black and Hispanic individuals are much more likely to have credit scores below 620 than white individuals.[11] And facial recognition software exhibits similar biases, leading, for example, to the misidentification and wrongful arrests of three Black men: Robert Williams, Nijeer Parks, and Michael Oliver.[12]

Third, privacy laws are only as strong as their enforcement, and they should be enforced through multiple channels. A privacy law should provide the New York Attorney General with rulemaking authority and civil penalty authority, and provide individuals with a private right of action. That way, the state can ensure privacy is protected as a general matter, and individuals who are harmed can avail themselves of the court system. Further, to ensure proper enforcement, the AG should be appropriated enough funds to build a dedicated privacy office and team, like in Texas.[12]

New York has the opportunity to pass strong privacy legislation that includes data minimization, civil rights protections, and multiple levels of enforcement. We look forward to working with you to achieve that goal, and I'm available for any questions you may have.

---

[1] Sixty-one percent of adults consider privacy policies to be an ineffective way for companies to explain data practices, and almost seventy percent consider privacy policies to be just something to "get past." Colleen McClain *et al*, *How Americans View Data Privacy*, Pew Research Center (2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy.

[2] Fifty-six percent of American adults say they agree to privacy policies without reading them, compared to only eighteen percent who say they rarely or never agree without reading. *Id.*
[3] A 2008 study estimated that people would spend 244 hours per year, or forty minutes a day, reading privacy policies if they read all policies that apply to them. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society 540,
[4] (2008),
https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/02/Cranor_Formatted_Fi nal1.pdf. Privacy policies have only gotten longer since. Ryan Amos *et al*, *Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset*, In Proceedings of the Web Conference (2021), https://arxiv.org/pdf/2008.09159.
[5] Wenjun Wang *et al.*, *An Exploration of the Influencing Factors of Privacy Fatigue Among Mobile Social Media Users From the Configuration Perspective*, Scientific Reports (2025), https://www.nature.com/articles/s41598-024-84646-z.
[6] Maryland Online Data Privacy Act,
https://mgaleg.maryland.gov/2024RS/chapters_noln/Ch_454_hb0567E.pdf.
[7] American Data Privacy and Protection Act,
https://www.congress.gov/bill/117th-congress/house-bill/8152/text; American Privacy Rights Act, https://www.congress.gov/bill/118th-congress/house-bill/8818/text. *See also* New Mexico's Community Privacy and Safety Act, SB 420,
https://www.nmlegis.gov/Sessions/25%20Regular/bills/senate/SB0420.HTML, and Massachusetts' Consumer Data Privacy Act, H. 78, https://malegislature.gov/Bills/194/H78.
[8] *See* Alana Wise, *Tea Encouraged Its Users to Spill. Then the App's Data Got Leaked*, NPR (Aug. 2,
[9]),
https://www.npr.org/2025/08/02/nx-s1-5483886/tea-app-breach-hacked-whisper-networks; *Update on a Security Incident Involving Third Party Customer Service*, Discord (Oct. 3, 2025), https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service. [8] Colleen McClain *et al.*, *How Americans View Data Privacy*, Pew Research Center (Oct. 18, 2023),
https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digit al-privacy-laws.
[10] Scott Medintz, *Americans Want Much More Online Privacy Protection Than They're Getting*, Consumer Reports (Nov. 20, 2024),
https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-prot ection-a9058928306.
[11] "More than 1 in 5 Black individuals have FICOs below 620, as do 1 in 9 among the Hispanic community, while the same is true for only 1 out of every 19 white people." Aaron Klein, *Reducing Bias in AI-Based Financial Services*, Brookings Inst. (July 10, 2020), https://www.brookings.edu/articles/reducing-bias-in-ai-based-financial-services.
[12] Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*,
WIRED (Mar. 7, 2022),
https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives. [12] Texas built a $5 million privacy-specific enforcement team and they have been out ahead on enforcement efforts. Cobun Zweifel-Keegan, *A View from DC: the Price of Privacy Enforcement*, IAPP (Feb. 28, 2025), https://iapp.org/news/a/a-view-from-dc-the-price-of-privacy-enforcement.

New York News Publishers Association
Written Testimony

Assembly Committee on Consumer Affairs and Protection

Assembly Committee on Science and Technology

October 14, 2025

We focus our comments on A.974/S.8524, the New York Data Protection Act, which would have a significant impact on newspaper and magazine publishers in New York State. We appreciate the opportunity to share our thoughts on how this legislation might serve as a model for other states in their endeavors to protect the personal data of individuals while also ensuring they have continued access to high-quality journalism.

The New York News Publishers Association represents a wide variety of news organizations including those which serve a global audience, weekly newspapers that have served a community through generations of a local family, publicly traded and privately owned publishers, not-for-profit and shareholder-owned newspapers, and newspapers which have never been printed on paper.

We appreciate your support for the press, and we urge you to consider the importance of maintaining consumers' access to high-quality journalism, which plays a vital role in supporting a healthy democracy, local communities, and the economy. Millions of New Yorkers rely on newspapers, magazines, and their associated websites and applications to stay up to date on the latest local, domestic, and international news, political developments, culture and society, and discussion topics related to their hobbies, activities, or areas of interest. News media entities play a unique and vital role in engaging audiences of all ages by presenting valued, trusted, curated content to consumers. The production of high-quality journalism, often provided at a reduced cost or for free to readers, depends in part on content supported by advertising. Likewise, responsible data practices are vital for sustaining the trusted, direct relationship between readers and publishers.

With some suggested revisions, we believe A.974/S.8524 will align with the emerging national privacy framework and ensure New Yorkers retain access to high-quality journalism. Our key recommendations include the following:

I. Preserve New Yorkers' access to quality, First Amendment-protected journalism by adding an exemption for journalistic activities, adding standard exceptions to the consumer deletion right and clarifying the bill's data minimization language. The bill lacks several essential provisions present in other privacy legislation that ensure that the law does not interfere with journalistic activities and that news publishers are able to meet other contractual obligations or other reasonable reasons for the retention of data. An explicit free speech exemption is crucial. We therefore recommend the addition of the following clarifying exception language: "The obligations imposed on controllers or processors under this article do not apply to any processing activities associated with journalistic activities including, without limitation, the collection, storage, use, or sharing of personal data for journalistic purposes, the publication of content of legitimate public interest, or the processing or transfer of personal data by a controller for such purpose." (§ 1205. Limitations. 4.)

II. We also recommend the addition of the following standard exceptions to the consumer deletion right: “it is reasonably necessary for the controller to maintain the consumer’s personal data in order to (a) comply with a legal obligation or assist others in complying with a legal obligation; (b) help to ensure security and integrity to the extent the use of the consumer’s personal data is reasonably necessary and proportionate for those purposes; (c) debug to identify and repair errors that impair existing intended functionality; or (d) exercise free speech, ensure the right of another consumer to exercise that consumer’s right of free speech, or exercise another right provided for by law.” (§ 1202. Consumer Rights. 7.(e)(iii))

In addition, we recommend the following tweak to the data minimization requirement: Limiting the controllers’ use and retention of personal data to what is “necessary or reasonably related to provide the services or goods requested by the consumer” retains the data minimization principle of the bill while preserving news publishers’ ability to maintain (with appropriate notice and support for opt-out) standard advertising practices that readers expect to support free or relatively low-cost ad-supported journalism. (§1203. Controller, Processor and Third Party Responsibilities. (d)(i)(A)). Further, we urge you to strike “necessary for the internal business operations of the controller” which overly restricts expected, related practices and is inconsistent with other frameworks. (§1203. Controller, Processor and Third Party Responsibilities. (d)(i)(B))

III. Clarify that “targeted advertising” is not “profiling.” A clear definition of commonly expected advertising practices is crucial for ensuring consumers have clear rights and that covered entities can distinguish between different restrictions intended to apply to different advertising practices. This is particularly the case for high quality journalism supported by advertising that appears directly on a publisher’s site but may be informed by third-party information. The bill’s current definition of targeted advertising is ambiguous and inconsistent with other frameworks.

We urge you to adopt the following definition of “targeted advertising”: "Targeted advertising" means advertising based upon profiling on personal data obtained or inferred from a person’s activities over time and across nonaffiliated internet websites or online applications subject to the consumer right to opt out pursuant to Section 1202. Targeted advertising does not include (a) advertisements based on activities within a controller or its affiliates’ own internet websites or online applications, (b) advertisements based on the context of a consumer’s search query, visit to an internet website or online application, (c) advertisements directed to a consumer in response to the consumer’s request for information or feedback, or (d) processing personal data solely to measure or report advertising frequency, performance or reach. It does not include recommendations by a controller to a consumer with whom the controller has an existing relationship that are made on the controller's and/or its affiliates’ websites or online applications and are based upon personal data that the controller has collected from the consumer on such websites or online applications regarding content, products, or services provided by the controller and/or its affiliates.” (§ 1200. Definitions. 24.)

Further, we urge you to strike the following: “targeted advertising and sale of personal data shall not be considered processing purposes that are necessary to provide service or goods

requested by a consumer." This section directly threatens the sustainability of ad-supported journalism. Because consumers may freely opt out of targeted advertising, it is also unnecessary for conveying the consumer rights intended by the Chair. (§ 1202. Consumer Rights. 2.(d))

IV. Revise deletion and retention language to ensure consumer intent is met, avoid unintended disruption of contracted subscriptions and services, or threaten important First Amendment protections for the press. We urge you to change the bill language to clarify that controllers may maintain a record of deletion requests. We recommend striking the section that directs a controller to delete all of a consumer's personal data upon receipt of a deletion request. Controllers must be able to alert a consumer when services would be disrupted in processing this request – for example, confirm whether a reader wishes to end an existing subscription. As written, the section could cause inadvertent violation of other consumer protection and contractual obligations of a covered entity. (§ 1202. Consumer Rights. 7.(a)(ii))

V. The Attorney General is the most appropriate entity to enforce the legislation exclusively. The following revisions will provide further clarity needed to maximize the successful good-faith compliance of covered entities. (§ 1206. Enforcement.) We urge you to clarify that a private right of action is expressly excluded by including the following language: "Nothing in this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of this act or any other law." Additionally, we recommend a number of other modifications to the Enforcement section, including: 1) A court should establish actual harm to the consumer. 2) The bill should provide a sixty day right to cure.

The bill's extensive operational requirements will require time for covered entities to comply. The bill must not take effect immediately but rather provide a two-year compliance preparation window. New Yorkers depend on high-quality journalism, and their access to news media resources must be preserved.

We look forward to continuing our work with you on this important legislation.

Respectfully Submitted,

Diane Kennedy
President
October 14, 2025

Joint Public Hearing on Data Privacy and Consumer Protections
Testimony of the New York Credit Union Association

Before the
Assembly Standing Committee on Consumer Affairs and Protection
Assembly Standing Committee on Science and Technology

Hon. Nily Rozic
Chair, Committee on Consumer Affairs and Protection

Hon. Steven Otis
Chair, Committee on Science and Technology

Tuesday
October 14, 2025
10AM
Hearing Room C
Legislative Office Building
Albany, New York

I. Introduction

Good morning, Chairperson Rozic, Chairperson Otis, and distinguished members of the Assembly Standing Committees on Consumer Affairs and Protection and Science and Technology. My name is Jeremy Newman, and I serve as Vice President of Legislative and Regulatory Affairs for the New York Credit Union Association (NYCUA), representing 275 federally- and state-chartered credit unions across New York State that collectively serve over 7 million members.

I appear before you today to address the critical importance of consumer data protection within New York's credit union system and to provide our industry's perspective on the development of comprehensive data privacy legislation. The New York Credit Union Association strongly supports the Committees' initiative to examine potential solutions for ensuring the protection and privacy of consumer data.

We share your concerns regarding the significant growth in personal data collection and the inconsistent nature of current industry protections. While we commend the intent behind the legislature's passage of the New York Child Data Protection Act in 2024, we agree that broader protections are essential for all New Yorkers, particularly vulnerable communities who deserve robust safeguards in our increasingly digital economy.

II. Commitment to Data Protection

Protecting consumer and member data represents the paramount priority for New York's credit unions. Unlike many commercial enterprises that may view data as a profit center, credit unions operate as member-owned, not-for-profit cooperative institutions where data protection directly serves our members' interests rather than external shareholders.

Credit unions recognize that fraud represents one of the most significant threats to consumer financial security in today's digital environment. Our focus on protecting consumer data and privacy serves as a critical defense against fraud risk, helping to prevent identity theft, account takeovers, and other financial crimes that can devastate members' financial well-being.

Our commitment manifests through comprehensive current measures including adherence to federal Gramm-Leach-Bliley Act privacy and safeguards requirements, and implementation of National Credit Union Administration cybersecurity guidance, and for our state-chartered credit unions full compliance with the New York Department of Financial Services Cybersecurity Regulation (23 NYCRR 500). Credit unions maintain robust incident response plans, conduct regular employee training programs, and employ safeguards like multi-factor authentication systems with encryption for data both in transit and at rest.

Addressing the Committees' concern about digital platforms that "actively collect, share, and sell data—often without the informed consent of individuals," credit unions operate under fundamentally different principles. We collect only data necessary for member services, maintain strict limitations on third-party sharing, and do not engage in data monetization practices. Our member-centric governance structure ensures that data protection policies align with member interests rather than profit maximization.

III. Alignment with Federal Standards

New York credit unions' data protection efforts carefully align with existing federal standards to ensure comprehensive coverage while avoiding regulatory conflicts. Our institutions adhere to the Gramm-Leach-Bliley Act's privacy and safeguards rules, which establish baseline requirements for financial institutions' handling of consumer information. Additionally, we comply with Federal Trade Commission guidance on data security practices and National Credit Union Administration cybersecurity guidance and examination procedures.

The importance of avoiding conflicts between state and federal requirements cannot be overstated. Conflicting or duplicative requirements create compliance confusion, increase costs disproportionately for smaller institutions, and may inadvertently weaken overall protections by creating regulatory gaps or inconsistencies. Industry experience suggests that New York legislation that builds upon and enhances federal standards rather than creating parallel or conflicting frameworks tends to be most effective. Specific federal regulations that guide our current practices include the GLBA Privacy
Rule (16 CFR Part 313), the GLBA Safeguards Rule (16 CFR Part 314), Regulation P (12 CFR Part 1016), NCUA's Cybersecurity Guidance including 12 CFR Part 748, and adherence to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This federal foundation provides a robust starting point for enhanced statelevel protections.

IV. Compliance Framework Considerations

Important considerations for any compliance framework might include core data protection principles with flexibility in implementation methods. For example:

Core Universal Principles: Credit union industry practices typically include maintaining annual risk assessments tailored to their operations, implementing appropriate encryption standards for data protection, establishing incident response plans proportionate to their complexity, conducting regular employee training on data security and privacy, maintaining written information security programs aligned with federal requirements, and implementing human oversight for all automated decision-making systems including AI.

Flexible Implementation Considerations: Credit unions often meet requirements through various approaches including shared service arrangements for smaller institutions, third-party vendor solutions with appropriate oversight, cooperative compliance programs among multiple credit unions, and scalable technology solutions that grow with institutional needs. Experience suggests that reasonable implementation timelines with ongoing assessment cycles tend to be most effective.

Risk-Based Adaptability: Effective frameworks typically focus on outcomes rather than prescriptive methods, allowing institutions to tailor their approach based on their specific risk profile, member demographics, and operational complexity. Regular selfassessments help ensure continued appropriateness of chosen methods.
This approach maintains consistent consumer protection standards while recognizing that different institutions may achieve these standards through different means based on their resources and circumstances.

Alternative Scalable Compliance Considerations

As an alternative to a universal framework, industry experience with tiered compliance systems can be effective in recognizing the diverse nature of New York's credit union landscape, which ranges from small community institutions serving a concentrated member base to larger organizations serving hundreds of thousands of members across multiple regions. It bears noting that unlike large commercial banks, even the largest credit unions in New York serve as their community financial institutions and therefore all credit unions, regardless of size, take customer data and privacy protection seriously as a fundamental obligation to their member-owners. The importance of ensuring any legislation and regulation are appropriately tailored to fit the risk profile and size of the institution cannot be overstated.

A scalable legislative approach could help ensure that enhanced protections do not create insurmountable barriers for smaller institutions, while ensuring that larger institutions with greater resources and more complex operations face appropriately comprehensive requirements.

This scalable approach could promote broader participation and effectiveness by ensuring that compliance requirements match institutional capacity while maintaining high protection standards across all tiers.

V. Risk-Based Approach Observations

Industry experience suggests that focusing regulatory resources on high-risk activities where consumer data faces the greatest exposure tends to be most effective. Based on industry experience and threat analysis, areas that typically receive priority attention include online and mobile banking platforms, cloud computing and data storage systems, payment processing networks, and third-party data sharing arrangements.

Online and mobile banking platforms represent the highest-risk area due to their 24/7 accessibility, large transaction volumes, and appeal to cybercriminals. These systems typically

require advanced authentication methods, real-time fraud monitoring, and robust session management protocols. Cloud and data storage systems demand particular attention regarding data sovereignty, encryption standards, and access controls, especially when utilizing third-party providers.

Payment processing systems warrant focused oversight due to their interconnected nature and the high value of financial transaction data. Industry practices often include specific risk assessment methodologies such as regular penetration testing, vulnerability scanning, and threat intelligence integration. Mitigation strategies typically encompass network segmentation, endpoint protection, and continuous monitoring systems.

Artificial intelligence deployment introduces additional risk considerations. AI-powered systems require special attention to algorithmic bias, transparency requirements, and cybersecurity vulnerabilities including adversarial attacks and AI-enabled social engineering threats.

This risk-based approach allows institutions to allocate limited cybersecurity resources where they provide maximum protective benefit while avoiding unnecessarily burdensome requirements for lower-risk activities.

VI. Safe Harbor Protection Observations

Safe harbor provisions in other regulatory contexts have typically included elements such as adherence to recognized industry security frameworks, particularly the NIST Cybersecurity Framework. Such provisions generally provide liability protection and reduced regulatory scrutiny for institutions that proactively implement comprehensive security measures.

Qualifying criteria in other contexts have typically included: implementation of the NIST Cybersecurity Framework or equivalent recognized standard; completion of annual independent third-party security assessments; maintenance of current cybersecurity insurance coverage; demonstration of prompt incident response and member notification procedures; participation in information sharing programs with regulatory authorities and industry organizations; and for institutions using AI, implementation of recognized AI governance frameworks with regular bias audits and human oversight requirements.

The benefits of safe harbor protection typically include reduced liability for data breaches when institutions have implemented reasonable security measures, streamlined regulatory examinations that focus on verification of safe harbor compliance rather than comprehensive security reviews, and regulatory certainty that encourages proactive investment in cybersecurity measures. This approach incentivizes best practices while providing reasonable protections for institutions that make good-faith efforts to protect consumer data.

VII. Current Industry Practices and Emerging Trends

New York credit unions currently employ comprehensive measures to safeguard consumer personal data and combat fraud threats. Many use advanced encryption techniques and standards for data at rest and data in transit, multi-factor authentication systems incorporating biometric verification where appropriate, network segmentation to isolate sensitive systems, regular security assessments and penetration testing, comprehensive employee training programs with phishing simulation exercises, and detailed incident response and business continuity plans. These protective measures are specifically designed to mitigate fraud risks and protect members from financial crimes that exploit vulnerable data systems.

Artificial Intelligence Applications: Credit unions are approaching AI with measured intentionality, with many applying a "crawl-walk-run" approach that favors purposeful, transparent adoption. Current AI applications include fraud detection systems that analyze transaction patterns more effectively than traditional methods, cybersecurity tools for real-time threat detection and 24/7 monitoring, and member service chatbots that provide multilingual support after business hours. AI-driven underwriting models help extend credit to historically underserved populations by incorporating alternative data like utility payments, leading to increases in loan approvals while maintaining underwriting standards.

AI Risk Management: Similar to the compliance framework, requirements related to AI risk management could ensure principles are maintained with flexibility in implementation methods, and a safe harbor for credit unions that demonstrate adherence to recognized industry standards. Options for managing risks associated with AI include implementing human oversight for all AI decisions, conducting regular bias audits to prevent discriminatory outcomes, maintaining explainable AI models to satisfy fair lending requirements, stripping personally identifiable information from datasets used by generative AI, and employee training on AI-specific threats including deepfake recognition and advanced social engineering attacks.

Emerging technologies being explored across the industry include zero-trust security architectures that verify every access request regardless of source, blockchain technologies for secure transaction verification and audit trails, enhanced data loss prevention systems with behavior analytics, and improved member communication systems that provide real-time security notifications and transparent privacy controls.

VIII. NYCUA as a Resource

NYCUA serves as the primary representative of New York's 275 credit unions, offering collective expertise in cybersecurity, compliance, consumer protection, and responsible AI deployment. We provide technical assistance in understanding credit union operations and challenges, access to industry best practices and emerging trends, and facilitate stakeholder input through member surveys and focus groups.

We are positioned to share aggregated data on cybersecurity incidents and trends, provide impact assessments for proposed regulatory changes, and participate in ongoing dialogue throughout the legislative process. Through our partner network our expertise extends to AI governance frameworks, bias testing methodologies, and responsible technology deployment strategies that other industries can learn from.

IX. Conclusion

The New York Credit Union Association reiterates our unwavering commitment to protecting consumer and member data as our highest priority. We recognize that effective data protection requires collaborative efforts between credit unions, regulators,
and the New York State Assembly to develop comprehensive, practical, and enforceable standards that address both traditional cybersecurity challenges and emerging AI-related risks.

We appreciate the Committees' leadership in addressing the inconsistent and voluntary nature of current industry protections and we stand ready to work with you in developing robust consumer protections that recognize the unique nature of credit union operations. Our member-owned, not-for-profit structure aligns our interests directly with consumer protection, making credit unions natural partners in advancing data privacy legislation.

Regarding artificial intelligence, industry experience suggests that smart regulation— clear rules against discrimination and fraud, strong transparency requirements, and high cybersecurity standards—paired with flexibility to innovate within those guardrails tends to be most effective. AI's potential to enhance consumer protection and financial inclusion could be recognized when properly governed through risk-based, outcomefocused regulation.

The NYCUA offers our expertise, resources, and ongoing collaboration to assist the Committees in developing effective legislation that protects all New Yorkers while preserving the ability of credit unions to serve their members effectively. We welcome the opportunity to participate in working groups, provide technical assistance, and offer feedback throughout the legislative process.

We respectfully suggest that any resulting legislation might incorporate the scalable, risk-based, and federally aligned approach we have outlined today, ensuring that enhanced protections strengthen rather than burden the credit union system that serves millions of New Yorkers. Thank you for your time and consideration.

NEW YORK BANKERS ASSOCIATION NYBA

TESTIMONY

OF

NIALL O'HEGARTY

GENERAL COUNSEL

NEW YORK BANKERS ASSOCIATION

New York State Assembly Committee on Consumer Affairs and Protection

New York State Assembly Committee on Science and Technology

Public Hearing on Data Privacy and Consumer Protections

October 14, 2025

COMMITMENT TO COMMUNITY

99 Park Avenue, 17th Floor, New York, NY 10016 • 212.297.1600 • nyba.com

The New York Bankers Association ("NYBA") represents smaller community, midsize regional, and large banks across every region of New York State. Together NYBA members employ nearly 150,000 New Yorkers, safeguard $2 trillion in deposits, and annually extend nearly $145 billion in home and small business loans. NYBA members also support their communities through an estimated $200 million in community donations and 500,000 employee volunteer hours. Our members share the Committees' concern with safeguarding data privacy and we welcome the opportunity to share our views on this important topic.

Summary

In many respects, banks are uniquely situated to offer insight on the importance of data privacy and the best means of ensuring that effective data privacy controls adapt to keep pace with the rapid evolution of technology and consumer preference. Unlike most industries, it is the stock and trade of banks to routinely and safely handle the most sensitive financial and other private information on behalf of business clients of all sizes, and on behalf of consumer clients of all ages, income levels, and demographic backgrounds. Moreover, because of their success as an industry in maintaining unparalleled data privacy protections, banks have consistently enjoyed comparatively high levels of consumer confidence in their ability to safely store and manage private information. Finally, banks are already subject to a uniquely comprehensive and detailed set of data privacy requirements codified in federal law and regulation, and are subject to ongoing oversight and regular examination to ensure their compliance with those requirements. In short, banks have long operated at the intersection of commerce and privacy, and more importantly, at the forefront of efforts to safeguard private consumer data.

With this background in mind, and with due regard to the importance of the Committees' work on

this issue, we respectfully offer the following comments and observations in support of the legislature's efforts to identify and develop an effective data privacy framework for New York State.

Uniform Data Privacy Standards Benefit Consumers and Industry

Any broad-based legislative framework governing data privacy should acknowledge the uniquely stringent data protection requirements already applicable to banks. Most industries that may be contemplated to fall within the scope of any new data privacy law in New York are not, like banks, already subject to comprehensive and detailed legal requirements governing their possession and use of consumer data. We strongly urge that State-level legislation and regulations addressing data privacy requirements for banks align closely with the detailed and expansive federal privacy regime requirements already in place.

The primary privacy and data security consumer protection law to which financial institutions are subject is Title V of the Gramm-Leach-Bliley Act ("GLBA").[1] The GLBA represented the first time that Congress enacted sector-specific, comprehensive privacy and data security standards, in this first instance for financial institutions and consumer financial data. With the GLBA, Congress carefully constructed a privacy and data security regime that provides consumers with meaningful privacy rights, while also ensuring that they can conduct financial transactions seamlessly and safely. These privacy rights apply regardless of where customers live and ensure that financial institutions can protect against fraud, illicit finance, money laundering and terrorist financing.

- **Rulemaking.** The GLBA provides various federal financial regulators with meaningful authority to adopt regulations to implement robust privacy and data security standards. For instance, the CFPB adopted Regulation P to enhance and provide guidance for the GLBA's consumer privacy standards.[2] o This has allowed the regulatory regime to be flexible and adapt over time as privacy considerations evolve.
- **Enforcement.** Under title V, federal financial regulators—including the CFPB, OCC, FDIC, NCUA, SEC, Federal Reserve and others—generally examine financial institutions for their compliance with privacy and data security requirements and have the authority to bring enforcement actions against institutions found to be out of compliance with these requirements.[2]
- **Opt-Out Notices.** The GBLA and its implementing regulations require financial institutions to provide consumers with a notice and opportunity to opt out **before** sharing a consumer's nonpublic personal information with an unaffiliated third party.[3] o *Exceptions:* While the law contains exceptions to this requirement, they are similar in subject matter and scope to exceptions in other state consumer privacy legislation (*e.g.*, to process a requested transaction, prevent fraud, with the consumer's consent, to comply with applicable law).[4]
- **Initial and Annual Privacy Notices.** Banks must provide consumers with an initial notice that clearly, conspicuously and accurately describes the institution's privacy polices and practices.[5] The law also mandates an annual notice if there have been any changes to privacy policy.[6]
- **Limits on Data-Sharing with Third Parties.**
    - **Sharing NPI.** A bank may disclose nonpublic consumer information with a non-affiliated service provider or joint-marketing partner only if it (i) offers the consumer an opt-out or (ii) the bank has a contract requiring the recipient to use the information solely to perform services/functions for the bank *and* the sharing was already described in a previous privacy notice to

the consumer.[7][8]

- **Limits on Reuse.** Recipients of consumer's nonpublic data may only use and disclose such information as permitted by Reg. P; broader reuse or further disclosure is restricted.[9]
- **Mandatory Vendor Oversight.** Banks must exercise due diligence in sharing consumer data with vendors, contractually require appropriate safeguards, and monitor vendors' performance as part of a written information-security plan, per the Interagency Safeguard Guidelines.[10]

- **Consumer Notification Upon Breach.**
  - Federal financial service regulators collaborated to create a uniform standard for notifying both an institutions regulator and its customers if consumer non-public information is breached.[9]
  - To address breaches of data shared with third parties, the Interagency Safeguard Guidelines require vendor contracts to ensure prompt notification to the banking institution if an incident occurs.[10]

While GLBA is the latest, and most significant, legislative scheme addressing privacy for financial services providers, it does not stand alone. The federal Fair Credit Reporting Act[11] and the Right to Financial Privacy Act[12][13] were each passed by Congress in the 1970s, establishing an early expectation that the banking industry would be subject to more stringent privacy requirements than those applicable to other businesses. On the State level, New York's own Cybersecurity Regulation,[15] promulgated by the Department of Financial Services ("DFS") in 2017 and since amended twice, sets out detailed and comprehensive data security requirements for State chartered banks. These include extensive requirements for, among other things, cybersecurity policies and plans, data encryption, third-party vendor management, access controls, regular audits and incident reporting. Similarly, the recently enacted Child Data Privacy Act contains significant new privacy requirements aimed specifically at safeguarding the data of minors.

For the most part these measures reflect efforts to carefully balance privacy protections with common sense exceptions to minimize disruptions to financial markets, transactions, and accounts. In a similar vein, we respectfully urge that any legislation to establish a State privacy standard must recognize the strong privacy and data security standards that are already in place for the financial sector under the GLBA and other State and federal financial privacy laws—a new State privacy framework must avoid provisions that duplicate or are inconsistent with those laws. Duplication and inconsistency carry a number of significant risks, including the creation of a patchwork of regulatory approaches that generate inconsistent or conflicting requirements and outcomes, are confusing to consumers, and difficult to implement.

Other states have recognized this risk and have responded by tailoring their State-level privacy legislation to promote a uniform approach. For example, **New Jersey[14], Maryland[17], Virginia[15], Colorado[16], Indiana[17], Iowa[18], Montana[19], Tennessee[20] and Texas[21] each include an entity-level *and* data-level GLBA exemption in their consumer-privacy statutes**; this is the preferred formulation of the exemption. This bipartisan trend reflects sound policy and we urge the New York State legislature to adopt a similar approach.

Enforcement of Privacy Laws Should be Left to Regulators

Another key concern regarding any new legislated data privacy controls relates to which entity or entities are tasked with enforcing the measure. As noted, when applied in the financial services

context, data privacy standards benefit greatly from uniformity. Uniform standards facilitate easier implementation across geographies and business models, generate consistent expectations for both business and consumers alike, and discourage inconsistent application of the law. We strongly encourage the legislature to ensure that any new data privacy legislation clearly vests the New York State Department of Financial Services ("DFS") with exclusive authority to enforce the measure against banks. Conversely, we discourage the use of private rights of action as an enforcement mechanism.

Vesting regulators with sole enforcement authority helps guard against disparate and potentially conflicting interpretations of privacy rules arising from private lawsuits litigated in courts around the State. In addition, private rights of action generally risk frivolous and unnecessary litigation, which in turn increases the costs and complexity of implementing data safeguards across the industry.

NYBA and its member banks welcome continued dialogue and collaboration with policymakers to ensure that data privacy protections evolve alongside technology and consumer expectations. As institutions long entrusted with safeguarding the most sensitive financial and personal information, banks bring a proven framework of compliance, oversight, and public trust to this conversation. We appreciate the opportunity to provide this testimony and look forward to working together to advance data privacy standards that are effective, consistent, and reflective of the industry's deep experience in protecting consumers.

[1] 15 U.S.C. Chapter 94 ("Privacy") [2]
See, 12 C.F.R. § 1016.1 et. seq.
[2] 15 U.S.C. § 6805.
[3] 12 C.F.R. §§ 1016.7 & 1016.9.
[4] 12 C.F.R. §§ 1016.13-1016.17.
[5] 12 C.F.R. § 1016.4.
[6] 12 C.F.R. § 1016.5.
[7] 12 C.F.R. § 1016.13. [9]
12 C.F.R. § 1016.11.
[8] C.F.R. Part 364, Appendix B. This appendix is the applicable financial services counterpart to the more widely known FTC Safeguard Rule.
[9] See, 12 C.F.R. Parts 53, 225, 305; *Agencies approve final rule requiring computer-security incident notification*, Joint Release of the Board of Governors of the Federal Reserve System, the FDIC, and OCC (Nov. 18, 2021) (https://www.federalreserve.gov/newsevents/pressreleases/bcreg20211118a.htm).
[10] 12 C.F.R. Part 364, Appendix B.
[11] 15 U.S.C. §§ 1681–1681x.
[12] 12 U.S.C. §§ 3401–3422.
[13] NYCRR Part 500.
[14] N.J.R.S. 56:8-166.13(10)(b) [17]
Md. Comm. Code § 14-4703.
[15] Va. Code § 59.1-576(B).
[16] C.R.S. § 6-1-1304(2)(q).
[17] Ind. Code § 24-15-1-1(a)(2).
[18] Iowa Code § 715D..2(2).
[19] Mont. Code § 30-14-2804(1)(e).
[20] Tenn. Code § 47-18-3210(a)(2).
[21] Tex. Bus. & Com. Code Ann. § 541.002(b)(2).

ADDITIONAL SUBMITTED TESTIMONY

Testimony of Dan Powers

Hearing on Data Privacy and Consumer Protections

October 14, 2025

Good morning, Assembly Members, and thank you for giving me the chance to offer my thoughts on data privacy regulation. Access to data is critical to small businesses like mine, and overbroad data restrictions will make it much harder for us to find customers, grow, and succeed.

My name is Dan Powers. Since 2005, I have operated Real Brave, a music lesson studio with multiple locations that has employed hundreds of New Yorkers over our 20-year history. I represent the visionaries that you intend to regulate: The baker, the restaurateur, the repairman… the small business owner. We are your neighbors. All we want is the freedom to find a customer and keep a customer for life.

At Real Brave, we post every day on social media and use messenger tools to reach potential clients. We rely on retargeting to re-engage people who have interacted with our posts, and use geo-targeting to ensure that specific “info-tainment” posts reach the communities we serve. In the past, webinars have been a key part of how we educate and engage new students, and we continue to rely heavily on email marketing to stay connected. These activities are not invasive; they’re the modern equivalent of local flyers (which are illegal to post now) or phone calls (which people assume are “junk”). And they’re far more efficient and affordable for small business owners.

Data helped me rebuild after the pandemic, and it keeps my school thriving. We use data-powered ads to reach people who are likely to be interested in taking lessons from us. We can’t see any kind of personally identifiable information. Instead, we partner with digital ad companies that make sure our ads are sent to phones and devices where people have been searching for music lessons. That helps us find students, and means we don’t waste money advertising to the 99.9% of people who aren’t searching for music lessons. It also means we don’t waste money doing things like sending ads for our Queens location to people who live on Staten Island.

These outreach tools are both effective and responsible. We maintain a 50% open rate on emails from subscribers who choose to receive updates. Our text messages have a high delivery rate, ensuring that clients receive important information in real time. Phone calls have become less effective because people often don’t answer, and traditional mail is too costly for its minimal return. Digital outreach is the only practical, affordable, and consent-based method we have left to communicate.

We also rely on data analytics to see things like which ads got lots of clicks, or how people arrived at our website — say, by searching online or clicking an ad or email link. That information is really valuable to us, because it allows us to pull or edit ads that aren’t working, and focus our marketing efforts and budget where they get the best results — whether that’s ads on a certain website or posts on a particular social media platform.

If the New York Privacy Act is enacted as currently written, even these standard outreach efforts could become expensive and restrictive. We would be forced to manage compliance systems meant for billion-dollar corporations, all while simply trying to reach our community and serve our

students. This would add layers of complexity that would threaten the very survival of small businesses that rely on digital communication.

When it comes to data privacy regulation, three things worry me. The first is strict data limitations that say a business can only use a customer's data to provide a product or service the customer specifically requested, like processing a purchase. That would make it really hard for me to reach customers and grow my business.

No consideration was given to small businesses during the Minimum Wage Raise Act of 2013. On behalf of the Partnership for NYC, I was the lone dissenting voice for small businesses at the public hearing. The Council's response to me was simple: "This only affects the McDonald's of the world." But that response illustrates the core problem with well-intentioned but overbroad legislation. No law, regulation, or bill — however noble its intent — helps the free market make the best decisions when it's written with sweeping language that punishes those just trying to run honest businesses. Every law like this that you pass diminishes the ability of small businesses to simply exist.

For instance, if someone spent time looking at my website, strict data limitations would prevent my business from using that information to send them an ad, because they hadn't requested that I (or my advertising partners) do so. That means I'd lose the chance to connect with a likely customer. I'd also lose the valuable data analytics that help me effectively market my school. Without data, I'd have to spend more money on advertising and marketing, but I'd find fewer students. That's a double-whammy for a small business like mine.

My second worry is data-use thresholds or "carveouts" that are meant to exempt businesses that deal with fewer than, say, 100,000 data points annually. But data is generated by every online activity (everything from opening a tab on a website to clicking on an ad), so almost any business with a website will easily surpass the threshold. Worse, if your small business succeeds, you'll generate more data. Then you'll surely surpass the threshold and likely have to rethink your entire digital marketing strategy. So the "threshold" will effectively punish success. Most importantly, small businesses partner with bigger companies to do things like send data-powered ads and email campaigns. The big guys will definitely have to comply, so small businesses like mine will be impacted, too.

My third worry is private right of action provisions, which would allow anyone to sue me for alleged data privacy violations. A private right of action opens the door to frivolous lawsuits that generate huge costs and stress for small business owners like me.
The state's privacy goals are understandable, but any bill must distinguish between exploitative data practices by large corporations and legitimate, permission-based marketing by small, community-based businesses. Without that distinction, the law will harm precisely the kind of innovative, creative small businesses New York aims to support.

I appreciate your interest in keeping New Yorkers' data secure. But as you craft legislation, I ask that you consider the impact that strict data limitations will have on small businesses throughout New York, and strive to create balanced regulations that both protect people and allow small businesses like mine to grow and thrive.

Testimony of Anthony Edwards, Jr.
Before the NY Assembly Committees on Consumer Affairs & Protection and Science & Technology
Hearing on Data Privacy and Consumer Protections
October 14, 2025

Good morning, New York legislators, and thank you for giving me the opportunity to speak to you about data privacy regulation. Smart data regulation is vital to small businesses like mine, because data empowers us to find customers, grow our businesses, and support our communities and the causes we care about.

My name is Anthony Edwards, Jr., and I'm the Co-Founder and CEO of EatOkra, an easy-to-use app that lets users find the best Black-owned food and beverage companies in their area.

My wife, Janique, and I founded EatOkra in 2016 to support Black-owned eateries and help other consumers discover and support them. Today, over 20,000 Black-owned restaurants use the EatOkra app to bring Black cuisine and culture to more than half a million customers nationwide. We like to say we're the Yelp of Black-owned restaurants.

Data is vital to our business in two key ways. First, we use data-powered advertisements to reach people who are likely to be interested in our app. We can't see anyone's personal information, and we're certainly not spying on anyone. Instead, we work with digital ad partners — including Instagram, Google, and Apple — who send ads for our app to people who have been searching online for Black-owned restaurants or apps. That lets us tell the right audience about EatOkra without wasting our money sending ads to people with whom our mission doesn't resonate. It is an incredibly cost-effective way to reach customers and grow our business.

Here's the second way data is critical to our business: We sell ad-space on our app. That ad-space is valuable *thanks in large part to data*. Here's what I mean. If someone is using EatOkra, they're likely interested in supporting other Black-owned businesses — which makes our app the perfect place for those businesses to advertise. It's a win-win-win. The other Black-owned business gains a customer, the customer connects with a business they want to support, and my business earns a steady revenue

stream from the sale of valuable ad space.

As you consider data privacy legislation, I strongly urge you not to overregulate how businesses can collect and use data. Some states have enacted strict limitations that only allow businesses to use data to fulfill a specific customer request, like completing a sale or return. If New York enacted those kinds of restrictions, I would lose the data that empowers me to find customers. At the same time, my ad-space would be worth far less, because — without data to power them — all digital ads would be less effective. In short, if the data supply dried up, my business model — which helps support thousands of other Black-owned businesses — would collapse. The same would be true for many minority-owned and -oriented businesses and apps.

As a final note, I'd like to point out that "carveouts" meant to exempt small businesses from data privacy regulations are largely meaningless. That's because almost any small business with a digital presence will easily exceed the proposed threshold of 50,000 customer data-points. In addition, most small businesses partner with larger digital businesses to help with their data-powered advertising and marketing. Those larger partners will certainly have to comply with the regulations, so small businesses will be seriously impacted, too. Worse, I'm now concerned that if a digital business like mine grows and succeeds, it will generate more customers and data, exceed proposed thresholds, and *then have to come up with an entire new digital marketing strategy*. That is, carveouts and thresholds effectively punish small businesses that use digital technology to succeed.

I understand and applaud your desire to keep New Yorkers' data secure. But overregulating data will crush New York's small businesses — especially those, like mine, that seek to reach — and empower — specific groups.

Thank you again for giving me the opportunity to share my perspective today.