NAIA
National Artificial Intelligence Association

August 20, 2025

__Via US Mail and Email__

The Hon. Ted Cruz
Chairman
Ctee. on Commerce, Science & Transportation
U.S. Senate
254 Russell Senate Building
Washington, D.C. 20510

The Hon. Maria Cantwell
Ranking Member
Ctee. on Commerce, Science & Transp.
U.S. Senate
254 Russell Senate Building
Washington, D.C. 20510

Re: THE CASE FOR THE AMERICAN DATA INTELLIGENCE ACT

Dear Mr. Chairman and Ms. Ranking Member:

NAIA commends the members of the Senate Committee on Commerce, Science and Transportation (the "***Committee***") for the thoughtful work on the AI Moratorium. NAIA supported this effort and takes heart that virtually every person and organization that commented on the moratorium cited the need for unifying Federal rules.

Since the moratorium was always a placeholder, we encourage the Committee to move ahead on a preemptive Federal statute. We appreciate the Chairman's recent statements affirming that goal.

In the 7 ½ years since General Data Protection Regulation (GDPR) took effect, most of the initial controversy around data privacy has been settled. In every meaningful way, starting with Apple's implementation of **APP TRACKING TRANSPARENCY** in 2020, Americans have made clear they want control of their personal information and to be free of commercial surveillance. ChatGPT has only reinforced the need for fair, reasonable and effective Federal rules on the use of personal information and development and use of artificial intelligence ("***AI***").

This letter describes NAIA's perspective on these issues and our recommendations for a new Federal statute. It reiterates our support of the Committee on these vital issues.

A. __President Trump's AI Action Plan__

First, a word on the newest development, the Administration's recent release of "***America's AI Action Plan (the "Plan")***" for "*winning the race*" for US global leadership of artificial intelligence. The Plan identifies 90 federal policy actions across the core pillars of "*Accelerate AI Innovation,*" "*Build American AI Infrastructure*" and "*Lead in International AI Diplomacy and Security.*"

The AI Action Plan contains many outstanding ideas and goals which NAIA supports, and we realize it will take time to implement. It kicks off with agency Requests for Information and a long series of research, technology and program studies by NIST, NAIRR, DOE, Department of Commerce, DoD, USDA, NIH, NSF, OMB and others. Several initiatives will likely lead to rulemakings that will roll out over the next 2-3 years. The national security and export controls can be implemented more readily.

One area we would like to address is the complex and confusing regulatory environment facing every business that collects and processes data. It takes nothing away from the importance of the issues we raise here, which are just as detrimental to AI innovation and global leadership as those targeted in the Plan.

We hope the Committee will continue to focus on the entire regulatory data landscape in the US, including in the states.

B. Some Key Conclusions

The following are our high-level conclusions regarding artificial intelligence and data privacy policy:

- There are 23 new state data privacy laws and 4 state AI laws with many more in the works. Some commenters don't count *consumer health data* laws as privacy laws, but we consider non-HIPAA health data as just another form of personal information. This landscape is very difficult to navigate and is only getting worse.

- Artificial intelligence laws are already here and expanding. They follow two basic models:

(i) specific prohibitions on specific harmful uses of AI technology and mandatory disclosure of the use of machine learning, the logic of its algorithms and the purpose of its automated decision making, or

(ii) detailed compliance regimes that mandate responsible AI development principles that must be in place before the system is built and must be applied throughout the system's lifecycle with continuous monitoring, testing and reporting.

(iii) Let's call the first model the Texas AI model and the second the EU & Colorado AI model (with California CPPA regulations somewhere in between).

- One problem with the Colorado model (which led to vetoes of AI bills in California and Virginia) is the lack of established standards by which to judge AI's performance. We need to distinguish the need for guardrails from imposition of smothering standards that are untested, unproven and immature. To realize the benefits of AI, we must give it time and space to develop while acting on its clear threats.

- The unacceptable risks of AI are particularly clear for the vulnerable and for our youth, who are subjected to the addictive effects of social media and the serious adverse impacts on their physical, mental and psychological health.

- Despite these new areas of AI focus, while state data privacy laws have expanded in recent years, their fundamental policies are substantially similar. If Congress could just enact the accepted consensus of these data privacy rules, it will advance important policy goals while providing time for AI compliance to mature.

- We are not the only country seeking to implement AI protections. For example, the Office of the Privacy Commissioner of Canada (OPC) is launching a consultation on a children's privacy code. Following the UN Convention on the Rights of the Child (UNCRC), the OPC defines children as those under age 18. It measures valid consent on the child's capacity, proposes "***privacy by default***" for location tracking, bans deceptive practices and requires privacy impact assessments.

- Europe is even working on amendments to GDPR to provide some flexibility for smaller company reporting. It has also considered a pause in implementation of the EU AI Act due to the lack of definite standards for responsible AI development (*i.e.*, valid, secure, resilient, transparent, explainable, accountable, human-centric, unbiased and privacy-enhanced);

- There are other important global leadership considerations for AI governance as Europe advances the EU Data Act, the Data Markets Act, the Data Services Act and others. The well-designed EU -US Data Privacy Framework requires a strong US regulator to protect the flexible transfer of EU data to the US.

- Finally, we believe that the objections to the AI Moratorium were misplaced. A Federal statute does not ***decrease*** data protection. It greatly expands it to the 27 or more states whose residents are either not currently protected or are given false protection by rules that are overreaching and conflicting. State AI laws are now being layered into this mix even though most of the new state data privacy laws already cover algorithms and AI.

- For context, if a company collects and processes ***personal information*** as defined in data privacy laws, it must comply with those laws and regulations. If they process any kind of data (not just personal data) to automate actions and make decisions, they must comply with AI laws. One does not replace the other. A company injecting personal data into AI models in Europe must comply with both GDPR and the EU AI Act. This is the same result in California, Colorado and Texas since all of them have both data privacy and AI laws.

- While the message is challenging, Congress should prohibit dangerous AI practices, enact reasonable AI guardrails and memorialize common sense data privacy rules that are consistent and understandable. That includes eliminating the end run on the state prohibitions of private rights of action through wiretapping and tracking technology lawsuits that were never meant to apply to the practices at issue.

C. The Current Legal Landscape

Attached as Appendix A is an overview of the key data privacy and AI laws that have been enacted. They reinforce the need for a single regulator to interpret and apply a new Federal law.

For the past 5 years, Federal data privacy legislation has deadlocked over two issues: (i) does the Federal law preempt state laws, and (ii) are violations of the statute subject to a private right of action.

As the AI Moratorium made clear, we believe there is now a broad consensus on the need for a common set of data privacy and AI rules. We believe it equally clear there should be no private right of action and that 95% of state data privacy laws got it right in prohibiting a private right of action for violations of those statutes.

The need for consistency in the interpretation of data privacy laws has even been recognized by the AGs of 7 states (California, Colorado, Connecticut, Delaware, Indiana, New Jersey & Oregon), who have formed a "*Consortium of Privacy Regulators.*" This approach, while helpful, cannot paper over the need for a uniform set of regulations promulgated, interpreted and enforced by a common regulator.

A word about liability. While state data privacy laws exclude a private right of action, they do not affect the private rights of action under state data breach laws. Also, there is no liability protection for harms caused by AI. Rather, damages from the use of AI are subject to standard tort, negligence and product liability laws.

Europe proposed a liability directive to address the difficulty of proving harms caused by "black box" AI tools. This directive sought to establish evidentiary presumptions in favor of claimants that would force AI developers to defend their AI operations. That effort is on hold for now but will likely return.

While we are not proposing any changes in the current liability regime for AI, we believe standard US tort law is sufficient protection for now and that a new Federal law, like state privacy laws, should preclude a private right of action for violations of the AI law.

A Federal bill should also eliminate the litigation harassment relating to tracking technologies that are data privacy claims masquerading as violations of wiretapping and common law privacy laws. They are often filed under laws permitting a private right of action such as the California Invasion of Privacy Act ("***CIPA***"). These are an abuse of judicial process as some appellate courts are now recognizing.

One final note on liability. Three states (Ohio, Tennessee & Nebraska) have enacted liability protections for businesses that have implemented a recognized data privacy framework (e.g., NIST, ISO, etc.). Ohio provides a safe harbor from data breach lawsuits; Tennessee provides an affirmative defense for violations of its data privacy law and Nebraska prohibits class actions against companies trying to do the right thing. These states recognize that businesses seeking to implement reasonable data protection programs can be victims just as data breach stakeholders are.

D. The American Data Intelligence Act ("*ADIA*")

We call our proposed Federal statute the "*American Data Intelligence Act*" ("***ADIA***") to cover both data privacy and AI. No single term is critical, and certainly others could be included, but we believe its elements reflect broad consensus among most constituencies. It would provide clear, consistent and predictable policies along with relief from the costs, delays and risks of the current regimes. Listed below are its elements:

(a) One Comprehensive Bill. A Federal statute must be comprehensive. ADIA would (i) memorialize broad data rights for consumers, (ii) standardize the consent rules for sensitive data, targeted advertising & profiling, (iii) incorporate ***privacy by design*** principles, (iv) preempt state laws that interfere with ADIA under consumer protection, wiretapping and state privacy laws, (v) incorporate responsible AI development principles in a rational manner, (vi) standardize data protection and AI risk assessments, (vii) shield US businesses from regulatory overreach, and (viii) protect victims of AI discrimination while protecting innovation.

(b) FTC Regulator. The FTC would be the primary Federal regulator and responsible for developing universal notice, compliance and assessment forms. It would be the PCAOB for purposes of the EU-US Data Privacy Framework and would be given broad regulatory authority for data protection and AI issues. Sector-specific data protection laws like HIPAA, Gramm-Leach Bliley and other Federal laws would retain their jurisdiction over sector data but the overlap of state data privacy laws would be eliminated.

(c) State Regulation of FTC Rules Retained. State regulators would retain their authority to interpret and apply ADIA in their own jurisdictions, similar to other Federal regimes such as CAN-SPAM.

(d) Artificial Intelligence Regulation.

(i) Prohibit dangerous, abusive and risky data processing and AI activities such as human manipulation, social scoring, certain biometric data collection and processing without consent, the production of sexually explicit content or child pornography and unlawful discrimination.

(ii) Prioritize transparency in AI development over strict compliance rules that apply before product completion, but with oversight of AI system operations and continuous monitoring, testing and reporting,

(iii) Establish responsible AI development principles for security, resilience, transparency, explainability, lack of bias, accountability & human centricity that apply in a manner that does not frustrate innovation,

(iv) Ensure effective export controls on international distribution & access to AI systems,

(v) Authorize an FTC sandbox for AI development under Federal oversight,

(vi) Require validation of IP rights, developer's right to model inputs & outputs and safe use of public AI development platforms.

(vii) Promote use of synthetic data & human-in-the-loop AI development and open source and open weight AI models,

(viii) Require use of valid training and test data and monitoring and validation of AI models throughout their life cycle,

(ix) Provide for FTC reporting of AI system security incidents,

(x) Require disclosure of generative AI uses with content alteration and indelible watermarking requirements,

(xi) Exclude national security and defense applications, and

(xii) Merge AI risk & compliance assessments with data protection assessments,

(e) ADIA Enforcement.

(i) Authorize state AG and data regulator enforcement of ADIA,

(ii) Prohibit private right of action for violations of ADIA.

(iii) Provide liability safe harbor for use of NIST RMF & other security frameworks,

(iv) Subject claims to a 60-day right to cure before an action can be filed,

(iii) Designate FTC as the Civil Liberties Oversight Board (PCLOB) to protect the validity of the EU-US Data Privacy Framework ("***DPF***") for EU transfers of data to the US, and

(iv) Pursue joint US-EU collaboration to harmonize data management enforcement by US & EU regulators.

(f) Children's Privacy Rights.

(i) Impose "***privacy by design***" principles for minor access and use of online platforms and devices,

(ii) Require informed parental consent for collection, use or disclosure of data of children under age 18 with parental disclosure & access controls for minor access to social media platforms,

(iii) Expand definition of children's data to include biometric identifiers (fingerprints, retina, voiceprints) and GPS location data,

(iv) Impose age verification for all websites, online services and mobile applications known to be accessed by minors,

(v) Require parental controls for website & device usage and the time and time of day spent on devices by minors,

(vi) Strictly limit sharing of children's data for profiling or targeted advertising,

(vii) Require social media design features that prevent addictive behavior, and

(viii) Increase fines and penalties for noncompliance.

(g) Data Privacy Regulation.

(i) Incorporate ***privacy by design*** into all data management regulations,

(ii) Apply ADIA to all profit and non-profit organizations, subject to small business and industry specific exemptions,

(iii) Provide that consumers, by default, control their personal data unless and to the extent they voluntarily and knowingly consent to other uses, including targeted advertising,

(iv) Impose unform data rights (right to know, correct, limit, opt-out, access & delete), including rights of opt-in or opt out,

(v) Ban online use of dark patterns,

(vi) Merge data protection & AI risk assessments,

(vii) Establish a common data security audit framework,

(viii) Preserve exemptions at the entity level for businesses regulated by HIPAA, GLBA, FERPA, FCRA, FCC & FTC but eliminate overlapping rules where data is regulated by both Federal law and state data privacy laws,

(ix) Eliminate record collection tests for applicability of the law but include a gross revenue test for a narrower set of regulatory requirements.

E. Conclusion

Thank you for considering these comments. We pledge our support for a broad, preemptive Federal law for data protection and AI and welcome the opportunity to work with the Committee on all of these and related issues.

About NAIA

The National Artificial Intelligence Association (NAIA) is a 503(c)(6) nonprofit organization comprised of over 1,500 members that seeks to preserve innovation and global competitiveness for American businesses subject to artificial intelligence & data privacy laws worldwide.

Sincerely, Caleb J. Max

Caleb Max

Co-Chairman and Director of Policy

National Artificial Intelligence Association

APPENDIX A

Summary of Data Related Laws & Regulations

1. ARTIFICIAL INTELLIGENCE LAWS

(a) **The EU AI Act.** The EU AI Act applies to general purpose and "***high risk***" AI models introduced into or used in Europe. Providers must (i) implement a responsible AI risk management system, (ii) train and continuously test the system with valid data throughout its lifecycle, (iii) validate the system as being "*accurate*," "*robust*," "*transparent*," "*secure*," "*unbiased*" and "*accountable*," (iv) perform an EU AI Act compliance assessment before launch and (vi) register the system in an EU-wide database. Fines can reach (the higher of) €15,000,000 or 3% of worldwide revenue.

(b) **State Artificial Intelligence Laws.** In the absence of a federal statute, states are enacting their own AI laws. This growing list includes Colorado, Utah, California, New York, Maine and Texas.

The Colorado AI Act mirrors the EU AI Act in many respects, labelling as *high-risk* any AI system making "*consequential decisions*" about education, employment, financial services, government services, healthcare, housing or insurance. It imposes detailed compliance requirements for foreseeable harmful uses of the system, the logic of its algorithms, its risk mitigation functions and AG reporting of algorithmic discrimination.

The governors of Virginia (**HB-2094**) and California (**SB-1047**) vetoed AI Acts that imposed the same scope of compliance regimes as Colorado and the EU due to their adverse effect on innovation. New York's Responsible AI Safety and Education Act **(AB-6453A)** (**RAISE Act**), if signed by the governor, will apply to large frontier model developers and is far narrower in scope than SB-1047 was so it may avoid SB-1047's fate.

Maine has enacted an AI transparency act that applies to AI tools that might deceive a "reasonable consumer" into thinking they are dealing with a human. It requires "clear and conspicuous" disclosure of the use of AI with violations subject to the Maine Unfair Trade Practices Act.

Utah's AI Act primarily covers generative AI, which it subjects to Utah's consumer protection laws, requiring disclosure of the use of an AI System in certain circumstances.

California also enacted AI training and transparency acts that require developers of generative AI models to publicly post 12 categories of information about the data used in their AI models and, for widely used platforms, to make an AI detection tool publicly and freely available. Another California law amends CCPA to grant data rights to the consumers whose personal information is used in AI models, tokens and weights. Finally, the California Privacy Protection Agency ("***CPPA***") is proposing detailed cyber audits and risk assessments for the use of automated decision-making technology ("***ADMT***").

When the Texas Responsible AI Governance Act (***TRAIGA***) was introduced, it was comprised of Colorado-type compliance rules. By the time it was enacted, it was greatly narrowed to prohibit specific harmful practices such as (i) human manipulation, (ii) the creation of social scores for natural persons based on their behaviors, (iii) capturing biometric data without consent, (iv) producing sexually explicit content or child pornography and (v) unlawful discrimination. TRAIGA also establishes a regulatory sandbox for AI system testing that protects AI developers from liability it they comply with NIST's AI Risk Management Framework (RMF).

2. Youth & Social Media Laws

Many state laws relating to minors' use of social media platforms have been enacted in recent years, including the following:

(a) Vermont enacted an Age-Appropriate Design Code Act that mirrors other US states and the UK. It applies to online services accessed by minors that collect personal information. Covered businesses may only collect and use minor personal data for the service the minor is actively using, and the AG is tasked with developing an age verification process,

(b) The Arkansas Children and Teens' Online Privacy Act provides data privacy protection to individuals between ages 13 and 16 and applies to operators of websites, online services and mobile applications. It also prohibits targeted advertising to children and teens,

(c) Arkansas SB 612 creates a private right of action for harm from social media platforms such as causing eating disorders, suicides or attempted suicides or platform usage addiction, though it does provide a safe harbor for prompt correction of the design, algorithm or feature,

(d) Nebraska enacted the Parental Rights in Social Media Act that restricts youth under age 18 from creating an account and requires age verification. Parents must consent to the opening of a social media account and can revoke their consent. It contains a private right of action for violations,

(e) The Florida Digital Bill of Rights requires certain social media platforms to prohibit certain Florida minors from creating new accounts and to verify the age of account holders,

(f) Georgia's Children on Social Media Act requires parental consent of an underage 16 minor's creation of a social media account and requires commercially reasonable efforts to verify the ages of account holders,

(g) Louisiana passed a law that restricts social media platforms' processing of personal data from minors under age 18 and restricts the display of targeted advertising to them, and

(h) California's Age-Appropriate Design Code Act regulates the delivery of online products, services or features to minors under age 18, requires the business to reasonably estimate the age of minors and to avoid designs that could harm minors.

3. Data Privacy Laws

(a) **GDPR.** GDPR has applies to the collection of EU personal data by both profit & nonprofit organizations, both online and offline. It taught us data subject rights (the right to know, correct, limit, opt-out, access & delete personal data) that are now part of every US data privacy law.

GDPR replaced the 1995 Data Protection Directive. "Directives" in Europe are a common set of guidelines that require each member state to pass a statute to implement. The '95 Directive led to many confusing, conflicting laws and led to GDPR. **Sound familiar? ADIA can be our GDPR.**

GDPR included the requirement of "***privacy by design***" (Article 25) in the design of data privacy programs requiring, *by default*, use of the most privacy protective rules. Had this requirement been included in CCPA and subsequent US data privacy laws, our task would be far less complex. The concept of *data minimization* is a weak substitute. ***Privacy by design*** should be included in any new Federal law.

(b) **What State Data Privacy Laws Have in Common**

Virtually every state data privacy law requires businesses to (i) fully disclose all categories of personal information collected, (ii) provide broad data subject rights, (iii) restrict the collection and use of sensitive data, (iv) control the transfer of data for targeted advertising and profiling, (v) require reasonable data security, and (vi) require broad data protection assessments that must be available to regulators on request.

All state data privacy laws other than Washington State exclude a private right of action for violations, though some trigger their own consumer protection laws. With no direct path to sue, plaintiff attorneys have filed class actions for the use of tracking technologies (cookies, web beacons, etc.) under state consumer protection laws, the Video Privacy Protection Act, common law privacy and the California Invasion of Privacy Act ("***CIPA***"), an anti-wiretapping law. Those cases are causing enormous costs and disruption to companies that often are merely monitoring their own website visitors.

A hopeful development is California **SB-690**, which would amend CIPA to exempt the use of tracking devices and tools used for "commercial business purposes." If enacted, it would drastically reduce the 1500 CIPA cases that were never intended to apply to the practices at issue. Unfortunately, the California Assembly recently classified SB-690 as a two-year bill, pushing relief off to at least 2027. ADIA should solve this issue directly and nationally.

(c) How State Data Privacy Laws Differ

While state data privacy laws are very similar in many ways, they differ in many other ways. For example, some state laws:

(i) apply to non-profit organizations while most do not,

(ii) require prior opt-in to the collection and use of sensitive information while others require a right of opt-out to such activities,

(iii) regulate online activities impacting the mental health of minors while others do not,

(iv) establish different ages of minority,

(v) impose different response deadlines for data access requests,

(vi) mandate automatic notices to regulators of denials of a deletion request while most do not,

(vii) the CCPA alone applies to employees and B2B contacts,

(viii) require prior notice and a right to cure for violations while others have no right to cure,

(ix) require disclosure of the "categories" of personal information collected while only California provides a list of categories (and says its list must be used if CCPA applies, and

(x) Washington State requires a separate consumer health data privacy notice under the Washington My Health My Data Act ("***WMHMDA***") and provides a private right of action for violations of the act, whereas other state laws provide no private right of action, and

(xi) Maryland, Connecticut, Washington & Nevada require prior consent for the collection of consumer health data and prohibit the geofencing of mental health and sexual health facilities.

Another stark difference is the jurisdictional triggers for applicability based on the number of state residents whose data is collected each year, as summarized below:

States	**Annual # of residents from whom personal data collected**
California, Colorado, Virginia, Utah, Minnesota, New Jersey, Iowa, Oregon, Indiana, Kentucky	100,000
Rhode Island, Maryland, New Hampshire, Delaware & Connecticut	35,000
Tennessee	175,000
Montana	25,000
Texas, Nebraska	One (1) resident

This letter and Appendix A were prepared with the assistance of NAIA's general counsel, Steve Britt (steve@thenaia.org), who holds IAPP's AIGP, CIPP/E & CIPM certifications.