National Artificial Intelligence Association

NAIA Comments to House Privacy Working Group

The document contains no business-proprietary or confidential information and may be used or distributed by the USG in any manner without attribution.

About NAIA

The National Artificial Intelligence Association (NAIA) is a 503(c)(6) nonprofit organization that ensures innovation and global competitiveness for American development and use of artificial intelligence ("***AI***"). Our membership is comprised of 750 public & private businesses, financial institutions, educational and other nonprofit organizations, healthcare providers, community organizations, small businesses and other stakeholders.

Our Comments

Our comments were developed with our leadership and members by our General Counsel, Steve Britt, Managing Partner of Britt Law LLC (steve@thenaia.org) (www.brittlawllc.com), who holds the AIGP, CIPP/Europe and CIPM certifications for artificial intelligence & data privacy.

A. Overview of Our Comments

We applaud the House Energy & Commerce Committee (the "***Committee***," "***you***" or "***your***") for tackling the complex issues of data privacy & artificial intelligence ("***AI***") with its REQUEST FOR INFORMATION (the "***RFI***"). We believe the RFI represents a unique opportunity to reset the rules that apply to every organization's use of data.

We begin with brief answers to your specific questions and then follow it with an overview of the legal landscape that now exists for "***data management,***" covering data security, data privacy and artificial intelligence. We hope this review will help level-set the context for the Committee's efforts and help build the case for a comprehensive solution.

We believe that addressing data privacy alone will not realize the potential benefits of the RFI, as AI is already presenting complexities for companies trying to understand and comply with unique state rules. Another strong argument for a comprehensive approach is the limited legislative calendar available for meaningful action. If we don't move quickly and comprehensively, we may not soon return to the data issues left behind.

Data management and AI regulations will not sit idly by as you proceed. For example:

- Data Transfers: GDPR prohibits the transfer of EU personal data to the US unless the US "adequately" protects the data consistent with GDPR. The EU-US Data Privacy Framework ("***EU-US DPF***") satisfies the lack of an "adequacy" finding by the EU, freeing businesses from having to use standard contractual clauses for cross-border transfers. Vacancies on the Privacy & Civil Liberties Oversight Board (PCLOB) should be filled. **A comprehensive Federal data privacy bill may ensure an EU "adequacy" determination and eliminate the need for the EU-US DPF**.

- US Development of AI. The EU AI Act applies to any AI System introduced into or used in Europe. This subjects all developers of AI Systems for use in Europe to the EU AI Act's strict compliance requirements,

- Preemption. The US needs one set of data subject rights based on privacy-by-design principles. **This can only happen with broad preemption of non-Federal laws**,

- Enforcement should be exclusively by the FTC & state AGs & privacy agencies, and

- Assessment Forms. The FTC should release form data protection and AI risk assessments to eliminate compliance uncertainties.

B. Answers to Your Specific Questions

I. Roles and Responsibilities

A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?

NAIA Comment: GDPR introduced the concept of data controllers (which set the rules for the use of personal data), data processors (which process the data for controllers) and third parties (which includes service providers, contractors & hosting providers). These terms have worked reasonably well. AI brings us new terms such as developers, deployers, importers and users. We need a common lexicon for data management that is codified across all US jurisdictions.

B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?

NAIA Comment: All data privacy laws require the implementation of reasonable data security protection and our primary goal for the regulation of financial services, securities, investment services, health care and other industries is clearer lines of separation for data privacy and AI regulation.

C. Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?

NAIA Comment: GDPR is the purest privacy statute because it applies to the collection and use of personal data by any size or type of entity, whether for profit or nonprofit and whether online or offline collection and use. We are sympathetic to considering an entity's size but believe the most beneficial goal for all entities is to unify and simplify the regime for data management.

II. Personal Information, Transparency, and Consumer Rights

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

NAIA Comment: State data privacy laws have reached consensus on definitions of both personal information and sensitive data, though the latter is expanding with the inclusion of GPS location data, biometrics and other terms. The expansion of legal requirements in individual state laws is introducing unproductive levels of complexity. Maryland's strict limits on the collection of personal data and the processing or transfer of sensitive data, *regardless of consumer consent*, is on the right track of how we should rethink Federal data management rules.

B. What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?

NAIA Comment: Full and detailed disclosure and a requirement of express user consent should apply to any use of data beyond the purpose of the data controller's initial collection thereof.

C. Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?

NAIA Comment: Consumer protection laws, wiretapping statutes, the California Invasion of Privacy Act, the Video Privacy Protection Act and common law privacy acts are the basis of private lawsuits and an end run on the lack of a private right of action in almost all data privacy statutes (excluding consumer health data laws). We believe the issue of a private right of action in all data management laws should be dealt with head-on and follow the initial lead of the states in prohibiting them. We also believe that all enforcement actions by any agency or person should require prior notice and a right to cure.

D. What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?

NAIA Comment: As referenced Section II.A above, we believe that all uses of sensitive personal information should require prior disclosure and express consent for any use by any person beyond the transaction giving rise to the initial collection of data.

III. Existing Privacy Frameworks & Protections

A. Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.

NAIA Comment: Many of the 23 state data privacy laws are not yet in effect and only a handful of states have enacted regulations. This confusing matrix will only get worse, forcing businesses to choose between (i) a nationwide solution that facilitates consistent program operations, at the risk of violating individual state rules, and (ii) a *whack-a-mole* process of individual state compliance that cannot possibly stay current. Our regime for data protection should not force this predicament on our businesses.

B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.

NAIA Comment: Data privacy protections are incredibly fragmented, triggering consumer protection, wiretapping and common law privacy lawsuits to make up for the fact that 95% of data privacy laws do not authorize a private right of action. We should continue to prohibit a private right of action in a Federal data management law.

C. Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?

NAIA Comment: We can only solve the unfair and unproductive regime now rolling out with a universal preemption of data management laws and regulations, including consumer protection, common law privacy and consumer health data laws.

D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA) and transfer of personal information.

NAIA Comment: This is an important area for analysis as consumer health data laws, tracking technology rules and other issues are moving outside traditional Federal regulatory regimes and creating additional uncertainty and compliance issues. We welcome a dialogue with the Committee in the context of other progress on a Federal data management law.

IV. Data Security

A. How can such a law improve data security for consumers? What are appropriate requirements to place on regulated entities?

NAIA Comment: For several years, states have been amending their data breach notification laws to require reasonable data security. All data privacy laws require reasonable data security and California's new assessment regulations provide reasonable specific audit

requirements. See Section VI.C below regarding state safe harbors from data breach litigation.

V. Artificial Intelligence

A. How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?

NAIA Comment: These state requirements must be subject to preemption or the rolling conflicts in data privacy laws will just be repeated for AI. We must act comprehensively and create regimes that will be honored by other regulators globally in order to support our technology developers and innovators.

VI. Accountability & Enforcement

A. Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.

NAIA Comment: This is the regime that applies to CAN-SPAM among others. We believe it is the only regime that can meet our policy goals of protecting victims while preserving US innovation and global technology leadership.

B. What expertise, legal authorities, and resources are available—or should be made available—to the Federal Trade Commission and state Attorneys General for enforcing such a law?

NAIA Comment: Exclusive plenary authority.

C. How could a safe harbor be beneficial or harmful in promoting compliance with obligations related to data privacy and security?

NAIA Comment: Ohio, Utah, Connecticut, Iowa, Oklahoma & Tennessee have passed versions of safe harbor laws that provide an affirmative defense to data breach tort claims if the company had implemented a cybersecurity program meeting industry best practices.

VII. Additional Information

We welcome any additional information that may be relevant to the working group as it develops a comprehensive data privacy and security law.

NAIA Comment: We provide additional context for these issues below and then outline our proposal for a comprehensive Federal data management statute.

C. Current Legal Landscape

Here is our review of the data management laws that have passed since 2022. We believe this explains the need for a broad, comprehensive bill addressing data management issues:

a. **GDPR.** Effective in 2018, GDPR automatically applies to all 27 EU member states and the collection of EU resident data by both profit & nonprofit organizations, online and offline. It applies to the collection of EU data by any organization located anywhere in the world.

   GDPR taught us data subject rights (right to know, correct, limit, opt-out, access & delete), which are now included in all US data privacy laws. GDPR imposed "***privacy by design***" that required implementation of designs that are the most protective of data privacy. Had ***privacy by design*** been included in US data privacy laws, it would have greatly simplified our data regulation challenges. We believe it should be part of a new regime going forward.

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

c. **State Artificial Intelligence Laws.** In the absence of a Federal AI law, states are enacting their own AI laws as follows:

   Colorado Artificial Intelligence Act

   Colorado's AI Act, effective February 1, 2026, mirrors the EU AI Act. It prohibits algorithmic discrimination in the making of "***consequential decisions***," which are those affecting a user's access to education, employment, financial services, government services, healthcare, housing or insurance.

   Colorado AI developers must document the foreseeable harmful uses of the system, explain the provenance of the system's training data, define the logic of its algorithms, explain its risk mitigation measures, and publish a statement on how the system manages known or foreseeable risks. Instances of algorithmic discrimination must be reported to the Attorney General.

Utah Artificial Intelligence Act

Utah 's artificial intelligence law took effect on May 1, 2024 and primarily covers generative AI, which it subjects to Utah's consumer protection laws. A person using generative AI in a regulated business must disclose, ***if asked***, that he or she is interfacing with a machine. A person providing services of a licensed occupation must ***affirmatively inform*** consumers they are interacting with AI.

California AI Acts and Cyber, Risk & ADMT Regulations

In 2024, California passed several AI laws, including the following:

(i) **AI Training Data Transparency Act:** Effective January 1, 2026, developers of generative AI models must publicly post on their web site 12 pieces of information about the training data used in their systems.

(ii) **(SB 942) California AI Transparency Act:** Effective January 1, 2026, generative AI systems producing audio-video content for 1,000,000 or more monthly users must make an AI detection tool publicly and freely available to its users.

(iii) **(AB 1008) Amendments to CCPA:** CCPA was amended to cover personal information in AI models, giving data rights to AI data, tokens and weights.

In addition, the California Privacy Protection Agency ("***CPPA***") is expected to propose regulations covering the following activities:

- **Cybersecurity Audits**

Every business processing data that poses a significant risk to consumers must complete an annual cybersecurity audit of key security controls performed by a qualified independent professional.

- **Risk Assessments**

Every business whose processing of data involves the (i) selling or sharing of personal information, (ii) the processing of sensitive information, (iii) the use of automated decision-making technology ("***ADMT***"), or (iv) for training ADMT must prepare a risk assessment that explains the quality of the data, the logic of the algorithms and the use of system outputs. A version of the assessment must be submitted to the CPPA.

- **ADMT Regulations**

A business that uses ADMT for "***significant decisions***" about a consumer regarding financial services, housing, insurance, education, employment, compensation,

healthcare or for extensive profiling must provide a "***Pre-Use Notice***" of the purpose of the ADMT, the consumer's right to opt out of such use, how the ADMT works, its logic, its intended outputs and how the business will use those outputs.

d. **State Data Privacy Laws.**

Our 23 state data privacy and "***consumer health data***" laws share many similar terms.

For example, virtually all of them require 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 available to regulators on request.

However, these similarities are overtaken by a broad range of conflicting or inconsistent terms. For example, (i) some state laws apply to non-profit organizations while most do not, (ii) some require prior opt-in to the collection and use of sensitive information while others require a right of opt-out to such activities, (iii) some regulate online activities impacting the mental health of minors and others do not, (iv) the age of minority varies by state, (v) the response deadlines for data access requests vary, (vi) some states mandate automatic notice to regulators for denials of a deletion request while others do not, (vii) the CCPA applies to employees and B2B contacts whereas other states exclude those categories of users, (viii) some states require prior notice and a right to cure for violations of the act while others have no right to cure, (ix) all states require disclosure of the "categories" of personal information collected while only California provides a list of categories, and (x) Washington State requires a separate consumer health data privacy notice under the Washington My Health My Data Act ("***WMHMDA***").

Perhaps the starkest difference in state data privacy laws are the jurisdictional triggers for applicability based on the number of records of the state's residents collected each year as summarized below:

States	**Annual # of residents from whom personal data is collected**
California, Colorado, Connecticut, Virginia, Utah, Minnesota, New Jersey, Iowa, Oregon, Indiana, Kentucky	100,000
Rhode Island, Maryland, New Hampshire, Delaware	35,000

Tennessee	175,000
Montana	50,000
Texas, Nebraska	One (1) resident
Florida	$1B in revenue

Almost all state data privacy laws preclude a private right of action for violations of the laws with the notable exception being Washington's My Heath My Data Act and Virginia's new consumer health data act (SB 754). With no direct path to sue, plaintiff attorneys have filed a series of class actions under state consumer protection, wiretapping, the Video Privacy Protection Act, common law privacy and California Invasion of Privacy Act.

As to AI, nothing changes traditional product liability, strict liability and negligence (tort) laws relating to the use of AI. Given the complexity of AI compliance, AI development definitely faces substantial litigation risk.

D. The American Data Management & AI Act ("*ADMAIA*")

NAIA recommends enactment of a comprehensive data management bill that we have named the "***American Data Management & Artificial Intelligence Act***" ("***ADMAIA***"). It has the following key elements:

a. One Comprehensive Bill. ADMAIA is a comprehensive bill that would (i) memorialize the data rights of consumers, (ii) standardize consent rules for sensitive data, targeted advertising & profiling, (iii) incorporate privacy by design principles, (iv) preempt all related state data laws, including consumer protection, wiretapping and state privacy laws, (v) incorporate responsible AI development principles with self-certification of AI standards that are not yet adopted, (vi) standardize data protection and AI risk assessments, and (vii) provide a sound liability regime with no private right of action but with a right to cure. Virginia and Utah data privacy acts are balanced models for a Federal statute.

b. Data Privacy Regulation. ADMAIA would (i) incorporate *privacy by design* principles that facilitate a privacy label with exceptions solely for express consent, (ii) ban online use of dark patterns, (iii) preempt all state laws & regulations applicable to data use, (iv) eliminate overlaps between state laws and Federal sector laws (HIPAA, FCRA, GLBA, etc.), (v) apply to nonprofit organizations, (vi) provide small business exemptions, (vii) merge requirements for data protection and AI risk assessments with FTC approved forms, and (viii) adopt a common data security audit framework.

c. Artificial Intelligence Regulation. For AI, ADMAIA would (i) prioritize transparency in AI development over assessments, (ii) impose trustworthy AI standards of security, resilience, transparency, lack of bias and human centricity, (iii) ensure secure export controls on international distribution and access to AI technologies, (iv) expand access to open source software under Responsible AI Licenses (RAIL), (v) promote use of synthetic training data and human oversight of AI development, (v) merge data protection and AI risk assessments, (vi) require disclosure of altered content by generative AI, and (vii) authorize quantum computing research for building synthetic data for AI models.

d. Enforcement. Enforcement of ADMAIA would vest solely in the FTC and state attorneys general and regulators. No private right of action would exist for violations of ADMAIA and a right to cure would be provided for any regulatory action.

e. Children's Privacy Rights. ADMAIA would (i) require informed parental consent for online services that collect, use or disclose the personal information of youth under age 18, (ii) expand the definition of children's data to include biometric identifiers and GPS location data, (iii) impose strict limits on the sharing of children's data for targeted advertising, (iv) require social media providers to prevent addictive behavior on their platforms, and (v) increase fines and penalties for noncompliance.

E. Conclusion

Thank you for the opportunity to submit these Comments. We look forward to supporting the Committee's efforts on data management.

Sincerely, NAIA

Steve Britt, General Counsel, on behalf of the Board of Directors of the National Artificial Intelligence Association