

April 7, 2025

RE: National Conference of State Legislatures Comments to the House Energy and Commerce Privacy Working Group

Members of the House Energy and Commerce Privacy Working Group:

Thank you for the opportunity to submit these comments on behalf of NCSL, the bipartisan organization representing the legislatures of our nation's states, territories, commonwealths and the District of Columbia. Our mission is to ensure that states have a strong, unified voice in the federal system as well as to advance the effectiveness and independence of state legislatures and foster interstate cooperation. We provide research, technical assistance and opportunities for policymakers to exchange ideas on pressing issues, ensuring that state perspectives are well represented in the national dialogue.

We have directed our answers to the questions we believe are most pertinent to state legislatures and where we received substantial input from our members. We hope this is just the start of the conversations and collaborations NCSL and its individual members will be having with members of the working group and others on the House Energy and Commerce Committee. We appreciate your consideration of these recommendations and look forward to working with you on the important issue of data privacy and security for all.

### **I. Personal Information, Transparency, and Consumer Rights**

NCSL supports the following principles in formulating laws and regulations that impact data privacy, security and online safety:

With the proliferation of data online, including the internet of things and mobile devices, the regulation of the collection, sales and transmission of consumer data is increasingly a priority for state lawmakers. NCSL recognizes the importance of consumer data privacy and security protections, as well as the role of the states as leaders in establishing those protections for their constituents.

States are working to protect against data breaches, mishandling of data and non-transparent sale of consumer data in a way that balances myriad competing interests and allows for innovation while safeguarding the rights of consumers.

Regarding children and adolescents, the internet poses certain increased risks as they may not be able to recognize dangerous situations online. Strong privacy laws combined with online safety laws could be a critical part of alleviating the mental health harms facing young people. States have enacted comprehensive privacy, security and online safety laws in the past few years and will not hesitate to act to protect the privacy, security and mental health of their residents, particularly their children and adolescents.

#### **Wayne A. Harper**

President, NCSL  
Senate  
President  
Pro Tempore, Utah

#### **John Snyder**

Staff Chair, NCSL  
Transportation Committee  
Staff Administrator,  
Kentucky Legislative  
Research Commission

#### **Tim Storey**

Chief Executive Officer,  
NCSL

If Congress develops a national standard on privacy, NCSL strongly encourages consultation with states and recognition of state expertise in addressing the varied interests of each state's unique constituency. In any federal legislation, NCSL urges Congress to prioritize transparency and informed privacy decisions to carefully consider the best method for consumer notice, disclosure and consent, and to ensure increased safeguards to protect the privacy, security and mental health of children and adolescents. NCSL further encourages Congress to consider issues of third-party access and sales, disposal of data, consumer rights to control data and the burden of protecting consumer data. States have also engaged in significant deliberation over the applicability of consumer protections to various data types, including how to define personal data and how categories of data collectors or sellers should be regulated.

NCSL also recognizes the rapidly evolving nature of data collection and urges Congress to consider biometric data, location data, and technologies like facial recognition and artificial intelligence when considering federal legislation.

Finally, NCSL strongly urges Congress to engage in regular and meaningful consultation with state lawmakers when considering federal privacy and security legislation, including legislation aimed at protecting children and adolescents. State lawmakers should be included in hearings, review of draft language, principle setting and other Congressional activity intended to impact state regulatory regimes. There is much the federal working group can learn by including states and NCSL in its policy considerations.

### **III. Existing Privacy Frameworks & Protections**

#### **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.**

Our bipartisan members have shared concerns that comments about "fragmentation" are overstated and are the result of differing pressures from industry who have actively contributed to this patchwork system. Several of our legislators point out that industry leaders had an opportunity to unite around state legislation that provided strong, uniform privacy laws, like California's Consumer Privacy Act. Instead, many companies have pushed for weaker laws in other states while simultaneously decrying the lack of uniformity—suggesting that their true objective is to limit regulation rather than ensure consistency. The working group should explore these state legislative experiences with input from legislators in states that have enacted privacy legislation.

A federal privacy framework is necessary to set a baseline standard that protects consumers, is straightforward for businesses and prevents a regulatory race to the bottom. However, any federal legislation must be carefully crafted to preserve states' ability to implement stronger protections where needed. An inflexible and complete preemption of state privacy laws that does not allow for states to tailor legislation to their specific and unique needs will stifle states' ability to respond to emerging risks.

State legislators who have been through the drafting, stakeholder engagement, hearings and ultimate passage of state privacy legislation maintain that, from a business perspective, the cost of compliance with multiple state laws can be mitigated by adopting privacy policies that align with the highest standards across jurisdictions. Many companies already take this approach, ensuring they meet the most stringent requirements rather than tailoring policies state by state. While compliance does impose some costs, these are often manageable and should be weighed against the broader societal and economic benefits of strong privacy protections.

Ultimately, the challenge is not fragmentation itself but the lack of a strong federal foundation that ensures basic consumer rights while allowing states to build upon those protections as necessary.

Moreover, there is, in fact, considerable uniformity in the way states have legislated to protect our mutual constituents. As Congress once again begins developing proposed legislation regulating data privacy and security, we urge this working group to ensure such legislation does not undermine the thoughtful work of the states and the protections they have already established.

State-level privacy protections have increasingly aligned around core principles, creating a more consistent framework for both consumers and businesses. Across states like California, Colorado, Connecticut, Texas, Virginia, and many others, privacy laws share key provisions that grant consumers significant rights over their personal data. In nearly every state with a privacy law, consumers can access, delete, and transfer their personal data, allowing them to have greater control over how businesses handle their information. Furthermore, most states provide consumers with the right to opt out of the sale of their data, targeted advertising and profiling for automated decision-making, reinforcing a broad commitment to data privacy.

State privacy laws also establish clear protection for sensitive personal data, requiring either opt-in consent or allowing consumers to opt out of its processing. Categories of sensitive data, such as racial or ethnic origin, biometric and genetic information, precise geolocation, health data, and financial data, are widely recognized across these laws. Additionally, businesses across multiple states are subject to reasonable security requirements to protect consumers' data from breaches and misuse, further demonstrating a common approach to safeguarding personal information.

Moreover, most state laws follow similar applicability thresholds, typically based on either the number of consumers affected, or the nature of data processing. Enforcement is also largely consistent, with state attorneys general overseeing compliance in nearly every jurisdiction. While some differences exist, such as California's unique private right of action, most businesses can adopt a single standardized privacy framework that meets the essential requirements of multiple states, reducing the burden of completely different laws in each location.

The broad adoption of these shared privacy laws signals a similar trend toward stronger consumer rights and responsible data practices across the U.S.

**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?**

NCSL strongly urges this working group and other federal lawmakers to avoid any preemption of state privacy laws when developing federal comprehensive data privacy legislation. Instead, Congress should maintain a collaborative federalism that respects states' roles and empowers them to remain the laboratories of democracies our mutual constituents have come to depend upon. This path forward bolsters the trust residents place in their state and local leaders to protect their interests and fosters unity and coordination among states without enshrining uniformity.

Since 2018, states have demonstrated their ability to act thoroughly, quickly and effectively to meet the challenge of protecting consumer data privacy and security while allowing industry to continue to innovate. The ability of state policymakers to adapt rapidly and nimbly to changing technological applications to protect consumers surpasses any action taken by Congress or the federal government. This will be a truth for the foreseeable future and Congress should not pursue a comprehensive data privacy law that limits states' ability to act in the best interests of residents and businesses.

NCSL has spoken at length with our membership and both our Republican and Democratic legislators uniformly agree that it is imperative for Congress to adopt legislation that sets a federal floor, not a ceiling, for critical privacy rights. A federal legal framework for privacy protections must allow flexibility to keep pace with technology and support residents of different states who may wish to have privacy protections that are stronger than those that can be provided through legislation requiring congressional consensus. This is best achieved through federal legislation that respects and does not override more protective state laws.

While a federal law would apply nationwide, any state privacy laws offering additional protections would remain effective. States would also retain the authority to enact new privacy laws. If a federal minimum standard were established, state privacy laws would only be invalidated if they provided protections that were less than the federal minimum.

Our American federalism creatively unites states with unique cultural, political and social differences into a strong nation. It is built on the concepts of shared sovereignty and delineated powers. The Tenth Amendment is the cornerstone of constitutional federalism and reserves broad powers to the states and to the people. Federalism protects liberty, enhances accountability and fosters innovation with less risk to the nation.

“The Constitution divides authority between federal and state governments for the protection of individuals.” *New York v. United States* 505 U.S. 144 (1992). This careful balance enhances the express protections of civil liberties within the Constitution. At its core, comprehensive privacy legislation is the protection of an individual’s most sensitive and self-defining information.

By retaining power to govern in this area, states can more confidently innovate in response to changing needs. As Justice Louis Brandeis wrote: “It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.” *New State Ice Co. v. Liebmann*, 285 U.S. 262 (1932)

It is a suitable role for the federal government to encourage innovation by states. Our country's founders did not contemplate a perfect union, but rather a more perfect union, meaning there must be room for policy experimentation and different methods of self-government at the state level. That is why Congress must allow states the flexibility to shape public policy. Creative solutions to public problems can be achieved more readily when state laws are accorded due respect. Moreover, states are inherently capable of moving more quickly than Congress to innovate, respond, correct errors observed in policy and be more sensitive to public needs. Again, this is particularly true when it comes to rapidly changing technological advances that underlie data privacy legislation.

Currently, 19 states—California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia—have enacted comprehensive data privacy legislation. This working group and Congress as a whole should respect the innovative, responsive, and thoughtful efforts of state policymakers. As with many recent areas of congressional action, they should safeguard a state-driven approach in the rapidly evolving and increasingly important field of data privacy and security.

Lastly, many of our members have pointed out that there is precedent for Congress ensuring a role for states in the legislative and regulatory arena, citing as examples HIPAA, FCRA, GLBA and COPPA, which provide a federal floor, but not a ceiling, of protections for individuals and businesses.

#### **D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA)?**

As this document has suggested, federal legislation that provides a basic framework for comprehensive privacy can be integrated with existing federal laws that also require some level of privacy. Legislative language such as, “this bill does not supplant any privacy standards or requirements found in other federal laws with privacy components,” addresses this question. Additionally, NCSL recommends this working group look to the states for a solution. All 19 states with comprehensive privacy laws provide exemptions for federal privacy laws and consistently offer data-level exemptions for entities subject to the Family Educational Rights and Privacy Act (FERPA). In fact, every state except New Jersey includes FERPA-related data-level exemptions. When it comes to GLBA, all states have exemptions, with 15 offering data-level exemptions and 16 providing entity-level exemptions. Similarly, every state law includes data-level exemptions tied to HIPAA, and over half of the states—10 in total—go further by including entity-level exemptions as well. All 19 states also offer data-level exemptions for FCRA and the Driver’s Privacy Protection Act (DPPA). Additionally, eight states align their definition of a child with COPPA, setting the threshold at under 13 years of age.

## **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?**

A federal data privacy law should not preempt state automated decision-making legislation. States must be allowed to innovate in this area and nimbly adjust to the integration of AI into our communities.

States are considering new AI laws, with Colorado passing the first-in-the-nation comprehensive AI law in 2024 containing new transparency and reporting requirements for deployers and developers of high-risk AI systems. The law creates consumer rights such as being notified about the use of the high-risk AI system, correcting inaccurate personal data processed by the system and the ability to appeal the decision made by the system, among other elements. Use of high-risk AI systems may also qualify as profiling under Colorado's Privacy Act, which requires notice of profiling and the right to opt out. This example shows how state legislators are considering how data privacy and AI-regulation can be used together to protect consumers.

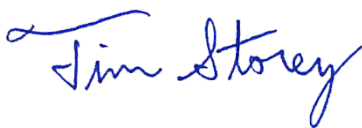
Definitions of "processing" and "profiling" in most state privacy laws include automated processes that apply to automated decision-making. State laws across the nation are similar in terms of providing the right to opt out of processing for targeted or cross-contextual behavioral advertising, sale of personal data and profiling. Most U.S. state privacy laws also require data protection assessments for high-risk processing activities.

## **VI. Accountability & Enforcement**

NCSL maintains that states must retain the right to establish their own legal rights of action, enforcement regimes and oversight authority. NCSL urges Congress to protect the right of the states to enforce data privacy provisions in any federal legislation.

Once again, thank you for the opportunity to provide comments. NCSL would appreciate the opportunity to meet with members of the working group to discuss how state legislators can be of assistance as the committee develops its privacy policy. We believe our bipartisan group can offer valuable insights into this critical work. If you have any questions, please feel free to contact me, or have your staff contact the following members of our state-federal affairs team: Barrie Tabin at [barrie.tabin@ncsl.org](mailto:barrie.tabin@ncsl.org)/ 202-624-3586 or Susan Frederick at [susan.frederick@ncsl.org](mailto:susan.frederick@ncsl.org)/202-624-3566.

Sincerely,



Tim Storey  
Chief Executive Officer  
National Conference of State Legislatures