National Small Business Association

Re: "Request for Information to Explore Data Privacy and Security Framework"

The National Small Business Association (NSBA) thanks Chairman Guthrie, Vice Chairman Joyce, and the Energy and Commerce Committee's data privacy working group ("Working Group") for the opportunity to respond to this request for information (RFI) exploring a framework for data privacy and security. NSBA is the nation's oldest small business advocacy organization representing the 70 million owners and employees that make up American small business, championing efforts that foster the growth, strength, and impact of small businesses.

As small business champions, we encourage the Working Group to consider the following principles in crafting a comprehensive data privacy and security law ("Law"):

- **Roles and Responsibilities**: The Law must consider an entity's size.
- **Existing Privacy Frameworks & Protections**: The Law must fully preempt existing state laws.
- **Artificial Intelligence:** The Law should preempt existing state-level AI frameworks and must provide flexibility in any provisions governing automated decision-making.
- **Accountability & Enforcement:**
    - The Law must prohibit a private right of action.
    - NSBA supports delegating enforcement authority to the Federal Trade Commission (FTC), but such authority must be clearly delineated such that the risk of capricious enforcement can be fully mitigated.

<u>Roles and Responsibilities: Considering an Entity's Size in Delineating Entity Obligations</u>

NSBA urges the Working Group to consider an entity's size in crafting the Law. By taking entity size into consideration, the Working Group can ensure that compliance requirements do not place an undue strain on small entities' resources. Reducing these compliance burdens will protect small entities from disproportionate regulatory impacts.

Nearly half of our members, when surveyed, indicated that they themselves as small business owners are primarily responsible for handling their online security. Meanwhile, only a quarter indicated that they outsource their online security operations and a little less than that indicated that they delegate these responsibilities to a member of their staff.[1]

[1] NSBA, "Issue Brief: Data Privacy Regulations," Jan 2025, https://www.nsbaadvocate.org/_files/ugd/fec11a_339fcee455e34614bcbc2c5827d31ca6.pdf.

In the absence of a dedicated digital security compliance staff, small businesses are at a disadvantage parsing through complex regulatory requirements. The EU's General Data Protection Regulation (GDPR), "which many states have cited as a model for their own privacy laws,"[2] exemplifies this challenge.

GDPR, among other things, "requires businesses of all sizes and sectors to have a dedicated data protection officer to guarantee compliance with the law." As acknowledged in a 2022 Information Technology & Information Foundation (ITIF) report, "[f]or a small business, hiring a data protection officer would be a significant endeavor likely involving a trade-off between hiring for compliance purposes and hiring for expanding a business's product or service." In contrast, one model that has accounted for this problem is the Virginia Consumer Data Privacy Protection Act (VCDPA), a comprehensive state privacy law that excludes nonprofits and small businesses from its requirements. [3]

Accordingly, we strongly encourage the Working Group to consider a carveout for small businesses, one that is clear and unequivocal, from any strenuous compliance requirements of a prospective data privacy and security law. NSBA recommends that the Working Group look to models like VCDPA, which upholds consumer data privacy rights while maintaining a small business-friendly regulatory posture, in crafting a carveout.

Existing Privacy Frameworks & Protections: Only Federal Preemption Can Alleviate the Burden of the Existing State Patchworks

NSBA urges the Working Group to craft a Law that fully preempts the existing state patchwork of data privacy laws. The current fragmented system creates significant compliance burdens for small businesses in particular, and in an increasingly digital economy, what could previously be deemed "state lines" becomes blurred.

The patchwork of data privacy laws in the U.S. is untenable for the future of America's small businesses: according to a 2023 U.S. Chamber of Commerce ("Chamber") report, "7 in 10 small businesses [stated] that limiting access to data could be harmful to their operations," noting that "most small businesses are concerned about having to comply with out-of-state technology regulations." The Chamber report also referenced the aforementioned ITIF

[2] Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," Information Technology & Innovation Foundation, Jan 2022, https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

[3] Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," Information Technology & Innovation Foundation, Jan 2022, https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

report, which "highlighted that a 50-state patchwork of privacy laws could cost the economy $1 trillion and specifically $200 billion for small businesses."[4]

As such, we reiterate our call for the Working Group to craft a Law that contains strong preemption language so that there is little confusion that the federal law supersedes state laws that address privacy. Only this language can provide uniformity in privacy standards and undo the complex patchwork of data privacy laws in the U.S.

Artificial Intelligence: Federal Preemption and Flexibility

Consistent with NSBA's position on federal preemption of state data privacy laws, we recommend that a comprehensive data privacy and security law preempt existing state-level AI frameworks. Additionally, NSBA encourages the Working Group to provide flexibility for small entities in any of the Law's provisions governing automated decision-making.

In the aforementioned Chamber report, over half of small business owners indicated they were "worried that changing technology regulations could harm [their businesses]," a finding that was underscored in the Bipartisan House Task Force on Artificial Intelligence's ("House AI Task Force") 2024 report.[5] The Chamber report also identified "staying informed about new [AI] compliance requirements" as a key challenge for small businesses.[6] Moreover, as demonstrated by the current state of patchwork data privacy laws, small businesses and the economy at large cannot afford to shoulder the burdens of a similar model for AI laws.

While we strongly support federal preemption of state-level AI frameworks, we also caution that preemption alone is unlikely to be sufficient to stave off the challenges that small

---

[4] U.S. Chamber of Commerce Technology Engagement Center, "Empowering Small Business: The Impact of Technology on U.S. Small Business," Sept 2023, https://www.uschamber.com/assets/documents/The-Impact-of-Technology-on-Small-Business-Report-2023-Edition.pdf; *see also* Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," Information Technology & Innovation Foundation, Jan 2022, https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

[5] U.S. Chamber of Commerce Technology Engagement Center, "Empowering Small Business: The Impact of Technology on U.S. Small Business," Sept 2023, https://www.uschamber.com/assets/documents/The-Impact-of-Technology-on-Small-Business-Report-2023-Edition.pdf; *see also* U.S. House of Representatives, "Bipartisan House Task Force Report on Artificial Intelligence," Dec 2024, https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf.

[6] [6] U.S. Chamber of Commerce Technology Engagement Center, "Empowering Small Business: The Impact of Technology on U.S. Small Business," Sept 2023, https://www.uschamber.com/assets/documents/The-Impact-of-Technology-on-Small-Business-Report-2023-Edition.pdf; *see also* U.S. House of Representatives, "Bipartisan House Task Force Report on Artificial Intelligence," Dec 2024, https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf.

businesses face in complying with complex regulatory regimes. As such, we echo the House AI Task Force's recommendation to consider approaches to crafting an AI framework as part of a larger data privacy and security law "that are not "one-size-fits-all" but tailored specifically to the type or size of audience a ruling would affect."[7]

Additionally, NSBA recommends that the Working Group adopt a tailored approach to any provisions governing automated decision-making. During the Biden administration, the Department of Labor's (DOL) Wage and Hour Division (WHD) published sweeping guidance that sought to clarify employer obligations under federal labor laws as they pertain to use of automated systems and AI. The guidance, which is no longer publicly available, essentially warned that certain uses of AI in the workplace may constitute violations of the Fair Labor Standards Act (FLSA) – leaving small employers in particular with uncertainty and stifling innovative approaches to AI use in the workplace.[8]

As small employers are more likely to be at the nascent stages of exploring the benefits and risks of AI use in the workplace, it is imperative that the Working Group provide maximum flexibility to small businesses to avoid further compliance challenges. In short, NSBA looks forward to collaborating with the Working Group to ensure that a comprehensive data privacy and security law covering AI (1) preempts state-level frameworks, (2) provides flexibility for small entities eager to integrate AI into their decision-making processes, and (3) does not hinder AI adoption by small businesses.

Accountability & Enforcement: Beware of Private Rights of Action and Capricious Enforcement

NSBA urges the Working Group to craft a Law that prohibits private rights of action and recommends that the Law delegate enforcement authority to the FTC in a clearly delineated manner such that capricious or inconsistent enforcement by future administrations will be avoided. In doing so, the Working Group can ensure that small businesses will be protected from frivolous litigation in the data privacy arena.

In a 2021 report by the Chamber's Institute for Legal Reform (ILR), the Chamber deemed the Illinois Biometric Information Privacy Act (BIPA) "a prime example of a misdirected law that has led to more litigation abuse than consumer protection." Citing the Illinois Chamber

---

[7] U.S. House of Representatives, "Bipartisan House Task Force Report on Artificial Intelligence," Dec 2024, https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf.

[8] Benjamin Perry, Danielle Ochs, Keith Kopplin, and Zachary Zagger, "DOL's Wage and Hour Division Issues New Guidance on Employers' Use of AI," Ogletree Deakins, May 2024, https://ogletree.com/insights-resources/blog-posts/dols-wage-and-hour-division-issues-new-guidance-on-employers-use-of-ai/#:~:text=On%20April%2029%2C%202024%2C%20the,and%20artificial%20intelligence%20(AI).&text=The%20DOL's%20Wage%20and%20Hour,of%20AI%20and%20similar%20technologies.

of Commerce, the ILR report noted that "it is mostly small companies in the state facing lawsuits." What's more, "[e]ven small technical mistakes can result in millions of dollars in liability, since BIPA allows plaintiffs to seek $1,000-$5,000 in damages per violation of the law."[9]

Similarly, the American Privacy Rights Act (APRA), introduced in the 118th Congress, included a private right of action and authorized courts to "award injunctive and declaratory relief, as well as the sum of actual damages, attorney's fees, and litigation costs."[10] As a coalition of state chambers of commerce expressed in a letter to Congress outlining their concerns about APRA, "[t]he APRA private right of action provisions would allow for an explosion of frivolous litigation by empowering the trial bar to sue small businesses, charities, and other actors who could be forced to settle because they lack the time, expertise, and financial resources to fight back."[11]

NSBA not only calls for an outright prohibition on private rights of action in the Law, but we also recommend that the Working Group provides a plain language directive to the FTC in delegating enforcement authority such that there will be no risk of capricious enforcement. In the absence of a federal law governing data privacy and security, past FTC leadership was free to enforce privacy violations in an unpredictable manner. Small businesses need clarity and consistency in the laws that govern data privacy, and so we urge the Working Group to provide this stability.

Conclusion

NSBA would like to reiterate our gratitude to Chairman Guthrie, Vice Chairman Joyce, and the Working Group for the opportunity to respond to this RFI. In summary, we recommend that the Working Group:

- Account for an entity's size in crafting the Law.
- Fully preempt existing state laws governing data privacy and security.
- Preempt existing state-level AI frameworks.
- Provide flexibility in provisions that govern automated decision-making.

---

[9] U.S. Chamber Institute for Legal Reform, "A Bad Match: Illinois and the Biometric Information Privacy Act," Oct 2021, https://instituteforlegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf.

[10] Ash Johnson, "How to Improve the American Privacy Rights Act," Information Technology & Innovation Foundation, Jun 2024, https://itif.org/publications/2024/06/06/how-to-improve-the-american-privacy-rights-act/.

[11] U.S. Chamber of Commerce et al., "State and Local Chamber Letter to Congress Outlining Concerns with the "American Privacy Rights Act"," May 2024, https://www.uschamber.com/assets/documents/APRA-Coalition-Letter_5.21.24.pdf.

- Avoid crafting provisions that could hinder small business adoption of innovative technologies.
- Expressly prohibit a private right of action in the Law and delegate enforcement authority to the FTC.
- Craft a plain language standard for FTC enforcement.

NSBA stands ready to help the Working Group's efforts to secure the U.S. as the preeminent leader of the global digital economy. Please do not hesitate to reach out to rgrey@nsbaadvocate.org if you have any questions.

Sincerely,

Rachel C. Grey

Director of Research & Regulatory Policy, NSBA