1411 K Street N.W.
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

March 27, 2025

Data Privacy Working Group
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Re: Request for Information on Data Privacy for the Data Privacy Working Group.
Submitted Electronically

Dear Chairman Guthrie, Vice Chairman Joyce, and Members of the Data Privacy Working Group:

We are thrilled to see the creation of the House Energy and Commerce Committee's Data Privacy Working Group and the continued effort toward passing a federal comprehensive data privacy and security law. Such a law has been a central focus of R Street's Cybersecurity and Emerging Threats team and we remain committed to helping that become a reality. We therefore appreciate the opportunity to respond to your request for information (RFI).

By way of background, the R Street Institute is a nonprofit, nonpartisan, public policy research organization, with a mission of promoting free markets and limited, effective government through policy research, analysis, and engagement with policymakers. A central focus of ours has been to identify solutions in accordance with these principles, and finding consensus on a federal data privacy and security law. In 2022, we published a report in conjunction with the Harvard Kennedy School's Belfer Center to provide recommendations that address some of the most challenging aspects of a federal data privacy and security law like preemption, a private right of action, and the role of the Federal Trade Commission (FTC).[1] Our research included consultations with more than 125 entities spanning the ideological spectrum. A key aspect of our ongoing work is the intersection of privacy and security, including how national security and data security should be key drivers in passing a federal law.

We believe the enactment of a federal privacy law would benefit consumers, industry, and national security, which is more pressing now as state privacy laws proliferate and emerging technologies like artificial intelligence (AI) evolve. At the core, a privacy law should enable innovation and economic progress, while fostering strong privacy.

[1] Tatyana Bolton et al., "The Path to Reaching Consensus for Federal Data Security and Privacy Legislation," R Street Institute, May 26, 2022. https://www.rstreet.org/2022/05/26/the-path-to-reaching-consensus-for-federal-datasecurity-and-privacy-legislation.

We appreciate Congress' continued interest in passing a comprehensive federal data privacy and security law. While recent attempts have been unsuccessful, we hope this group will be able to make big strides toward producing a product that can gain sufficient support to be enacted into law.

The working group's RFI seeks information on a number of critical areas. We have done significant research and analysis on each question posed. In the interest of space, we have responded to several that are most applicable to our Cybersecurity Team's work, while a second filing from our Technology and Innovation Team focuses in greater detail on how a privacy law might impact AI in particular.

Data Security (Section IV)

We fully agree with the RFI's framing that a foundational goal for a federal comprehensive privacy law should be to increase the security of Americans' personal information. After all, strong data security is necessary to ensure data privacy. Data privacy is often seen as a consumer issue, but the failure to secure our personal data has both national security and cybersecurity implications.

The risk of adversaries collecting and exploiting vast amounts of Americans' sensitive data is not theoretical, it is a reality.[2] Risks to personal data can have far reaching consequences and bad actors acquire this data in a number of ways. This can range from a nation-state actor like the Chinese Communist Party's (CCP) collection of Americans' data for strategic benefit, to criminal groups attempting to steal data for financial gain. Specifically, this data can be used to carry out more effective cyber attacks, target disinformation campaigns, carry out blackmail against high-profile individuals, or even cause direct physical violence to those in conflict.

This threat has been pointed out by a number of prominent government officials and has been highlighted in a number of U.S. policy documents. For example, a former Federal Bureau of Investigation Director claimed "if you are an American adult, it is more likely than not that China has stolen your personal data"[3] and that "China's vast hacking program is the world's largest, and they have stolen more Americans' personal and business data than every other nation combined."[4]

There was an effort to reduce access to this data through the passage of the "Protecting Americans' Data from Foreign Adversaries Act" and Executive Order 14117, titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" with the subsequent promulgation of Department of Justice regulations. However, those actions only addressed part of the problem surrounding commercial purchases and sales of data. They do not

[2] Testimony of Brandon Pugh, House Energy and Commerce Committee, "Economic Danger Zone: How America Competes to Win the Future Versus China," 118th Congress, February 2023. https://d1dth6e84htgma.cloudfront.net/Brandon_Pugh_Testimony_020123_Hearing_36ecfd8b92.pdf?updated_at=2023-02-01T14:31:57.744Z.

[3] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Hosting Entity: Hudson Institute, July 7, 2020. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-partyto-the-economic-and-national-security-of-the-united-states.

[4] Chloe Folmar, "FBI head: China has 'stolen more' US data 'than every other nation combined'," The Hill, Nov. 15, 2022. https://thehill.com/policy/cybersecurity/3737251-fbi-head-china-has-stolen-more-us-data-than-everyother-nation-combined.

address the underlying risks around data collection, use, and security. Much more is needed, and much more is possible though a federal privacy law. Key considerations for the working group should include:

A. *Allowing data use for security-related purposes.* Data in itself has many beneficial purposes and is essential to innovation and emerging technologies, but it is critical that we ensure this data is safeguarded and to take steps to prevent bad actors from leveraging it for nefarious purposes. It is vital that a privacy law encourage, not restrict, the use of data for security-enhancing and security-related purposes. This could entail adding security-related purposes to a list of permissible purposes or as an exception to instances where data collection and use might be limited, depending on the law's structure. For example, data should be permitted to be used for cybersecurity purposes, such as protecting networks, fighting against spam, and responding to incidents, among other applications. Some types of data are also important to leverage in security contexts like IP addresses.

B. *Exploring incentives to increase data security.* Entities should be encouraged to act on data security and cybersecurity practices, even those that might exceed those required by a data privacy law. For example, this could entail liability waivers for entities that engage in pilot programs, such as implementing privacy enhancing technologies. Another method could entail a liability waiver if they implement existing cybersecurity frameworks, which is similar to a concept enacted in Ohio.[5] This allows entities to invest in security up front to potentially save on litigation in the future.

C. *Implementing flexible security requirements and leaning upon those that exist now.* Currently, there is no universal requirement to safeguard data that is collected, absent sector-specific laws. A comprehensive privacy law could require entities to safeguard information they collect through a flexible, non-prescriptive approach to protect the confidentiality, integrity, and accessibility of covered data and to prevent unauthorized access through administrative, technical, and physical security protections. However, the standards should be flexible because not all entities have the same amount and sensitivity of data, or the resources to implement robust security measures. In addition, many entities already align to best practices and frameworks like those made by National Institute of Standards and Technology (NIST) and can serve as good examples. While nothing is foolproof, this would go a long way toward ensuring that data is safeguarded and out of the hands of bad actors.

D. *Clarifying the "reasonable security" standard.* Many laws and regulations require "reasonable security," but there is not a universal definition of the term, and requirements have varied over time when viewed through the eyes of a regulator.[6] As part of any data security requirements it would be helpful for guidance or standards to set expectations for secure data. This would help provide a degree of certainty.

E. *Considering data minimization.* Data minimization is a privacy principle that limits the amount of data collected in the first place. This is especially important as few consumers

[5] Ohio Code Ann. § 1354.02 (2018). https://codes.ohio.gov/ohio-revised-code/section-1354.02.

[6] Steven Ward, "The Quest for "Reasonable Security," *R Street Policy Series,* March 2025. https://www.rstreet.org/commentary/the-quest-for-reasonable-security-part-3-deducing-reasonable-security-from-federal-regulators-rulemaking-and-enforcement-action.

read or understand privacy notices that can bury how an entity will use their data and therefore the consumer often blindly consents. Data minimization offers security benefits—if a covered entity never collects the data, then the data is less at risk. This often forces entities to fully understand why they need the data and how it can be used. However, structuring data minimization in statute must be done carefully to ensure it is not too restrictive on legitimate uses or too inflexible to account for future needs we might not be aware of now.

F. *Providing consumer notification for transfers to countries of concern.* Privacy policies could be required to contain information on whether covered data is "transferred to, processed in, retained in, or otherwise accessible to a foreign adversary …" This is important so consumers know whether their data might be accessible by "foreign adversaries" like China and have the option to forego the transaction.

G. *Accounting for data brokers.* Not all data brokers are equal and there are valid uses for their services, especially to combat fraud and detect victims of crime. However, some data brokers do not adequately secure data they collect and are not transparent about their activities. Any action directed at data brokers should be balanced to ensure both realities, which might include transparency rules and potential security requirements, especially in the case of sensitive data.

Data security has always been paramount, but in the era of AI it is even more important. Given the amount of data utilized by AI at all stages, especially when it leverages either classified or sensitive data, we must ensure it is adequately protected.

Artificial Intelligence (Section V)

In an appearance before the House AI Taskforce in 2024, I conveyed that a federal comprehensive data privacy law is timelier now than ever given the increased usage and sophistication of AI.[7] AI is about data at its core, and data is necessary to continue to ensure America leads on AI, yet protecting privacy is still important. Concerningly, AI-specific bills at the state level have the potential, if enacted, to result in an impossible patchwork of inconsistent rules and regulations that carry enormous compliance challenges and costs similar to that which we've experienced in privacy policy.

I offered several principles for Congress to consider when crafting a federal privacy law in the era of AI, and they still hold true. Similar sentiments were expressed in response to the White House's AI Action Plan RFI.[8] These include a federal privacy law that:

A. *Focuses on privacy,* rather than venturing into broader considerations like specific AI measures. Privacy is applicable across all forms of technology, so it is ideal to have a framework that can be

[7] Testimony of Brandon J. Pugh, Esq., Bipartisan Task Force on Artificial Intelligence United States House of Representatives, "Privacy, Transparency, and Identity," 118th Congress, June 28, 2024. https://www.rstreet.org/outreach/brandon-pugh-testimony-hearing-on-privacy-transparency-and-identity.

[8] "Comments of the in Request for Information on the Development of an Artificial Intelligence (AI) Action Plan," Federal Register Number 2025-02305, March 15, 2025. https://www.rstreet.org/outreach/comments-of-the-r-street-institutes-cybersecurity-and-emerging-threats-team-in-request-for-information-on-the-development-of-an-artificial-intelligence-ai-action-plan.

applied broadly with more specific measures considered separately where gaps emerge in existing law.

B. *Does not unduly limit innovation*. This includes ensuring a law is applicable to data uses that we might not be considering or even know of. It should also look to incentivize further innovation, like the use of privacy enhancing technologies (PETs).[9] Many see AI as potentially harming privacy, but it is imperative to leverage the technology to actually safeguard privacy, along with cybersecurity.[10] R Street's AI and Cybersecurity working group showed that cyber defenders can have an edge in cybersecurity when leveraging AI.[11]

C. *Protects consumers' rights and ensures transparency* into how their data is collected, used, and transferred. After all, most Americans do not enjoy these rights and transparency benefits and most blindly accept privacy notices without reading or understanding them.

D. *Ensures compliance,* and more importantly, *enables compliance*, by all types and sizes of businesses. This is particularly important for AI as many companies doing amazing research and deployment are small and their resources shouldn't be needlessly wasted on compliance.

Existing Privacy Frameworks & Protections (Section III)

Countries around the world have acted on privacy legislation, including most notably the European Union's General Data Protection Regulation (GDPR). Meanwhile, the United States is becoming an outlier without a federal privacy law. This forces U.S. companies to follow frameworks from around the world and allows those frameworks to become the default standard. These often have provisions or approaches that hamper innovation and place large burdens on industry. The U.S. has an opportunity to correct course by enacting a comprehensive federal law that strikes a better balance between privacy, security, and innovation.

At the same time, there are currently 19 states with comprehensive privacy laws, and the number continues to increase, creating many compliance burdens on the private sector.[12] Some point out that the differences between the already-enacted state laws are small and therefore do not pose a significant burden, but the differences that do exist already, combined with those that are currently under consideration and those likely to emerge, should not be understated. What is more, most states can amend legislation quickly or engage in far-reaching rulemaking. However, there are principles in existing state laws that ought to inform and guide Congress, including those from the states of Texas, Kentucky, and Virginia.

[9] Steven Ward, "Leveraging AI and Emerging Technology to Enhance Data Privacy and Security," *R Street Policy Study* No. 317, March 2025, p. 2. https://www.rstreet.org/research/leveraging-ai-and-emerging-technology-to-enhance-data-privacy-and-security.

[10] Haiman Wong and Brandon Pugh, "Key Cybersecurity and AI Policy Priorities for Trump's Second Administration and the 119th Congress," R Street Institute, Jan. 6, 2025. https://www.rstreet.org/research/key-cybersecurity-and-ai-policy-priorities-for-trumps-second-administration-and-the-119th-congress.

[11] "R Street Cybersecurity-Artificial Intelligence Working Group," R Street Institute, last accessed March 18, 2025. https://www.rstreet.org/home/our-issues/cybersecurity-and-emerging-threats/cyber-ai-working-group.

[12] "US State Privacy Legislation racker 2025," IAPP, last accessed March 18, 2025. https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

The patchwork of laws has created a compliance challenge for businesses, especially small- and medium-sized businesses, as they have to traverse this evolving landscape. This forces many to put limited time and resources into navigating a privacy maze instead of innovating and furthering their business goals. In fact, some estimate that each state added to the privacy patchwork costs startups between $15,000 - $60,000+ in additional compliance costs.[13]

This makes it critical for any federal privacy law to have strong preemption and ensure that the federal law is not merely a "floor" that allows states to have stricter laws. Failing to do so could force entities to navigate a compliance thicket of both a federal law and fifty state variants. In addition, a federal law constructed appropriately could be a barrier to state approaches that are less friendly to innovation.

To accomplish this, we believe it is important to include: 1) a congressional intent section stating that the goal of the legislation is to set a national standard, 2) clear preemption language on state frameworks, and 3) an allowance for states to legislate in select areas not meant to be preempted by the law. Importantly, however, any carve outs must not become a backdoor to states legislating or regulating privacy on a comprehensive basis.

Additional Information (Section VII)

When crafting a federal privacy law, there are several other themes to consider. We outline several of these in our "Key Data Privacy and Security Priorities for 2025" explainer.[14]

One key consideration includes how a privacy law interacts with kids' privacy. A federal privacy law should protect the rights of all Americans, regardless of age or position. While child-specific provisions may be appropriate in specific circumstances, they should be passed as part of comprehensive legislation. Doing so could help avoid the free speech and identity verification issues some child-specific proposals face and ensure that all Americans receive privacy protections.

A final key consideration is enforcement. To increase privacy in a non-burdensome manner that all companies can comply with, any well-constructed privacy law should include compliance incentives like a safe harbor provision that protects companies deploying industry best-practices, a right-to-cure provision that allows organizations to avoid penalties if they fix the issue, and special considerations for small and medium-sized businesses without large amounts of sensitive data. For example, state attorneys general and/or the Federal Trade Commission (FTC) should be allowed to enforce the law. Although the FTC should be provided specific areas for rulemaking to ensure the commission does not encroach on Congress' role as would have been the case with its 2022 Commercial Surveillance and Data

[13] *"Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups," Engine, March 2023.* https://link.quorum.us/f/a/1GX7ijzLTEyxEwbOv8s7TA~~/AACYXwA~/RgRn-9duP0SNaHR0cHM6Ly9zdGF0aWMxLnNxdWFyZXNwYWNlLmNvbS9zdGF0aWMvNTcxNjgxNzUzYzQ0ZDgzNWE0NDBjOGI1L3QvNjQxNGE0NWY1MDAxOTQxZTUxOTQ5MmZmLzE2NzkwNzQ0MDA1MTMvUHJpdmFjeStQYXRjaHdvcmsrUHJvYmxlbStSZXBvcnQucGRmVwNzcGNCCmYQeVIZZmwHecdSEWJwdWdoQHJzdHJlZXQub3JnWAQAAAAA.

[14] Brandon Pugh and Steven Ward, "Key Data Privacy and Security Priorities for 2025," R Street Institute, Jan. 15, 2025. https://www.rstreet.org/research/key-data-privacy-and-security-priorities-for-2025.

Security Rulemaking.[15] A private right of action (PRA) has emerged in recent proposals as a way for individuals to enforce their rights. Given the potential for abuse, we recommend avoiding a PRA.

Conclusion

We are grateful for your attention to this important issue and for the opportunity to share our expertise and perspective. We stand ready to assist you in this endeavor in an effort to get good policy across the finish line and signed into law.

Respectfully submitted,

Brandon J. Pugh, Esq.
Policy Director and Senior Fellow,
Cybersecurity and Emerging Threats
R Street Institute
bpugh@rstreet.org

[15] Federal Trade Commission, *Commercial Surveillance and Data Security Rulemaking,* Advance Notice of Proposed Rulemaking, Aug. 11, 2022. https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.