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

Free Markets. Real Solutions.
www.rstreet.org

April 16, 2024

The Honorable Gus Bilirakis
Chair
Subcommittee on Innovation,
Data, & Commerce
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation,
Data, & Commerce
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Bilirakis, Ranking Member Schakowsky and members of the Subcommittee:

Thank you for holding a hearing on April 17, 2024, titled “Legislative Solutions To Protect Kids Online And Ensure Americans’ Data Privacy Rights.” My name is Brandon Pugh, and I serve as the policy director and resident senior fellow for the Cybersecurity and Emerging Threats team at the R Street Institute, which includes our data privacy and security portfolio. I had the honor of testifying before your subcommittee in the 117th Congress on data privacy and security.[i] The R Street Institute and I continue to urge the enactment of a comprehensive federal data privacy and security law in the United States and see it as a top priority for this Congress.

By way of background, the R Street Institute is a nonprofit, nonpartisan, public policy research organization, whose mission is to engage in policy research and outreach to promote free markets and limited, effective government. A central focus of ours has been 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).[ii] Our research included consultations with over 125 entities of varying ideologies. 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 appreciate Congress' continued interest in passing a comprehensive federal data privacy and security law on a bipartisan, bicameral basis. We’re particularly pleased by the steadfast leadership of Congresswoman Cathy McMorris Rodgers and Senator Maria Cantwell, as most recently seen through the release of their American Privacy Rights Act of 2024 (APRA) discussion draft. R Street was fortunate to release one of the first analyses comparing the similarities and differences between the American Data Privacy and Protection Act (ADPPA) and APRA.[iii] We believe a comprehensive federal data privacy and security law would benefit consumers, industry, and security. We look forward to continuing to work with the sponsors and any member interested in the discussion draft, but we believe it is a positive step forward for several reasons.

Preemption is critical for a comprehensive federal privacy and security law.

The number of states with privacy laws continues to increase rapidly with at least fifteen state versions already on the books and many others at varying stages of the legislative process.[iv] This is not a new trend as we saw at least 60 comprehensive bills introduced in at least 25 states in 2023.[v] Some point out that the differences between the already-enacted state laws are insignificant, but the differences that do exist already, combined with those that are 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.

This 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.[vi]

I understand why some might call for a federal privacy law to be a “floor” and to allow for there to be stricter state laws. However, this would not improve the patchwork of laws we see now. Instead, entities might need to deal with a compliance thicket of both a federal law and fifty state variants. Not to mention, a federal law constructed appropriately could be a barrier to state approaches that are less friendly to innovation.

For this reason, both ADPPA and APRA have correctly relied on preemption. However, APRA includes a congressional intent section that clearly articulates that it “establishes a uniform national privacy and data security standard in the United States” and “expressly preempts laws of a State” as provided in this section, which is followed by preemption language of not having “any law, regulation, rule, or requirement covered by the provisions of this Act or a rule, regulation, or requirement promulgated under this Act.” This helps alleviate concerns in ADPPA around the section's intent and whether states might leverage ambiguity to legislate or regulate privacy, which must be avoided.

A recommendation of R Street's past research, notably on preemption, called for substantive privacy bills at the state level to be preempted with select state carve outs.[vii] Our research identified ten areas where this ought to be done. This is an approach that APRA continues from ADPPA, including "state law preservation" for criminal law, contract law, and state laws addressing surveillance. These are areas that APRA is largely silent on so it makes clear that the intent is not to create a gap in areas that states have been acting on for years and where states have had traditional state control even before the emergence of state privacy frameworks. However, I fully agree that these carve outs must not become a backdoor to states legislating or regulating privacy on a comprehensive basis, which would contradict R Street's prior recommendations and appears contradictory to the sponsors' intent.

Data security and national security would be advanced by a federal privacy law.

The risk of adversaries collecting and exploiting vast amounts of Americans' sensitive data is not theoretical, it is a reality. This has been pointed out by a number of prominent government officials and has been highlighted in a number of U.S. policy documents, including the recent Executive Order "to protect Americans' sensitive data from exploitation by countries of concern."[viii] As one example, Federal Bureau of Investigation Director Christopher Wray claimed "if you are an American adult, it is more likely than not that China has stolen your personal data"[ix] 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."[x] This data can be used to carry out more effective cyber-attacks, target disinformation campaigns, carry out blackmail against high profile individuals, or even direct physical violence to those in conflict.[xi]

The White House E.O. and H.R. 7520, the "Protecting Americans' Data from Foreign Adversaries Act," aim to address some of these concerns by targeting commercial sales to select countries. However, they do not address the underlying risks around data collection, use, and security when done incorrectly. Many members of industry proactively embrace privacy and do more than required, but that is not always the case.

A comprehensive data privacy and security law would provide additional safeguards. Absent limited exceptions like regulated industries, there is generally no requirement to safeguard collected data. APRA would require covered entities to establish and maintain reasonable data security practices to protect "the confidentiality, integrity, and accessibility of covered data" and "covered data of the entity against unauthorized access." A number of considerations are provided to ensure requirements are not rigid and not a one size fits all approach. While nothing is foolproof, this would go a long way toward ensuring that data is safeguarded and out of the hands of bad actors.

In addition, privacy policies would 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. Other relevant measures range from provisions on data brokers to parameters for sensitive data collection and use. Equally as important, APRA includes security under permitted purposes for collection and use of data.

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 further.

Compromise is important to make a comprehensive federal privacy law a reality and to have a United States vision for privacy.

Countries around the world have acted on privacy legislation, like the European Union's General Data Protection Regulation (GDPR). Meanwhile, the United States is becoming an outlier without a federal law. This forces U.S. companies to follow frameworks from around the world and allows international 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.

Differences in approaches and substantive provisions have been the downfall of past attempts to pass a privacy law at the federal level. While Congress should not pass a bad bill simply to fill the void, we do believe compromise is important and will require all sides to consider provisions that might not be ideal from their perspective. We also believe that all or nothing thinking is generally unnecessary when considering the provisions of a comprehensive privacy law. This is one of the reasons we are encouraged to see another bipartisan attempt to identify areas for both consensus and compromise.

Thank you again for holding this hearing and for taking my views into consideration. Please do not hesitate to let me know if R Street or I can be a resource or any answer questions that might arise. We look forward to hopefully making a comprehensive federal data privacy and security law a reality in 2024.

Sincerely,

Brandon J. Pugh
Brandon J. Pugh, Esq.
Director and Senior Fellow
Cybersecurity and Emerging Threats
R Street Institute

[i] Testimony of Brandon J. Pugh, Subcommittee on Innovation, Data, and Commerce, House Committee on Energy and Commerce, “Economic Danger Zone: How America Competes To Win The Future Verses China,” 117th Congress, February 2022. https://www.rstreet.org/commentary/house-subcommittee-on-innovation-data-and-commerce-hearing-overview-featuring-r-streets-brandon-pugh.
[ii] 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/commentary/the-path-to-reaching-consensus-for-federal-data-security-and-privacy-legislation.

[iii] Brandon Pugh, “Breaking Down The American Privacy Rights Act Discussion Draft,” R Street Institute, April 7, 2024. https://www.rstreet.org/commentary/breaking-down-the-american-privacy-rights-act-discussion-draft.

[iv] Andrew Folks, “US State Privacy Legislation Tracker,” International Association of Privacy Professionals, April 8, 2024. https://iapp.org/resources/article/us-state-privacy-legislation-tracker.

[v] Heather Morton, “2023 Consumer Data Privacy Legislation,” National Conference of State Legislatures, September 28, 2023. https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation.

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

[vii] Tatyana Bolton et al., “Preemption in Federal Data Security and Privacy Legislation,” R Street Institute, May 31, 2022. https://www.rstreet.org/commentary/preemption-in-federal-data-security-and-privacy-legislation.

[viii] Brandon Pugh, “Is 2024 The Year We Finally Care About Adversaries Buying And Exploiting Our Data?,” R Street Institute, Feb. 28, 2024. https://www.rstreet.org/commentary/is-2024-the-year-we-finally-care-about-adversaries-buying-and-exploiting-our-data.

[ix] 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-party-to-the-economic-and-national-security-of-the-united-states.

[x] 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-every-other-nation-combined.

[xi] Jessica Dawson and Brandon Pugh, “Ukraine conflict heightens US military’s data privacy vulnerabilities,” Defense News, April 14, 2022. https://www.defensenews.com/opinion/2022/04/14/ukraine-conflict-heightens-us-militarys-data-privacy-vulnerabilities.