July 10, 2024

The Honorable Maria Cantwell
Chair
U.S. Senate Committee on
Commerce, Science & Transportation
Washington, DC 20510

The Honorable Ted Cruz
Ranking Member
U.S. Senate Committee on
Commerce, Science & Transportation
Washington, DC 20510

RE: Full Committee Hearing on "The Need to Protect Americans' Privacy and the AI Accelerant" to be held on July 11, 2024

Dear Chair Cantwell and Ranking Member Cruz:

The Main Street Privacy Coalition (MSPC)[1] and its 20 national trade association members appreciate the significant efforts the Chair and other members of the Senate Commerce Committee have made in developing legislation to establish a national privacy framework. We also appreciate the committee holding a hearing on July 11 on the need to protect American's data privacy as well as the opportunity to share our views with you on the importance of enacting a federal privacy law. MSPC supports the goal of establishing a national data privacy and law that applies equivalently to all businesses handling consumers' personal information and avoids potentially unintended consequences that would lead to a disproportionate impact on Main Street businesses and, in turn, negatively impact consumers and the American economy.

The MSPC members represent a broad array of companies that line America's Main Streets. From retailers to Realtors®, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, and self-storage to convenience stores, including franchise establishments, our member companies interact with consumers on a daily basis. These businesses can be found in every town, city, and state, providing jobs, supporting our economy, and serving Americans as a vital part of their communities. Collectively, the industries that MSPC trade groups represent directly employ approximately 34 million Americans and constitute one-fifth of the U.S. economy by contributing $4.5 trillion to the U.S. gross domestic product.

MSPC firmly believes that consumers across the country should be empowered to control their personal data. Having data privacy laws that create clear protections for Americans while allowing our members' businesses to serve their customers in the ways they have come to rely upon is a key goal. Achieving that goal, however, has been elusive. One of the challenges central to the Committee's legislative effort is that the overwhelming focus on the data practices of so-called "big tech" companies can obscure the reality that data privacy laws also apply to, and must work for, Main Street businesses that directly serve Americans in their daily lives.

[1] The Main Street Privacy Coalition website and member list may be accessed at: https://mainstreetprivacy.com.

MSPC Principles for Federal Privacy Legislation

As discussed in greater detail in MSPC's May 7 letter to the Committee sent in advance of the subcommittee hearing on data security, Main Street businesses focus on earning and preserving their trusted relationships with customers, including by protecting and responsibly using the personal data customers share with them. As the Committee crafts privacy legislation, we ask you to embody in it the following core principles to ensure an effective national privacy law:

- **Establish a Uniform National Privacy Law:** Congress should enact a federal data privacy law that benefits consumers and businesses alike by ensuring all personal data is protected in a consistent manner regardless of the state in which a consumer resides.

- **Protect Consumers Comprehensively with Equivalent Standards for All Businesses:** Federal data privacy frameworks should apply requirements to all industries that handle personal data and should not place a disproportionate burden on certain sectors of the economy while alleviating others from providing equivalent protections of personal data.

- **Create Statutory Obligations (Not Contractual Requirements) for All Entities that Handle Consumers' Data:** Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts. Service providers and third parties must have statutory privacy obligations when offering data processing, transmission, storage, or other services to tens of thousands of Main Street businesses.

- **Preserve Customer Loyalty Rewards and Benefits:** Any federal data privacy framework should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships such as loyalty programs.

- **Require Transparency and Customer Choice for All Businesses:** Consumers deserve to know the categories of personal data that *all* businesses collect, how it is generally used to serve them, and the choices they have regarding those uses.

- **Hold Businesses Accountable for their Own Actions:** Privacy legislation should not include terms that potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of a business partner.

- **Effective Enforcement**: Effective enforcement holds accountable all businesses handling consumer data to *equivalent* privacy standards, thereby creating proper incentives across industry. Because "mistake-free" compliance is unlikely in a complex area of the law like data privacy, we support the state privacy law model of coupling governmental entity enforcement with the ability to "cure" non-compliant practices upon notice and within a limited period of time to correct them, which will drive broader compliance with the law.

MSPC Views on H.R. 8188, the "American Privacy Rights Act" (APRA)

Our previous letter to the Committee provided out initial views on a discussion draft version of the American Privacy Rights Act (APRA) released in April. Since then, some of our concerns with the draft text, such as with the treatment of customer loyalty plans and businesses sharing a common brand, were addressed during the House Energy & Commerce Committee's process. However, we have continuing significant concerns with the bill's private rights of action (PRA) provision and its potential consequences for over one million American businesses we collectively represent. We also believe the preemption provisions and service provider requirements need further improvement, as outlined below, before we can support the bill.

As shown in the attached chart, the PRA contained in the House-introduced version of the APRA (H.R. 8188) disproportionately impacts Main Street businesses: notably, *all* of the subsections of the bill enforceable by PRA apply to our businesses as "covered entities," however *only 3* PRA-enforceable subsections apply to Big Tech "service providers" and *none of them* apply to Big Tech "third parties." Moreover, section 111(a)'s and (b)'s direct requirements for Big Tech service providers and third parties, respectively, are <u>not</u> subject to the PRA.

As drafted, our members are concerned that H.R. 8188 would lead to tens of thousands of demand letters sent annually to Main Street businesses for *alleged* violations of the bill that threaten costly but meritless litigation unless settlements are quickly paid. Further, H.R. 8188 provides no opportunity to "cure" claims for damages, leaving businesses with the unenviable "choice" of either paying unjust, demanded settlement payments, or paying exponentially more money to go to court to defend themselves against what they believe are baseless claims that cannot be dismissed another way. We urge the Committee to address these significant concerns.

We appreciate the intent of H.R. 8188 to establish a single, uniform national privacy law by preempting the increasing patchwork of state privacy laws that potentially conflict and threaten the ability to provide comprehensive and uniform privacy protections to all Americans. We are concerned, however, that the bill's current preemption provision is unlikely to withstand anticipated legal challenges in federal court, potentially allowing States to continue adopting their own data privacy laws that leave Americans with different rights depending on where they live and burdening Main Street businesses with standards differing from those set by Congress.

MSPC has offered suggested edits to the preemption provision that would meet the standards for express preemption language that the Supreme Court has consistently ruled sufficient to create a preemptive federal law. For instance, the APRA could be modified in form and language to avoid using a general rule that necessitates two and a half pages of exceptions – a form of drafting that federal courts have cited as unclear and used as a basis to reject federal preemption clauses to preserve similar state laws. Instead, the APRA could specify precisely which State laws are specifically preempted and clarify that future laws related to the specifically preempted laws would be similarly preempted. Such an approach would make the APRA much more likely to achieve its primary goal of creating a single, uniform national privacy law for all Americans.

Lastly, we recognize that consumer-facing businesses represented by MSPC are often the businesses with whom consumers directly interact and share their personal information, but Main Street businesses do not monetize consumer data in opaque and deceitful ways and should not be held liable for data privacy violations committed by their Big Tech service providers or third parties that H.R. 8188 does not hold accountable. Where Big Tech entities may view the consumers' data as *their* product, we do not. Our businesses responsibly use data that consumers share with us to better serve them the actual goods and services that are *our* products.

We therefore urge the Committee to craft legislation, consistent with our principles, that would hold accountable Big Tech service providers and third parties to the *same* extent as Main Street businesses by carefully aligning the APRA's service provider requirements to match the more consumer-protective provisions adopted in nearly every one of the 19 enacted comprehensive state privacy laws. Improving the APRA this way would help Main Street businesses by creating statutory obligations for service providers and third parties that ensure they include these statutory obligations in their contracts with covered entities or else be in violation of federal law. More importantly, it would protect against privacy loopholes that leave consumers unprotected when their personal data is handled by these business partners that most covered entities cannot police through contracts alone given the imbalance in negotiating leverage.

Conclusion

We appreciate your consideration of our views on federal data privacy legislation. We also stand ready to work constructively with you to ensure legislation adopted by this Committee reflects our principles above and effectively preempts state laws to establish a uniform national standard, avoids disproportionately impacting Main Street businesses compared to other industry sectors, and properly holds Big Tech service providers accountable to an equivalent level under the law.

Sincerely,

The Main Street Privacy Coalition

Attachment

cc: Members of the U.S. Senate Committee
on Commerce, Science & Transportation

Disproportionate Impact of APRA's Private Rights of Action ("PRA") on Main Street Businesses ("Covered Entities")[1]

APRA Sections Subject to PRA	Covered Entities (X = section applies)	Service Providers (N/A = not applicable)	Third Parties (N/A = not applicable)
Data Minimization (§102)			
• §102(b) Sensitive Data Transfers	X	N/A	N/A
• §102(c) Biometric Info and Genetic Info (e.g., includes collection, processing, retention, transfer, etc.)	X	N/A	N/A
Transparency (§104)			
• §104(a) Privacy Policy Publicly Available	X	X	N/A
• §104(e) Material Changes to Privacy Policy (including Notice and Opt Out)	X	N/A	N/A
Individual Control Over Covered Data (§105) (e.g., consumer rights of access, correction, deletion, and portability of covered data):			
• §105 (all subsections)	X	N/A	N/A
Opt-Out Rights and Universal Mechanism (§106)			
• §106 (a)	X	N/A	N/A
• §106 (b)(2)	X	N/A	N/A
Interference with Consumer Rights ("Dark Patterns Prohibited") (§107)			
• §107 (all subsections)	X	N/A	N/A
Prohibition on Denial of Service and Waiver of Rights (including, "Service or Pricing" in "Bona Fide Loyalty Programs") (§108)			
• §108 (all subsections)	X	N/A	N/A
Data Security and Protection of Covered Data (§109)			
• §109 (a) – "to the extent such action alleges a data breach arising from a violation of subsection (a)"	X	X	N/A
Service Providers and Third Parties (§111)			
• §111(a) Service Provider Requirements – **NOT subject to the PRA**		N/A	
• §111(b) Third Party Requirements – **NOT Subject to the PRA**			N/A
• §111(d) Reasonable Care in Selecting Service Providers or Transfers of Data to Third Parties	X	X	N/A
Data Brokers (§112)			
• §112(c)(4) – "Do Not Collect" and "Delete My Data" Requests	X *(a data broker is a "covered entity" that meets the definition of a "data broker")*	N/A	N/A

[1]*Chart prepared by Main Street Privacy Coalition based on section 117(a)(1) of H.R. 8818, the American Privacy Rights Act (APRA).*