May 7, 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

The Honorable John Hickenlooper
Chair
U.S. Senate Subcommittee on
Consumer Protection, Product Safety,
and Data Security
Washington, DC 20515

The Honorable Marsha Blackburn
Ranking Member
U.S. Senate Subcommittee on
Consumer Protection, Product Safety,
and Data Security
Washington, DC 20515

RE: Hearing on " Strengthening Data Security to Protect Consumers" on May 8, 2024

Dear Chair Cantwell, Ranking Member Cruz, Chair Hickenlooper, and Ranking Member Blackburn:

The Main Street Privacy Coalition (MSPC) appreciates your holding a subcommittee hearing on May 8 and the opportunity to share our initial views on the discussion draft of the American Privacy Rights Act (APRA). MSPC supports the goal of establishing a national privacy and data security law that applies equivalently to all businesses handling consumers' information and avoids potentially unintended consequences that would have disproportionate impacts on Main Street businesses and, in turn, negatively impact consumers and the American economy.

The House Energy and Commerce Committee's efforts last Congress on the American Data Privacy and Protection Act (ADPPA) included, in some instances, ways to address concerns that had long been difficult to reconcile. In some specific provisions affecting our members, such as preserving customer loyalty plans, service provider requirements, and the treatment of franchise businesses, however, the APRA significantly departs from the successful compromises achieved in the consideration of the ADPPA. We look forward to working collaboratively this year with you and your colleagues on the Senate Commerce Committee to address the issues outlined below with the ultimate goal of enacting privacy legislation that establishes a single, uniform national privacy law.

MSPC firmly believes that consumers across the country should be empowered to control their personal data. Having data privacy and security 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 whose employees directly serve Americans in their daily lives.

The MSPC is comprised of 20 national trade associations that together represent more than a million American businesses—a broad array of companies that line America's Main Streets[1] and interact with consumers day in and day out. 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, the businesses represented by MSPC member associations 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 members represent directly employ approximately 34 million Americans and constitute over one-fifth of the U.S. economy by contributing $4.5 trillion (or 21.8%) to the U.S. gross domestic product (GDP). Our success depends on maintaining *trusted* relationships with our customers and clients: trust that goods and services we provide are high quality and offered at competitive prices; and trust that information customers provide to us while we are serving them is kept secure and used responsibly. For these reasons, our associations have been actively engaged for many years with policymakers on data privacy legislation and regulations.

Six Principles for Effective Federal Privacy Legislation

Main Street businesses have no higher priority than earning and preserving trusted relationships with their customers, including by protecting and responsibly using the personal data that customers share with them. As policymakers consider the APRA and other legislative solutions to address data privacy concerns, our coalition urges adoption of legislation meeting the following core principles to ensure a comprehensive and effective national privacy law:

- **Establish a Uniform National Privacy Law:** The United Stats should have a sensible federal framework for data privacy legislation that benefits consumers and businesses alike by ensuring that consumers' personal data is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws with a set of federal rules for all businesses handling consumers' personal data is necessary to achieve the important public policy goal of establishing a single, uniform national privacy law.

- **Protect Consumers Comprehensively with Equivalent Standards for All Businesses:** To protect consumers comprehensively, federal data privacy frameworks should apply requirements to all industries that handle personal data and not place a disproportionate burden on certain sectors of the economy while simultaneously alleviating other sectors from providing equal protection of consumer data. An equivalent data privacy standard

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

should apply, regardless of whether a business directly collected data from a consumer or obtained it in a business-to-business transaction.

- **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 obligations like all other entities to ensure their compliance with a federal privacy framework, particularly 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 and set the terms of those relationships. Legislation should include safe harbors to ensure that consumers can purchase, or otherwise obtain, the goods and services they want by taking advantage of benefits, incentives, or enhanced services they earn from being loyal customers, even if other customers choose not to engage in such loyalty programs.

- **Require Transparency and Customer Choice for All Businesses:** Consumers deserve to know the categories of personal data businesses collect, how it is generally used to serve them, and the choices they have regarding those uses. These policies should be clearly disclosed in company privacy policies and readily accessible to consumers. These transparency and choice obligations should apply to *all* businesses handling consumers' personal data, including service providers, third parties, and financial services businesses.

- **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. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability for other businesses that do not fulfill their own obligations under a federal privacy law.

Main Street Privacy Coalition Views on the APRA Discussion Draft

We appreciate Chair Cantwell's efforts to develop the APRA discussion draft with House Energy and Commerce Chair Rodgers, however, we have initial concerns that the bill, as drafted, disproportionately and negatively impacts the industry sectors MSPC member associations represent. We appreciate the opportunity to work constructively with Senate Commerce Committee members and their staff to address the potential unintended consequences of new language in the APRA prior to its introduction and advancement in Committee markups, consistent with our coalition's history of productive dialogue on past legislation, such as the ADPPA.

1. **Preemption of State Law**: We appreciate the Senate Commerce Committee's past efforts to develop preemptive legislation that would establish a single, uniform national privacy law benefitting consumers and businesses alike by ensuring privacy protections are the same regardless of the State in which a consumer resides or a business is located. This is necessary to address the increasing patchwork of newly enacted state privacy laws that conflict and threaten the ability to provide comprehensive and uniform privacy protections to all Americans. Despite the underlying goal of preempting state laws in past committee legislation, we are concerned the APRA's current preemption provision is unlikely to withstand anticipated legal challenges in federal court, potentially leaving States free to continue adopting privacy laws that would leave American consumers with different rights depending on where they live and would saddle Main Street businesses with compliance burdens exceeding the federal standards set by Congress. We therefore urge the Committee to modify the APRA's preemption provision to meet the standards the Supreme Court has consistently ruled sufficient to create a preemptive federal law. For instance, the APRA could avoid using a general rule that necessitates pages of exceptions – a form federal courts have used as the basis to preserve similar State laws and frustrate Congressional intent – by instead specifying precisely which State laws are preempted by the APRA and making clear 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.

2. **Private Rights of Action**: We understand the Committee's interest in authorizing private rights of action (PRA) in privacy legislation as a politically desirable element to advance a bipartisan privacy bill through Congress. Our member companies are concerned, however, with the APRA taking a leap that no State law has taken due to the technical complexity involved in entities achieving mistake-free compliance with data privacy laws, as well as Main Street companies' extensive experience with large volumes of demand letters threatening lawsuits with questionable legal claims that recently have proliferated under other areas of the law (e.g., patent trolls and ADA website accessibility claims). More importantly, the APRA differs significantly from the ADPPA in that the APRA does not authorize the PRA to enforce the requirements for service providers or third parties under Section 11(a) through (c) because it limits the PRA's application only to covered entities under subsection 11(d). This is a surprising reversal of the ADPPA's application of the PRA in this section that disproportionately impacts Main Street businesses compared to their business partners. Under this PRA, private litigants' *only* recourse would be to sue the covered entities for failing to exercise reasonable judgment in selecting service providers or transferring data to third parties because they cannot sue the service providers or third parties directly for their own failures to comply with their Section 11 requirements. Further, the APRA does not offer a way for well-intentioned Main Street businesses to avoid litigation because it denies them any opportunity to cure *alleged* violations in claims for damages. All too often, provisions like this PRA permit potential litigants to exploit the Main Street business reality that obtaining legal representation to defend against alleged claims under a complex federal law is too expensive. Those costs lead Main Street businesses to agree to settlements of even non-meritorious claims simply to avoid litigation, which has the compounding effect of making it more challenging for them to cover operational expenses and consequently costs Americans their jobs. Due to the complexity of achieving compliance, the disproportionate impact that the APRA would have on Main Street businesses, and their inability to avoid litigation for alleged violations, our members would prefer the Committee adopt an enforcement approach similar to what all State privacy laws have adopted as the most effective way to drive compliance with privacy laws: exclusive government agency enforcement against

businesses after a 30- or 60-day cure period following agency notice of non-compliance. If that is not achievable politically, we urge the Committee to at least address the serious concerns raised above to ensure that America's Main Street businesses, their employees, and the customers they serve are not disproportionately impacted, compared to other stakeholders, by the APRA's enforcement provisions as currently drafted.

3. **Preserving Customer Loyalty Rewards and Benefits**: It is clear that Americans overwhelmingly wish to continue participating in their customer loyalty programs that provide rewards, discounts and other benefits.[2] Additionally, the fifteen States that have passed comprehensive data privacy laws have all preserved loyalty program benefits for consumers by protecting the ability of businesses to continue offering better prices and services to customers who voluntarily participate in bona fide customer loyalty, club or rewards programs. Under the State privacy laws, loyalty plan clauses protect against construing the laws to prohibit (as discriminatory acts) the offering of discounted prices or other benefits to customers who voluntarily choose to participate in the plans, even if other customers choose not to participate in them. However, the APRA adds a new page of novel requirements for loyalty plans not seen in any State law. We have significant concerns that the draft text alters the carefully balanced language of the ADPPA that MSPC member associations previously supported after all stakeholders negotiated with the House Energy and Commerce Committee to ensure the ADPPA provision would preserve customer loyalty programs. For example, one of the current APRA requirements prohibits all transfers of *any* data in ways that exceed the bill's already established data transfer provisions that permit covered data transfers subject to an opt-out and sensitive covered data transfers subject to an opt-in, excluding permissible purposes. With these same APRA transfer provisions applying to covered entities offering loyalty programs, similar to how all State privacy laws' consumer rights and privileges apply to plan participants' data as well, it is unclear why the draft APRA would impose a new, more restrictive data-transfer regulation on loyalty programs that consumers must already opt into under the law. In its forthcoming consideration of the APRA, we urge the Committee to restore the previous balance achieved in the ADPPA's loyalty provision that mirrors the balance achieved in all enacted State laws. This is important to American consumers who wish to maintain their earned points, rewards and discounts, and is a critical need for Main Street businesses.

4. **Service Provider and Third Party Requirements**: Similar to the loyalty plan provisions, we are concerned that the APRA draft text of Section 11 alters the carefully achieved balance previously achieved in the ADPPA's service provider and third party requirements following stakeholder negotiations with House Energy and Commerce Committee staff over that bill's provisions. We appreciated that the ADPPA placed direct statutory obligations on service providers and third parties, and enforced these obligations with the same enforcement mechanisms as covered entities, to ensure their compliance with the law. However, we are concerned the draft APRA has altered the text of these requirements to remove both the direct statutory obligations as well as the enforcement mechanisms for service providers and third parties in ways that obviate their obligations to protect the consumer data received from covered entities. The APRA ultimately allows service providers and third parties to avoid liability by shifting it onto covered entities through subsection 11(d), the only subsection enforceable by

[2] According to a survey by Bond Brand Loyalty Inc., 79% of consumers say loyalty programs make them more likely to continue doing business with brands that offer them, and 32% of consumers strongly agree that a loyalty program makes their brand experience better. Bond Brand Loyalty Inc., The Loyalty Report (2019).

private rights of action (as explained in point 2 above). As a result, under the APRA, nationwide and global service providers would not have the equivalent privacy requirements or enforcement provisions that apply to even the smallest Main Street businesses. To protect Americans' data privacy comprehensively, the APRA should ensure that businesses in all industry sectors face equivalent privacy requirements and enforcement of the law in order to close of any privacy loopholes that would leave consumers unprotected when their personal data is handled by a range of service providers and third-party businesses. For example, the APRA's critical data minimization obligations do not apply to service providers or third parties – these are privacy requirements that exist nowhere else in federal privacy law and should be required of all businesses in the APRA.

5. **Common Branding**: One issue that the House Energy and Commerce Committee was able to resolve in their consideration of the ADPPA was an unintended consequence of holding franchisors and franchisees liable for each other's privacy law compliance. Many franchisees and franchisors share common branding but are distinct companies and should be treated as such. But the language of the APRA currently defines them as one single "covered entity" because the businesses operate with "common branding." That language had been used in the ADPPA at one time, but the bill sponsors recognized that it could lead to unintended consequences and took the "common branding" language out of the ADPPA before it was reported by the House Energy and Commerce Committee in July 2022. The same should be done for the APRA in its definitions of "covered entity" and "third party" to avoid making broad groups of independent businesses jointly liable for one another's behavior.

We appreciate your consideration of the views of Main Street businesses regarding the APRA as the Committee considers the discussion draft before it is introduced. This is not just a bill for "big tech" companies, and Main Street businesses will bear the full burden of complying with the regulatory obligations under the APRA. As you consider ways to improve the APRA prior to its introduction and advancement in the legislative process, the members of the MSPC appreciate your consideration of the above principles and concerns with the discussion draft, as well as our efforts to address these concerns prior to approving the APRA in Committee. We look forward to continuing our constructive dialogue with the Committee on these critical matters and welcome the opportunity to address each specific topic with your staff.

Sincerely,

The Main Street Privacy Coalition

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