Main Street
PRIVACY COALITION

September 22, 2020

The Honorable Roger Wicker
Chairman
U.S. Senate Committee on Commerce,
Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on Commerce,
Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

RE: Senate Commerce Committee hearing on "Revisiting the Need for Federal Data Privacy Legislation," held September 23, 2020

Dear Chairman Wicker and Ranking Member Cantwell:

The Main Street Privacy Coalition (MSPC), a coalition of 19 national trade associations representing more than a million American businesses,[1] appreciates your focus on the need for federal data privacy legislation and offer this statement for the hearing record. MSPC is comprised of a broad array of national trade associations representing businesses 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, MSPC member companies interact with consumers day in and day out. Our members' businesses can be found in every town, city and state in our nation, providing jobs, supporting our economy and serving Americans as a vital part of their communities.

Collectively, the industries that MSPC member associations represent directly employ nearly 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 the goods and services we provide are high quality and offered at competitive prices; and trust that the information customers provide to us is kept secure and used responsibly. For these reasons, our associations are actively engaged in the discussions surrounding data privacy and have come together to support enactment of a comprehensive and uniform federal data privacy law.

MSPC is dedicated to the enactment of a federal data privacy law that creates privacy obligations for all businesses handling consumers' personal information, and we support the Committee's efforts to bring greater attention to the need for a such a law. We strongly believe that the views of Main Street businesses should be considered on this issue given that Main Street represents the backbone of the United States economy. Main Street businesses, many of whom have remained open to continue to serve consumers during the COVID-19 pandemic, will bear the full burden of regulatory obligations under some proposed privacy bills the committee is now considering, which largely exempt telecommunications companies and big tech service providers from similar obligations to protect consumer privacy. Further, despite federal data privacy legislation being motivated by privacy violations that occurred at social media and

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

technology companies, much legislation has focused on Main Street businesses and not financial institutions, data brokers and social media companies that routinely process more sensitive consumer information. MSPC therefore urges the Committee to hear from and work with all stakeholders to advance a federal data privacy bill that applies equivalent provisions to all businesses handling consumers' personal information.

While the hearing focuses on the need for federal data privacy legislation generally, MSPC notes that Chairman Wicker introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act last week. We are pleased the Chairman has introduced legislation from which the Committee can work, but we would like to point out areas in which MSPC believes that the SAFE DATA Act would benefit from additional consideration, especially with the input of Main Street businesses that would be obligated to comply with nearly all of its provisions.

Virtually every industry sector – whether consumer-facing or business-to-business – handles significant volumes of consumer information. To protect Americans comprehensively, any federal data privacy legislation, including the SAFE DATA Act, should ensure that all industry sectors are covered and that there are no privacy loopholes that leave consumers unprotected when their personal data is handled by a business. All of the companies involved in handling the chain of personal data should have legal obligations to protect it under a federal privacy law, and we should not rely on private contracts to create those legal obligations between parties, particularly ones that vary greatly in size (i.e., Main Street businesses and global service providers).

MSPC is thus concerned with provisions in the SAFE DATA Act that would exempt service providers and third parties from certain statutory obligations to honor consumer rights exercised to protect their privacy. These exemptions for service providers would be extended to businesses in the telecommunications industry, technology companies, and data cloud storage entities—the very industries represented by witnesses at the Committee's hearing. Additionally, the SAFE DATA Act explicitly states that service providers cannot be considered data brokers, further exempting the telecommunications industry from this legislation even if they continue to siphon and sell consumer data from the Internet traffic running through their networks.

There are more effective ways to protect Americans' privacy. For example, the Consumer Data Privacy and Security Act, introduced by Senator Jerry Moran (R-KS), takes a more equitable approach to these issues. Senator Moran's privacy bill is based on the premise that each business handling consumers' personal data should have statutory requirements to do what it is able to do to protect the consumer privacy established in the legislation. Furthermore, the bill does not make consumer-facing businesses responsible for privacy violations by businesses that they cannot control, such as much larger service providers. Because it takes this approach, Senator Moran's privacy legislation would more effectively secure the consumer rights it establishes and treat industry sectors fairly by making them responsible for their own conduct.

The SAFE DATA Act, on the other hand, requires Main Street businesses to be responsible for the privacy practices of service providers and third parties without equivalent requirements for these exempt entities to comply. Privacy responsibilities should not simply be shifted from one industry sector onto another – not only because that is an ineffective way to protect consumer information but also because it is manifestly unfair to businesses that bear the

brunt of those burdens for what should be the other businesses' own obligations to the consumer. Because our members include small businesses, they know that all too often powerful businesses within the telecom and tech industry sectors may use their superior market position to shift what should be their responsibilities onto their clients, typically leaving Main Street businesses with outsized compliance burdens and costs. And, if this approach is taken by Congress, it will leave holes in consumer privacy rights because federal enforcement agencies will have no effective way to compel service providers or third parties to comply with the law, and Main Street businesses will lack the financial and legal resources to hold them accountable for privacy practices that harm their customers.

MSPC is additionally concerned with the exemption for financial institutions and other entities subject to the Gramm Leach Bliley Act (GLBA) from the consumer privacy protections of the SAFE DATA Act. GLBA, a law enacted in 1999 that is significantly outdated in its extremely narrow privacy protections, which do not provide anything close to the privacy protections that the SAFE DATA Act extends to consumers. For instance, GLBA requires that an entity sharing consumer financial data with unaffiliated third parties for marketing purposes provide an annual opt-out notice in writing, which most consumers never read. It does not however require any access, correction or deletion of consumers' financial data upon request, as SAFE DATA would require of every other consumer-facing business on Main Street that is not a bank or credit union. Therefore, exemptions for financial institutions and other entities subject to GLBA permit these select consumer-facing businesses to avoid the bill's privacy requirements and leave consumers unprotected while feeling a false sense of security they are fully covered.

Moreover, the SAFE DATA Act's newly included provisions for covered internet platforms is overly broad and will pull in many Main Street businesses that are not platforms and simply make sales or market their products or services through their own websites. The provision would create potential problems for a large swath of commercial websites employing algorithms, including those that only allow searches of their own products and service offerings. This new compliance burden would interfere with consumers' efforts to find the products and services they want even when dealing directly with businesses that they know and with which they want to transact, while providing no additional privacy benefits to consumers.

Despite MSPC's concerns with certain aspects of the SAFE DATA Act noted above, we support and appreciate a number of the bill's provisions. First, we support the SAFE DATA Act's call for a uniform, preemptive federal privacy bill that sets a national standard for consumer privacy protections that aids consumers and businesses alike. The diversity and complexity of different state privacy laws is one of the key reasons a federal privacy law is needed today. We also appreciate that the bill does not cover employee data and publicly available data. That helps guard against unintentionally impeding many of the basic functions of employers that we expect.

With that in mind, MSPC believes that any federal privacy bill, including the SAFE DATA Act, should establish a uniform, nationwide and consumer-centric federal data privacy law that includes these principles:

1. <u>Industry Neutrality and Equal Protection for Consumers Across Business Sectors</u> – Federal data privacy frameworks and legislation 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 should apply, regardless of whether a business directly collected data from a consumer or obtained it in a business-to-business transaction. In short, a federal privacy law should provide consumers' data with uniform legal protections across all industries handling it.

2. Direct Statutory Obligations (Rather than Contractual Requirements Alone) for All Entities that Contact Consumer Data – Effective consumer protection regulations cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. Data service providers and other third parties need direct statutory obligations to ensure they comply with relevant privacy laws, particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of small businesses.

3. Preservation of Customer 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. Federal law 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 programs. For businesses to offer such programs, they must necessarily keep track of the business transactions of their customers who choose to enroll so that they can offer rewards and allocate benefits.

4. Transparency and Customer Choice – Consumers deserve to know what categories of personal data businesses collect and how that data is generally used. These policies should be clearly disclosed in company privacy policies readily accessible to consumers to ensure that they can learn how customer data is collected and used by the business to provide goods or services. These obligations should apply to all businesses handling consumers' personal data, including service providers and third parties.

5. Accountability for Business's Own Actions – Privacy law should not include terms that could 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 if other types of businesses do not fulfill their own obligations under the law.

6. Data Security & Breach Notification – A federal data privacy law should include a reasonable data security standard for all businesses handling consumer data, as well as a uniform process for businesses suffering a data security breach to notify affected individuals. Currently, consumer-facing industry sectors are required to comply with 54 state and U.S. territorial laws on data breach notification requirements, and nearly half of the states have enacted data security laws. However, financial institutions and service providers are often exempt from these state breach notice requirements. All businesses handling consumers' data should be required to protect personal data and provide notice of their own security breaches when they occur.

7. Establishing Uniform Nationwide Rules and Enforcement for Data Privacy – Congress should create a sensible, uniform federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws and enacting an alternative set of nationwide rules is necessary to achieve the important, national public policy goal of uniformity.

As you consider ways to advance federal data privacy legislation, the members of the MSPC urge you to include these key principles in your bills and continue to solicit input from all affected industries and from businesses of all sizes during the legislative process. We look forward to a constructive dialogue with you on these matters as you craft federal data privacy legislation in the remainder of this session and in the next Congress.

Sincerely,

The Main Street Privacy Coalition

cc: The Honorable Mitch McConnell
The Honorable Charles E. Schumer
Members of the Committee on Commerce, Science, and Transportation