November 6, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725, Attn: Privacy RFC
Washington, DC 20230

Via email at *privacyrfc2018@ntia.doc.gov*

Re: National Telecommunications and Information Administration's Request for Comments
Docket No. 180821780-8780-01

The National Business Coalition on E-Commerce & Privacy (the "Coalition") appreciates the opportunity to provide comments to the National Telecommunications and Information Administration ("NTIA") on ways to advance consumer privacy while protecting American prosperity and innovation. Founded in 2000, the Coalition represents prominent American companies in finance, manufacturing, and information services. For the past eighteen years, the Coalition has been actively involved in a broad range of issues effecting consumer privacy, including targeted marketing, data security/breach notice, identity verification, enforcement, and the creation and enforcement of sectoral driven privacy laws.

Like the Administration, the Coalition recognizes the importance of protecting consumer privacy and not unnecessarily hampering innovation or preventing companies from providing data-driven products and services of interest to consumers. To date, the United States' sectoral approach to privacy, focused on regulating specific privacy risks, has struck this balance. International markets and consumer advocates, nonetheless, demand that the United States implement an omnibus privacy law, but while doing so they ignore the distinct cultural and legal differences between how data is used and laws are enforced in the United States.

While international markets, especially the European Union (EU), have very strict, uniform data protection laws and regulations, they do not enforce those laws and regulations with the same enthusiasm that the trial bar and government authorities (both state and federal) do in this country. For example, the 28 Data Protection Authorities in Europe are very different from one another and do not have the robust enforcement budgets that typify State Attorneys General in this country. Moreover, unlike the United States, there is no federal enforcement agency in Brussels that can remotely compare with the enforcement expertise of the Federal Trade Commission ("FTC") and sector

specific regulators (*e.g.*, the U.S. Department of Health and Human Services' Office for Civil Rights).

In addition to these demands, the passage of the California Consumer Privacy Act ("CCPA") of 2018 in June of this year underscores, more than ever, the inherent inconsistency with which businesses and consumers alike are confronted when states compete with one another to regulate data flows that, by their very nature, constitute interstate commerce. The resulting patchwork of state privacy laws inevitably overlap and contradict federal privacy laws and, in this respect, the CCPA is the most recent and conspicuous example. To address these issues, therefore, the Coalition encourages the Administration's efforts and supports the development of a preemptive, risk-based multi-factored regulatory approach to assessing the validity of data privacy practices.

The Administration's proposal should provide the FTC with a framework that allows for the assessment of a multitude of specific, competing factors, including the benefits and harm, if concrete, to consumers, in order to determine the legitimacy of data privacy practices. We believe this framework, unlike Europe's prescriptive one-size-fits-all model, would protect consumers, small businesses, innovators, and the United States' dominant position in the digital economy. In developing this framework, the Coalition encourages the Administration to develop a new and different approach, one which seeks to define "reasonableness" so that its subsequent application is predictable and compliant. This "new approach" should also: (i) limit the law's application to consumers only; (ii) recognize existing federal privacy laws; (ii) assess the relative merits of State Attorneys General enforcement as a back-up to federal enforcement; (iii) address via preemption the current patchwork of state privacy laws; and (iv) explore offering companies an affirmative defense for adopting reasonable policies and practices with respect to data privacy. With respect to this last point, we refer the NTIA to Section 1354.01 (effective November 2), Chapter 1354 of the Ohio Statutes. Ohio has just enacted a safe harbor for security systems.

Protecting Consumers and their Families.

A federal privacy law designed to protect the privacy interests of consumers should only apply to products and services intended for personal, family, or household use. The extension of consumer-driven privacy laws to areas of employment and government are bound to have an unintended negative effect. For example, the application of Europe's General Data Protection Regulation ("GDPR") to personal information collected within the context of an individual's employment is bad policy. Employees should not be given proprietary rights with respect to how innocuous information, such as company

email addresses, is used, retained, and disclosed by their employer and other businesses.

Existing Federal Privacy Laws.

To date, the United States' approach to data privacy and security has been sector driven. Unlike the European model, which has embraced across-the-board rules, U.S. regulators have recognized the continuing importance of innovative practices by focusing on regulating specific privacy laws, although not perfect, are the product of careful deliberation and analysis and should not be viewed as somehow inferior. To date, they have successfully balanced the privacy needs of consumers and the ability for industry to bring products and services to market. Any federal privacy law should defer to federal functional regulators whose data practices are already covered by these carefully crafted and proven laws.

State AG Enforcement.

There are currently twenty-four federal laws that grant enforcement power to state attorneys general. Since the passage of the first statute granting this authority in 1976, there has been a particular focus on granting these enforcement rights with respect to consumer protection laws. Through NTIA's deliberation process, we believe a thorough assessment of the benefits and costs of granting State Attorneys General this back-up enforcement power is in order.

Specifically, we encourage the NTIA to examine the relative merits of authorizing State Attorneys General to utilize their resources in support of federal enforcement efforts. This blend of State and Federal resources has always been a traditional byproduct of properly structured preemption, so long as the State Attorneys General serve a secondary, or back-up, function when Federal authorities either fail to act or lack the requisite resources enabling them to do so. Federal authorities should always have priority when enforcing Federal law, and so State Attorneys General should be granted ancillary but not duplicative enforcement powers. Specifically, State Attorneys General should not be able to bring enforcement claims with respect to data privacy practices that have already been or are subject to federal adjudication. Otherwise, counterproductive and duplicative enforcement actions, as well as inconsistent interpretation and application of law, would be inevitable.

A Federal Breach Notification Standard.

Consumers' embrace of the digital economy has resulted in a dramatic increase in the amount of electronic records. This shift has resulted in unprecedented efficiencies and consumer benefits. Unfortunately, state

sponsored and criminal schemes, as well as human error, have resulted in, and will undoubtedly continue to cause, unauthorized disclosures of personal information. In response to these breaches, businesses are now required to navigate fifty different state breach notification laws with varying requirements with respect to the timing, content, and notification triggers. Compliance with this patchwork of laws demands the unnecessary expenditure of considerable time and resources, drawing attention and resources away from remediation. In addition, certain impacted consumers sometimes do not receive notice simply because they live in the wrong state. A consistent national approach to providing notice to impacted individuals, which tightly pre-empts the existing patchwork of state laws, should be part of any Administration's effort.

Data Security as an Affirmative Defense.

In addition to the patchwork of state breach notification laws, at least thirteen states, including California, have enacted data security laws that generally require businesses to implement and maintain "reasonable security". The FTC has also leveraged its Section 5 Authority under the Federal Trade Commission Act to bring enforcement actions against companies that allegedly failed to implement reasonable security measures to protect consumer information. These laws, and the entities enforcing them, provide little guidance for what steps businesses must take to achieve reliable compliance. To address this concern, and to the extent that NTIA includes data security within its ambit, we propose that the Administration's framework create an option that encourages businesses to upgrade their data security apparatus, for the ultimate benefit of consumers, and to do so by allowing businesses to obtain independent third-party certification against established industry data security standards (*e.g.*, U.S. Commerce Department's National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity). If such certification were to be achieved, the affected business would be shielded from liability under the rationale that even with its best efforts, the reliable adoption of "reasonable" date security practices was insufficient to protect their system, as well as its customers, from unauthorized access.

Sincerely,

Thomas M. Boyd
Counsel