November 9, 2018

Mr. David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: **NRF Comments to NTIA Request for Comments published September 26, 2018: "Developing the Administration's Approach to Consumer Privacy"**
(Docket No: 180821780–8780–01; RIN 0660-XC043)

Dear Mr. Redl,

In response to the Request For Comments (RFC) published by the National Telecommunications and Information Administration (NTIA) on September 26, 2018, the National Retail Federation respectfully submits below its comments for your consideration on "Developing the Administration's Approach to Consumer Privacy."

The National Retail Federation (NRF) is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and internet retailers from the United States and more than 45 countries. Retail is the nation's largest private-sector employer, supporting one in four U.S. jobs — 42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

I. Introduction: NRF's Efforts to Develop Retail Principles to Protect Consumer Data Privacy

NRF has worked closely with its member companies on the development of data protection policy for more than two decades. We view our active engagement with Congress and federal departments and agencies on proposed federal privacy policy as part of a continuum of our long-term efforts to help ensure the retail industry maintains best practices on data privacy and security matters. We have worked with members of the congressional committees of jurisdiction for dozens of years to develop appropriate federal legislation on data privacy matters, specifically, and we look forward to continuing our important collaboration with the newly elected 116th Congress (2019-2020) to advance federal privacy legislation that the retail industry can fully support.

Beginning in the late 1990s, NRF formed a privacy working group with its most active member companies to develop principles for retailers on customer data privacy. Absent federal or state legislation requiring specific privacy practices, members engaged in this effort to create a set of voluntary industry privacy principles reflecting the best practices of retailers with respect to the

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

information they collected about their customers. The guiding principle was that retailers should maintain the level of data privacy they reasonably anticipate would be expected of them by the shopper in a given context.

The objectives of reasonableness and meeting customer expectations are at the heart of retailers' customer privacy practices and form the foundation of data protection regulations in the U.S. and globally. While these concepts have stood the test of time, several recent regulatory developments, including the enactment of the California Consumer Privacy Act (CCPA) and the launch of the European Union's General Data Protection Regulation (GDPR), have led to industry-wide re-examinations of current privacy principles and practices. In light of these developments, our members are also undertaking a review of NRF's privacy principles and will consider appropriate updates to guide retail industry practices with respect to customer information going forward.

As we undertake our retail sector privacy review, we value the opportunity to provide our initial views for your consideration in response to your request for comments on consumer privacy that we hope will inform future Administration policy, actions and engagement. Our comments below are divided in two parts, as follows:

- First, we provide below some important contextual information about how retail companies use consumer data to better serve their customers. Retailers' customer-centric approach to consumer data is different than third-party businesses that do not interact with consumers directly but whose revenue is based on monetizing consumer data they handle. These differences between retailers and third parties help inform our industry's approach to protecting customer data privacy as well as NRF's recommendations regarding public policy approaches. This opening discussion also sets the foundation for our comments on the Administration's proposed high-level goals for federal action on consumer privacy.

- Secondly, we provide below a set of specific comments on the "High-Level Goals for Federal Action" that NTIA enumerated in part I.B. of the RFC. We agree with you that it is an important first step for the Administration to formulate its goals for federal action to "provide the leadership needed to ensure that the United States remains at the forefront of enabling innovation with strong privacy protection," as your RFC states in its second paragraph. Once a federal policy approach is appropriately framed, the Administration will then be in position to promote within that approach – through various policy tools, including federal legislation – its desired privacy outcomes for consumers.

II. Retailers' Use of Customer Data and Interests in Protecting Consumer Privacy

Protecting customer data privacy is one of retailers' highest priorities. Retailers know that establishing long-term relationships with their customers requires more than just providing the merchandise they want at the prices they are willing to pay. Successful retailers win their customers' trust and provide a satisfying shopping experience so that consumers continue to shop with them time and again. A critical element of establishing that trusted relationship lies in how well retailers perform as stewards of the information their customers share with them when shopping.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations for service. Whether online or in store, over mobile devices or through phone orders,

retailers use data to provide personalized experiences that consumers value. Customers, in turn, expect retailers to process their personal information responsibly and seamlessly when they are shopping in their retail channel of choice. To meet these high customer expectations, retailers make significant investments in technological solutions and can spend years developing comprehensive methods to comply with state, federal and global regulations on data collection and usage that will further their customer relationships and not frustrate them.

In short, retailers use customer data for the principal purpose of serving their customers as they wish to be served; the data collection is not an *end* in itself, but merely a *means* to the end of improving customer service. This practice differentiates retailers' principal use of customer data from other businesses – typically third parties unknown to the consumer – whose principal business is to monetize consumer data by collecting, processing it and selling it to other parties as a business-to-business service. As the Administration considers the appropriate goals for federal action, and as members of the 116th Congress craft federal data privacy legislation, it is important for government policymakers to recognize the fundamental differences in data usage between businesses that are known to the consumer because they serve them directly (i.e., consumer-facing businesses) and businesses that traffic in consumers' data without their knowledge.

In 2009, the Federal Trade Commission (FTC) explained in its staff report on online behavioral advertising the distinct differences between "first-party" and "third-party" uses of data, particularly regarding consumers' reasonable expectations, their understanding of why they may receive certain advertising, and their ability to register concerns with, or avoid, the practice. Indeed, millions of Americans learned of the significant risks of harm to them personally that can flow from irresponsible data practices by third-parties who are unknown to them, as we saw in the well-publicized Cambridge Analytica and Equifax incidents during the past fourteen months. The FTC's report was noteworthy in the example in which it compared retailers' use of data to third-parties:

> For example, under the "first party" model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site (e.g., "based on your interest in travel, you might enjoy the following books"). In such case, the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.[1]

[1] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), pp. 26-27, available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

American consumers expect all businesses handling their sensitive information to do so responsibly, regardless of when and where that data is handled. By developing a data privacy law that does not pick regulatory winners and losers among industry sectors, the Administration and the 116th Congress can work together to ensure that Americans' privacy will be protected by federal law regardless of which business is collecting, transmitting, storing or otherwise processing their sensitive personal information. We support the Administration's efforts to lead these efforts by establishing the high-level goals for federal action to protect consumer data privacy.

As Congress and the Administration consider proposed federal data privacy legislation and regulations in the coming months and years, we look forward to working with policymakers across the government to help them understand the flaws in the approaches taken by the CCPA and GDPR, and to develop a principled approach to consumer data privacy protection that meets a reasonableness standard and consumers' expectations of privacy when interacting with American businesses.

In Part III below, we provide NRF's comments for your consideration on how the Administration could drive forward such a principles-based approach to consumer data privacy protection by establishing a broad outline for the direction that federal action should take. We agree with NTIA that this may be done by establishing a set of high-level goals for the Administration to adopt, and the views we share next provide our recommendations on how the Administration can achieve these goals through its public policy efforts and support for federal privacy legislation.

III. Specific Comments on the Administration's High-Level Goals for Federal Action

We appreciate NTIA's request for feedback on the proposed high-level goals for federal action enumerated in Part B of the RFC. NRF believes establishing such goals is the most important step that the Administration can take now to lead the direction of congressional efforts to advance federal privacy legislation. We also believe that establishing the goals for federal action is a prerequisite to the Administration's ultimate goal of achieving privacy outcomes for consumers. While a range of industry sectors and companies are developing and proposing various sets of principles to achieve particular privacy outcomes, there is *greater consensus* among industry sectors and businesses at this time regarding the set of high-level goals for federal privacy legislation.

Within this context, we focus our views in this section on what retailers believe is a consensus set of goals for federal action that reflect not only the views within our own industry sector but also across many other industry sectors. These views have been informed by our conversations and meetings to date with broad-based industry trade associations and cross-sector business coalitions representing a vast array of U.S. businesses. Our comments on how to achieve these goals include a set of principles for federal privacy legislation we have recently proposed in NRF's letter to Chairman John Thune (R-SD) and Ranking Member Bill Nelson (D-FL) that supports the U.S. Senate Commerce Committee's efforts to develop federal privacy legislation that would establish nationwide privacy rules and preempt related state privacy laws. These proposed objectives for federal privacy legislation also have been informed by our two decades of experience on data privacy policy issues and, more recently, our extensive work on the GDPR and CCPA. We hope you take into consideration our views on those laws in our letter (available for your review at the link above) in addition to the goals for federal action we provide here.

To help the Administration set the broad outline for the direction that federal action should take on consumer privacy, we offer for your consideration the following comments to what the RFC describes as a "non-exhaustive and non-prioritized list of the Administration's priorities." *(Please note our comments below are in the same order as the goals enumerated in Part B of the RFC.)*

1. Harmonize the Regulatory Landscape

NRF strongly agrees with the Administration's observation in the RFC that "there is a need to avoid duplicative and contradictory privacy-related obligations placed on organizations" and that "[w]e are actively witnessing the production of a patchwork of competing and contradictory baseline laws." We also agree that "this emerging patchwork harms the American economy and fails to improve the privacy outcomes for individuals…who may not have equal protections, depending on where the user lives."

American businesses, including retailers, recognize that they cannot solely concentrate their data privacy protection practices on compliance with U.S. federal and state data privacy regulations. Conceivably, a data regulation adopted halfway around the world – such as in the European Union (EU) – may impact a U.S. business operating entirely within our national borders and employing only American workers. Retail businesses are also acutely aware of the potential for 50 different U.S. states and an untold number of foreign governments to propose new data regulations each year that have a global reach, just like the nature of the data each law intends to regulate.

Global governmental and institutional privacy regulations, even if well-meaning in their desire to achieve privacy outcomes for consumers, may ultimately make it impossible or extremely costly for businesses to use data responsibly to serve their customers in the many ways consumers have come to expect. Moreover, proposed regulations that are not based in reasonableness and customer expectations will likely hinder the adoption and growth in innovative technology to serve customers, largely because of the risks that companies could face from government fines or penalties in class action litigation if they misjudge how best to use technology to serve their customers.

We therefore urge the Administration, as we have urged other federal entities, to set as its primary goal for federal action the establishment of a uniform and fair framework for consumers and businesses alike that respects and promotes consumer privacy. This goal would best be achieved in federal legislation that can statutorily preempt conflicting state laws in the U.S., but it will also require international solutions to harmonize the U.S. rules with those in other regions of the world. With respect to global harmonization of privacy regulations to protect consumer data, we applaud the significant and successful work of the International Trade Administration of the U.S. Department of Commerce (DOC) for its efforts to maintain and improve the EU-U.S. Privacy Shield framework and to promote greater awareness and adoption of the APEC Cross-Border Privacy Rules (CBPR) System.

Failure to achieve this primary goal of federal action – to harmonize the regulatory landscape – would largely defeat the effort to achieve a consistent set of privacy outcomes for consumers because any outcomes hoped to be achieved by federal action would be lost in a sea of conflicting state and international privacy laws. Without this harmonization of consumer privacy laws, American businesses may decrease their investment in technological innovations that would better serve customers, while protecting their privacy, out of fear of tripping over a hodge-podge of potentially

conflicting state, national and multi-national regulations that each authorize excessive fines for non-compliance.

NRF's Recommendation for U.S. Federal Privacy Legislation: The Administration asks how each goal for federal action may be achieved and, as noted above, we believe harmonization of the U.S. regulatory landscape can best be achieved through the passage by Congress of federal privacy legislation. Within this broad recommendation, however, we believe that federal privacy legislation should contain the following element that would help achieve this primary goal of federal action:

- **Federal Preemption of Related U.S. State Laws:** Congress should create a sensible, uniform and federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that all sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting related state laws is necessary to achieve this important, national public policy goal. Without effective preemption of state law, Congress would simply add another data privacy regulation to what may eventually become a 50-state regulatory regime, where the U.S. laws fall within a larger, unworkable global regulatory gauntlet for businesses as state, national and multi-national laws all potentially conflict. Congress's effort to bring sensibility and certainty to data regulation is as important to the future of e-commerce as maritime law was to trans-oceanic commerce centuries ago.

2. Legal Clarity While Maintaining the Flexibility to Innovate

The Administration proposes as another goal for federal action to "ensure that organizations have clear rules that provide for legal clarity, while enabling flexibility that allows for novel business models and technologies, as well as the means to use a variety of methods to achieve consumer-privacy outcomes." NRF agrees with this objective as a fundamental goal for federal action on consumer privacy.

U.S. businesses should have the ability to work confidently within a clear but flexible national framework for consumer privacy protections without fear of unwarranted government enforcement actions and litigation over expansive interpretations of ambiguously-worded statutes and regulations. Businesses that invest in technology to fulfill their well-intentioned and good faith efforts to serve their customers in a privacy-protected manner should have the flexibility to achieve these beneficial consumer outcomes in a variety of ways, particularly in a highly competitive industry sector like the U.S. retail industry. Balancing legal clarity, flexibility and consumer privacy is essential to preserving business competition and technological innovation that benefits consumers.

We also agree that the goal of preserving both technological innovation and consumer protection simultaneously is the hallmark of U.S leadership on privacy issues in the international arena, and the Administration should continue to seek privacy outcomes that maximize both objectives rather than trade off one for the other. The Administration should therefore work to establish a US. privacy framework that permits competitive businesses to harness the power of technological innovations to minimize and prevent individual harms from the misuse of consumer data while it strives to provide the most innovative services to American consumers. Achieving this goal would truly give consumers "the best of both worlds," and we believe it is not just aspirational.

The Administration can find very good precedents to achieve this high-level goal for federal action in U.S. and international consumer protection and privacy laws that show how legal balancing tests can effectively be used to weigh business needs and consumer interests to produce beneficial outcomes for consumers.

Section 5 of the Federal Trade Commission Act, the federal law protecting American consumers from unfair or deceptive acts or practices, requires the FTC to engage in an array of legal balancing tests that take into consideration not only the government's interest in protecting consumers but also related business realities. In many aspects of its enforcement of consumer protection laws, the FTC examines the reasonableness of business practices in light of a particular business context and set of circumstances, as well as the affected consumers' expectations, awareness and ability to avoid possible harm. In this way, the FTC Act uses a flexible framework that helps the U.S. government achieve the end result that permits robust and fair competition that best serves consumers while ensuring that they are protected from unfair and deceptive acts or practices.

When it comes to international precedents for privacy regulations, the GDPR similarly adopts some legal balancing tests – although not to the same extent as the FTC Act – to achieve privacy outcomes that aim to maximize consumer protection while providing organizations with some degree of flexibility in achieving this outcome. While retailers have identified a set of concerns with implementing critical elements of the GDPR (as discussed in further detail in the NRF letter to the U.S. Senate Commerce Committee), we also recommend the Administration review the elements of the GDPR that provide flexibility to businesses in assuring consumer privacy protections.

We urge the Administration to learn the lessons of the U.S. industry's experience with these current legal precedents and work with Congress to develop and enact a new federal privacy law that will establish a clear and flexible privacy framework benefitting consumers and businesses alike. We offer one suggested element for a U.S. federal privacy law immediately below for your consideration.

NRF's Recommendation for U.S. Federal Privacy Legislation: One way the U.S. can preserve both consumer protection and technological innovation in privacy protections is to include within the legislation itself flexible regulatory concepts (e.g., legitimate interest) that are not binary in nature (e.g., opt-in vs. opt-out). We would propose including the following elements in a federal bill that can provide legal clarity while maintaining the flexibility to innovate:

- **Legitimate Interest to Process Data**: Federal privacy legislation should promote well-understood fair information practice principles, such as transparency and consumer choice, with respect to sensitive customer data. Businesses handling such data should be transparent about their collection and use of sensitive data and should provide consumers with meaningful choices in how such data is used. Retailers support principles like the GDPR's "legitimate interest" concept as a lawful basis for processing sensitive customer data, which properly aligns consumer expectations with business needs by balancing a business's legitimate interest in processing personal information (to serve its customers) with the customer's interest in protecting her data from misuse. The legitimate interest basis for data processing provides the regulatory flexibility necessary to ensure that businesses can use consumer data responsibly in ways that avoid frustrating the customer experience with incessant notifications and/or requests for consent where it is unnecessary to do so. In this way, the legitimate interest basis ensures consumer privacy protections

through a balancing test that enables businesses to proceed confidently in using technology to better serve customers while having the flexibility to achieve required privacy outcomes in a variety of ways.

3. Comprehensive Application

We strongly agree with the Administration's goal of comprehensive application of federal approaches to consumer privacy, and specifically its conclusion that "[a]ny action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data in activities that are not covered by sectoral laws." We also agree that differences in business models are best addressed through application of a risk-based and outcome-based approach, which allows for "similar data practices in similar context to be treated the same rather than through a fragmented regulatory approach."

American consumers expect *all* businesses handling their sensitive personal information to do so responsibly, regardless of when and where that data is handled or by whom. Meeting consumers' privacy expectations in this respect is crucially important within our networked economy where many businesses must share consumer information to fulfill their customers' desired transactions with respect to goods or services.

For example, when a customer uses her credit card in a retail store to make a purchase, she rightfully expects that the privacy and security of the card number will be maintained by all businesses throughout the entire transaction. That is true even though the consumer may not be aware of every business (across a variety of industry sectors) that will handle her credit card number to ensure approval of the purchase, including the:

- ***retail store*** where the card is initially inserted or swiped in a point-of-sale terminal;
- ***telecommunications carrier*** (e.g., Verizon) over whose lines the card number travels;
- ***payment card processor*** (e.g., First Data) that routes the payment to the card network;
- ***branded card network*** (e.g., Visa) whose system enables the financial transaction; and
- ***financial institution*** (e.g., JPMorgan Chase) that issued her the credit card.

The Administration should therefore help Congress develop a federal data privacy law that treats all businesses the same when they are handling similar consumer data in a similar context, like the typical payment card transaction example above. This would ensure that the government does not craft a law that picks regulatory winners and losers among numerous businesses that all must share the same or similar consumer data to fulfill customers' wishes. To achieve this goal, we recommend that the Administration work with Congress to enact a federal law that ensures American consumers' expectations of comprehensive privacy protections will be met by all businesses handling their sensitive data, regardless of which business is collecting, transmitting, storing or otherwise processing their sensitive personal information at any given time.

As noted above, NRF has engaged in discussions with a range of industry trade associations, including the U.S. Chamber of Commerce, which share the goal of federal action ensuring a comprehensive application of privacy regulations. In its recently released privacy principles, the U.S. Chamber highlighted the importance of "industry neutrality" noting that its privacy principles "apply to all industry sectors that handle consumer data and are not specific to any subset of industry

sectors." [2] NRF will continue to collaborate with the U.S. Chamber and other industry trade associations in endorsing this important goal for federal action proposed by the Administration.

In addition to the consensus position of national trade associations that support this principle, we urge the Administration to fully examine the lessons to be learned from state laws of *purported* general application which contain statutory language does not ensure consumers' expectations of privacy will be met comprehensively across industry. As we did in the NRF letter to the U.S. Senate Commerce Committee, we have raised concerns about the CCPA, enacted by the California state legislature this past summer, and its lack of comprehensive application of its regulations to businesses handling the same or similar consumer data. On August 31, 2018, the final day of the California legislative session, the CCPA was amended by passage of "clean-up" legislation to clarify the statutory language of the law that had been enacted two months before, on June 28, 2018. However, several of the so-called improvements were refinements to the *exemptions* in the law that permit businesses with highly sensitive customer information to avoid the data privacy requirements that must be borne by other businesses handling the same or even less sensitive information.

While we agree with the intended goal of avoiding duplicative regulations at the federal and state level, which is consistent with our harmonization comments above, we highlight for the Administration that for many provisions of the CCPA, there is actually no corresponding federal privacy law that would require the exempted industry sector from providing *equivalent* consumer data privacy protections. The CCPA's disparate treatment of businesses handling sensitive consumer data is one reason why Congress should move forward with comprehensive federal legislation that preempts the CCPA in favor of establishing a uniform set of requirements nationwide that applies evenly to all industry sectors handling similar sensitive personal information.

NRF's Recommendation for U.S. Federal Privacy Legislation: In order to achieve the Administration's proposed goal of comprehensive application of a federal approach to consumer privacy for all U.S. private sector organizations, we recommend that Congress craft a federal data privacy law that meets the following principle of uniform application of the law:

- **Uniform Application of Federal Law to All Entities:** Federal data privacy legislation should apply to all industry sectors that handle the same or similar consumer data, and Congress should not craft rules that are specific to any subset of industry or permit exemptions that pick winners and losers among competitive industry sectors. To protect consumers comprehensively, a federal data privacy law should apply equivalent requirements to all industry sectors handling similar sensitive personal information in a similar context.

4. Employ a Risk-Based and Outcome-Based Approach

The Administration correctly points out that compliance models for data privacy regulation often require cumbersome procedures for businesses and consumers "without necessarily achieving measurable privacy protections," and it concludes that the federal "approach to privacy regulations should be based on risk modeling and focused on creating user-centric outcomes." NRF agrees with

[2] *U.S. Chamber Privacy Principles* (released September 6, 2018), available at: https://www.uschamber.com/press-release/us-chamber-releases-privacy-principles

the Administration's recommended approach here, which is also consistent with retailers' customer-centric approach to data privacy discussed in detail above in Part II of our comments.

We agree that risk-based approaches allow organizations to balance business needs with consumer expectations when making decisions about protecting customer data. Retailers believe that consumers' most sensitive data deserves greater protection, for instance, than less sensitive data. A customer's shoe size, if mistakenly disclosed, is not harmful, whereas a credit card number that is obtained illegally by a hacker can be used to make fraudulent purchases on a customer's account. When businesses allocate their finite set of resources to protecting data, they use risk modeling to ensure that the greatest amount of resources are deployed to prevent data compromises that would cause the greatest risk to consumers and the business. Likewise, with respect to privacy outcomes, consumers would expect businesses to provide greater transparency and choice with respect to uses of their most sensitive data, and therefore greater resources should be allocated to consumer requests regarding the collection, use or sharing of that data compared to non-sensitive or non-personal data.

NRF's Recommendation for U.S. Federal Privacy Legislation: One way the Administration can achieve the goal of ensuring a risk-based approach to privacy outcomes is to set criteria in federal privacy legislation that defines the highest risk uses of data for which enhanced consumer privacy protections should be required. This approach should be scalable, where data practices having greater risk also have reasonably enhanced requirements to ensure the protection of consumer privacy. Such an approach would align with existing industry risk modeling practices that result in greater resource allocation to data uses that present greater risks to consumers. We therefore recommend that the Administration work with Congress to craft a federal data privacy law that adopts the following principle when establishing a risk-based approach to data privacy regulation:

- **Risk-Based Approach to Federal Privacy Regulations Should Scale Requirements by the Sensitivity of the Consumer Data (among other factors reflecting increased risk):** Federal data privacy legislation should adopt a regulatory framework with scalable protections that apply reasonably more enhanced privacy requirements to more sensitive consumer data. Data with the highest degree of sensitivity typically creates the greatest risk of consumer harm if misused or otherwise compromised. For example, consumers' Social Security Numbers or financial account numbers that are compromised, disclosed in a data breach by a bank or credit union, or otherwise used in an authorized manner could result in significant financial harm to a consumer, such as identity theft, account takeover or other financial fraud. Conversely, disclosure of a list of names and related mailing addresses in a direct mail marketing database may present very little risk of harm to consumers, as most of this information is already publicly available in online or printed phone books or directories. A risk-based approach adopted in federal privacy regulations applying comprehensively to all businesses should recognize these differences and ensure that businesses processing the most sensitive data have the greatest privacy protections in place to meet consumer expectations.

5. Interoperability (with International Privacy Laws)

The Administration accurately observes in its high-level interoperability goal that the global "internet-enabled economy depends on personal information moving seamlessly across borders," however foreign governments may approach consumer privacy differently and in ways that later

require mechanisms to bridge the differences between international privacy regulations. While we agree with the Administration's statement that one of its objectives for federal action is to "reduce the friction placed on data flows," we caution it against developing a U.S. privacy framework that is merely "consistent with the international norms and frameworks in which the U.S. participates."

As the DOC's International Trade Administration recognizes, all international norms and frameworks are not created equally, and the U.S. should closely examine and evaluate whether an existing international framework in which it participates will ensure the consumer privacy outcomes it desires in the type of harmonized, flexible, comprehensive and risk-based approach to consumer privacy it advocates for use within the U.S. An international privacy regulation or framework whose principles are far different from ones our nation values, or is rigid and not focused on risk-based or outcome-based regulations, may not necessarily be a suitable privacy framework to which the U.S. government should ensure our laws are "consistent." Rather, we urge the Administration to lead the global community on international frameworks that embrace the objectives of promoting consumer protection and technological innovation simultaneously to ensure privacy outcomes that maximize consumer privacy and business needs alike. That should be the basis on which the Administration determines the frameworks in which it will "participate," and if it adopts that approach, then ensuring consistency makes sense.

As discussed above in our first recommendation for federal legislation that would harmonize the regulatory landscape, NRF believes the Administration should establish as its primary goal for federal action to work with Congress to enact a sensible, uniform and federal framework for U.S. data privacy regulation that benefits consumers and businesses alike by ensuring that all sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. We observed above that Congress's effort to bring certainty to data regulation on a global scale is equally as important to the future of e-commerce as maritime law was to trans-oceanic commerce centuries ago. Given its mission, history and institutional experience, the DOC is uniquely positioned among U.S. federal government departments to recognize the parallels drawn here and the importance of participating in international legal frameworks – consistent with U.S. principles and laws protecting consumer privacy – that enable global commerce.

In addition to the International Trade Administration's focus on international frameworks, the NTIA is fully equipped to lead the federal government's efforts to help Congress achieve the goal of enacting a uniform set of U.S. federal privacy regulations with consistent, nationwide application. After establishing a U.S. national framework – harmonization within the American legal system itself – the DOC will have greater leverage to work with its international counterparts to harmonize the new U.S. data privacy law with the laws of other nations and multi-national regions, such as the EU.

The EU recognized the same need a decade ago when it initiated its efforts to develop the GDPR with the primary goal of establishing a uniform set of data privacy rules that would apply evenly throughout its member states – twenty-eight nations of Europe. Congress now needs to do the same by passing preemptive federal data privacy legislation to give U.S. government officials the single-most important tool they need to harmonize U.S. data privacy law with international privacy laws. A comprehensive U.S. federal privacy law ensuring consumer privacy outcomes is one the DOC could support and promote worldwide as the leading global standard for data privacy regulation that protects consumer privacy without sacrificing technological innovation or business competitiveness.

6. FTC Enforcement

The Administration's high-level goal in support of the FTC as "the appropriate federal agency to enforce consumer privacy with certain exceptions made for sectoral laws outside the FTC's jurisdiction" must be carefully considered with respect to the exceptions. We agree that other federal enforcement agencies (or even certain state enforcement authorities for some industry sectors) may be required to enforce comprehensive federal regulations with the same power and authority as the FTC would enforce them against entities subject to its own jurisdiction.

The exceptions to FTC enforcement should therefore not permit *inequivalent* enforcement among federal agencies such that some may not enforce a comprehensive privacy law to the same degree against businesses within their own jurisdiction as the FTC does against businesses under its jurisdiction that are handling the same or similar sensitive data within a similar context. To address this concern, the Administration should look to enforcement harmonization models in existing federal laws that either require memorandums of understanding or inter-agency policy agreements among federal enforcement agencies to ensure that each agency with the appropriate authority enforces a comprehensive law equally against all businesses subject to its jurisdiction. Failure to adopt a similar harmonized approach to privacy law enforcement among federal agencies could create disparate treatment and even disincentives within the less-regulated industry sectors to fully assure the same customer privacy outcomes that sectors subject to FTC enforcement would ensure.

Additionally, with respect to the FTC's enforcement authority itself, the Administration should recognize that businesses subject to its jurisdiction are remarkably diverse in their size and scope of operations, and differ greatly with respect to their use of consumer data and the sensitivity of data they process. The FTC therefore employs legal balancing tests, as discussed above regarding flexible approaches, to calibrate the reasonableness of a business practice. For these reasons, "one-size-fits-all" data security standards are unworkable, and the application of one sector's data security standards to *all* commercial businesses under the FTC's jurisdiction is unwarranted, especially considering its enforcement of a *reasonable* data security standard under Section 5 of the FTC Act.

We appreciate the FTC's past recognition of the significant differences between financial institutions and retail businesses in the sensitivity of customer data they collect and use, as well as the Commission's consumer-centric and risk-based approach to enforcement of Section 5 of the FTC Act. We also appreciate the Commission's understanding of the differences in the enforcement of data security standards by the respective federal agencies for financial institutions versus commercial businesses. NRF believes the recognition of these differences by the FTC supports the position that comprehensive federal privacy legislation that includes a provision on data security for all businesses, and empowers the FTC to enforce this standard, should be reasonable and appropriate for the types of businesses to which the standards would apply.

FTC enforcement of comprehensive privacy regulations that uses a scalable reasonableness approach, grounded in determining the appropriateness of business practices in light of consumer expectations of privacy and data security, would provide the vast array of businesses subject to the FTC's jurisdiction with the necessary flexibility in their implementation of reasonable privacy and data security standards, and would permit the Commission to enforce such regulations fairly and equitably to ensure businesses' compliance with them.

7. Scalability

While NRF generally supports the high-level goal of scalability "to ensure that the proverbial sticks are used to incentivize strong consumer privacy outcomes are deployed in proportion to the scale and scope of the information an organization is handling," we call out for comment NTIA's statement in this section that "there should be a distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations."

As discussed in greater detail above in our support for the high-level goal of comprehensive application of the law, we describe a typical credit card transaction in which credit card numbers pass through multiple "third-party" vendors in order to complete a payment card transaction. Between the retail store, where the card is swiped, and the cardholder's bank, which issued the card, the are many third parties that should be held to the same standards to protect the privacy of the cardholder's sensitive personal information to the same degree as the bank that issued the card and the merchant that accepted it for payment.

The Administration's proposal to exempt third-party vendors that process personal data on behalf of other organizations is inconsistent with its own high-level goal for comprehensive application of federal privacy regulations. We urge the Administration to consider the consumer harms that could arise if third-party vendors do not protect consumer information to the same degree as other businesses, particularly in our networked, internet-enabled and data-sharing economy.

The Administration should recall that in Part II of our comments above, we provided an overview of the context in which retailers operate and their focus on a customer-centric approach to data privacy. We also point out that the FTC considered situations in which third-parties unknown to consumers handle their personal data, and concluded that those contexts raise greater privacy concerns than ones in which first-parties (i.e., consumer-facing companies) handle the same data.

For these reasons, the Administration should reject this proposed third-party exception in its scalability goal for federal action as inconsistent with the high-level goal of comprehensive application of a federal privacy law. It is a proposed exemption that we believe, if adopted, will fail to ensure the privacy outcomes for consumers that is the purpose of the Administration's proposed consumer-centric approach to privacy.

Wherever consumer data flows, appropriate privacy protections should follow. That is the golden principle upon which the Administration's comprehensive application and scalability goals should rest; exemptions for third-party vendors are inconsistent with this principle.

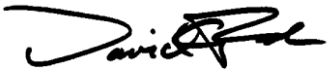
IV. Conclusion

We have developed our views above on which principles are critical to a U.S. federal data privacy law through the past two decades of working with our member companies on data privacy policy. There are certainly lessons to be learned from recently enacted laws: some areas of enlightened thinking that we support, such as the GDPR's legitimate interest basis for processing customer data, as well as areas of concern with the CCPA we hope the Administration addresses with Congress to find alternative methods to achieve the public policy ends of a federal data privacy law.

We look forward to discussing our comments with you as the Administration develops its approach to consumer privacy and high-level goals for federal action. If you have any questions regarding our comments above, please contact Paul Martino, Vice President, Senior Policy Counsel, at MartinoP@nrf.com.

Thank you again for the opportunity to provide our views for your consideration.

Sincerely,



David French
Senior Vice President
Government Relations

cc: The Honorable John Thune
The Honorable Bill Nelson
The Honorable Greg Walden
The Honorable Frank Pallone