RILA
RETAIL INDUSTRY LEADERS ASSOCIATION

1700 N. Moore Street, Suite 2250, Arlington, VA 22209

November 9, 2018

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

Re: **Request for Comments on Developing the Administration's Approach to Consumer Privacy (Docket No. 180821780-8780-01)**

On behalf of the Retail Industry Leaders Association (RILA), I write to commend the National Telecommunications and Information Administration (NTIA) of the Department of Commerce for requesting comment on ways to advance consumer privacy while protecting prosperity and innovation and to highlight the care retailers take in the collection, storage, and use of customer personal information.

RILA is the trade association of the world's largest and most innovative retail companies. RILA members include more than 200 retailers, product manufactures, and service suppliers which together account for more than 1.5 trillion dollars in annual sales, millions of American jobs and more than 100,000 stores, manufacturing facilities, and distributions centers domestically and abroad.

Retail Privacy in the (R)Tech Age

U.S. and global consumers are driving change in retail at an unprecedented rate. Ubiquitous internet access, and changing consumer values, preferences, and lifestyles, have led to disruption in virtually every industry; retail perhaps more than any other. This digital revolution continues to transform the way customers buy and interact with retailers and products. And the pace and depth of these changes is both unprecedented and accelerating. Retailers are adapting to this new consumer landscape through the pursuit of transformative innovation. The convergence of retail and technology ((R)Tech) means that the retail business model has fundamentally changed, resulting in a business imperative to delight profoundly empowered consumers. To thrive in this era of (R)Tech, retailers must maintain and deepen customer trust relationships.

Retailers embrace the careful stewardship of customer data not only because maintaining customer trust is a core business imperative, but because it is the right thing to do. In designing data management systems, retailers think about the process from end-to-end. Retailers carefully consider a variety of elements to determine whether to collect data as well as the appropriate scope of collection. Some of these elements include customer benefits, business purpose of collection, customer insights available from the data, transaction friction, sensitivity and volume of data, parts of the business that need the data, and retention period. Retailers also evaluate whether a business need can be accomplished by some other means. The business reality of (R)Tech is that any friction in a retail transaction or service may undermine both customer experience and sales. Retailers understand that creating customer experiences that both enhance consumer trust and minimize needless friction ultimately will determine their success or failure.

Retailers are deeply focused on providing a delightful customer experience which begins with providing customers what they want, when they want it, wherever they are. Retailers care about customers and do everything possible to protect their data. Retailers are judicious about what data is collected, how it is used and stored, and with whom it is shared. Retailers recognize the unfortunate reality of modern cybersecurity that every sector of the economy is the target of sophisticated and coordinated cyber actors and have invested heavily to protect their customers' data.

Retail Privacy Public Policy: A Pragmatic Approach

Retailers believe that a sound public policy approach to privacy must be grounded in pragmatism. We believe in the basic proposition that retailers collect personal information about customers to help our customers find the products and services they want at the time, place, and manner of their choosing. Retailers are encouraged by the objectives and goals outlined by NTIA. As we reviewed NTIA's approach, we offer the following commentary highlighting elements retailers believe are critical to a pragmatic and workable approach to privacy at scale.

1. **National Privacy Framework.** Retailers believe a sound privacy policy framework must be national in scope to better protect customers and reduce state-level burdens on interstate commerce. Strong federal preemption is necessary to prevent a balkanized regulatory landscape and bring uniformity and rationality to myriad potential approaches. We agree with NTIA's goal to create a harmonized regulatory landscape because a national framework will better allow companies to implement privacy at scale and create clear and predictable consumer outcomes to meet their expectations.
2. **Risk-based Practical Scope.** Retailers believe that NTIA is correctly focused on a risk-based approach to privacy. Retailers support a precise and targeted definition of personal information. This core definition of sensitive personal information should be clearly linked to areas where there is a real risk of tangible financial harm. Overly broad definitions containing data that is publicly available, household level, pseudonymous, harmless, or employee data should not be included in such a definition. Creating a scope that allows companies to draw real boundaries around truly sensitive consumer personal information while enabling harmless data to be used in the context of a national privacy framework to benefit customers is vital to having a functioning privacy policy framework. Unrealistic and broad mandates that are untethered to the realities of operating at scale or enhancing privacy should find no home in this public policy framework.
3. **Reasonable Consumer Control, Access, and Correction.** Retailers believe in respecting our customers' wishes by providing reasonable control over their personal information. But, too often this debate descends into the binary options of mandatory consent for every use on the one hand and no consent for any use on the other. Retailers support providing such control, access, and correction within the reasonable context of the use of such data. Retailers agree with NTIA that "which controls to offer, when to offer them, and how they are offered should depend on context." This context includes a variety of legal, technical, financial, and security requirements that must be correctly weighed. A privacy approach that evaluates data use in context better addresses the business models and uses of data in the marketplace today rather than relying on foundational consent models alone. One area where retailers believe further research by policymakers is required involves data portability. This is an important concept which can, for example, in the social media space, enhance competition, but in other industries porting certain user generated data may ultimately create anticompetitive outcomes. To avoid these unintended consequences, retailers supports research into both the types of data that should be eligible

for portability as well as the implications of different transfer methods (e.g., direct to consumer or business to business).

4. **Incentives for Good Faith Actors**. Retailers support creating strong incentives for good faith actors to go beyond basic privacy frameworks. For example, policymakers could create legal safe harbors for good faith actors who implement additional privacy enhancements beyond baseline privacy. Retailers believe providing such incentives will not only encourage companies to embrace innovative privacy practices and technologies, but it may also serve to find new ways to eliminate impediments to enhanced consumer privacy. NTIA's stated goal to encourage privacy research is laudable, but it should be paired with an equal embrace of incentivizing innovative uses of that research in practice.
5. **Strong and Fair Enforcement**. Retailers support fair, consistent, and equitable enforcement of privacy laws. Retailers agree that the Federal Trade Commission is the appropriate enforcement agency and that enforcement of privacy laws should be consistently applied by the FTC based on cases of actual financial harm. Retailers strongly believe that enforcement through a single federal expert agency will create the correct balance between strong consumer privacy and harmful inconsistent enforcement that would occur if alternative mechanisms like private rights of action were employed.

Retailers are Committed to Protecting Customer Data and Enhancing Consumer Trust

Retailers share NTIA's desired outcome of "a reasonably informed user, empowered to meaningfully express privacy preferences, as well as products and services that are inherently designed with appropriate privacy protections..." and we are encouraged by NTIA's approach. In addition, retailers support the launch of a process by the National Institute of Standards and Technology to create a risk-based privacy framework. Retailers take a pragmatic approach to privacy that is grounded in the realities of operating global businesses that interact with millions of consumers in both the digital and physical world every day. We encourage NTIA to take a similar approach and consider the practical realities that impact Main Street. Retailers support this important NTIA effort and stand ready to work with policymakers and all stakeholders to continue to advance consumer privacy.

Sincerely,

Nicholas R. Ahrens

Nicholas R. Ahrens
Vice President, Privacy and Cybersecurity