RETAIL INDUSTRY LEADERS ASSOCIATION

1700 North Moore Street
Suite 2250
Arlington, VA 22209

www.rila.org

TESTIMONY OF

BRIAN A. DODGE, CHIEF OPERATING OFFICER

RETAIL INDUSTRY LEADERS ASSOCIATION

BEFORE THE

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

HEARING ON

"POLICY PRINCIPLES FOR A FEDERAL DATA PRIVACY FRAMEWORK IN THE UNITED STATES"

February 27, 2019

Chairman Wicker, Ranking Member Cantwell and Members of the Committee, my name is Brian Dodge and I am the Chief Operating Officer of the Retail Industry Leaders Association (RILA). Thank you for the opportunity to testify today about consumer privacy, federal data privacy legislation and the care retailers take in approaching privacy. Despite the rapid transformation of the retail ecosystem over the past two decades, our members' core business remains straight forward – to sell products and services to customers. To do so, retailers have always sought to know their customers well in order to better serve them – from the friendly chat at the market stall to recommending new products at the general store – retailers have always tried to learn more about their customers' needs and preferences in order to improve their shopping experience. While methods and technologies may have changed, leading retailers are guided by this simple purpose, to better serve customers. It is why we care so deeply about the national conversation on privacy we are engaging in today. Retailers support Congress' leadership in finding a sensible path to set clear privacy expectations for all Americans through federal data privacy legislation.

RILA is the U.S. trade association for leading retailers. We convene decision-makers, advocate for the industry, and promote operational excellence and innovation. Our aim is to elevate a dynamic industry by transforming the environment in which retailers operate. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together account for more than $1.5 trillion in annual sales, millions of American jobs, and more than 100,000 stores, manufacturing facilities, and distribution centers domestically and abroad.

Retail Today

U.S. and global consumers are driving change in retail like never before. Ubiquitous internet access coupled with changing consumer values, preferences, and lifestyles, have led to significant disruption in the industry. This digital revolution continues to transform the way customers interact with retailers and buy products. And the pace and depth of these changes are both unprecedented and accelerating. Retailers are adapting to this new consumer landscape through the pursuit of transformative innovation. The convergence of retail and technology (RTech) means that the retail business model has fundamentally changed, resulting in a business imperative to meet the desires of highly empowered consumers who have many choices for how and where to shop. To thrive in this era, retailers must maintain and deepen trust in customer relationships.

Customers can still reach retailers in physical stores and can now connect directly through digital mediums like websites and apps and indirectly through search and other social media platforms. Competition in retail is now a click or voice command away which means that retailers operate within the most competitive industry in the world. This competitive environment has empowered consumers, which means retailers must focus on more than the transaction. They must focus on building and maintaining long-term relationships with customers through positive interactions and experiences. Customers' high expectations for how retailers safeguard their data to power these interactions and experiences is equal to their expectations regarding the quality of the products they buy. Failure to meet their expectations erodes the trust that is essential to maintaining a mutually beneficial customer-retailer relationship. Robust competition in retail ensures a daily referendum on the state of retailers' relationship with their customers. Unlike some tech or telecom companies whose services or platforms tend to dominate their sectors, if a customer loses trust in one retailer, they can easily shop with another. These customer relationships grounded in trust shape how retailers approach meeting customer privacy expectations and needs.

Retailers Use Customer Data to Benefit Customers

As retailers look to personalize the experience for their customers, they rely on data that customers provide, and data that they collect when customers interact with their brands, to help those customers find the products and services they want at the time, place, and manner of their choosing. Leading retailers seek to use customers' data to better serve customers. Everyone in this room shops online, mobile, and in-store. You can all appreciate when technology or good service makes your life easier and the shopping experience better. It is within this context that leading retailers collect and use personal information and customer data.

Retailers who better know their customers can offer products that customers want. Customer data is what tells a retailer to stock your favorite brands, in the right varieties, at the right time, and in the right place. Whether it is stocking Ole Miss shirts and blankets in football season or the right Gonzaga gear in basketball season, personal information helps retailers decide how much merchandise to buy, where it needs to be and when. Data fuels retailers' ability to ensure that the small home improvement contractor can order supplies to be delivered to the appropriate jobsite and the crafter can get their

holiday supplies. Knowing what customers purchase also helps retailers stock up stores before natural disaster events with the products customers need most.

Customer data not only helps retailers make important decisions throughout their supply chains, but it also produces dividends for consumers. For many retailers, loyalty programs are an essential component of their business model, and one that provides mutual benefit. Loyal customers receive discounts and curated services and products, and retailers gain valuable insight into customer needs and preferences. Loyalty programs enable retailers to offer teachers and parents key discounts or other special offers on classroom supplies at back to school time. These discount programs often help retailers give back to the communities they serve.

Customer data also enables the services customers demand. Leading retailers are now offering the ability to order online and pick up at the store without the customer ever leaving their car. Data tells retailers how many employees need to be assigned to provide that service, identifies peak times, and specifies locations. For the dad or mom of little kids, picking up diapers or groceries with the convenience of drive-through is a game changer. Many leading retailers now offer delivery services, often in as short as two hours. Consumer opt-ins sharing geolocation or personal information ensures delivery of products to any desired location.

Personal information also enables beneficial curated experiences. When consumers interact with retailers online or via mobile app, it is personal information that allows the customer to see products and deals that are more relevant to their needs. It also allows retailers to understand the context of their relationship with each unique consumer, and to prompt individual customers with offers that are tailored to their needs and preferences. The Sunday circular once arrived on your doorstep and gave everybody one list of what was on sale within a given week in a store. Data allows leading retailers to leverage technology and advanced supply chains to target individual consumers with offerings tailored to their needs and lifestyle. Offerings like baby registries enable new parents to discover curated products based on their preferences that a new parent might not know they will need.

Personal information fuels other services that leading retailers provide to benefit communities such as flu trackers. Developed as a timely, local resource, consumers, health officials and the media now use it to track flu activity in their community. These flu trackers are compiled using retail prescription data for antiviral medications used to treat influenza across thousands of stores. In addition to helping the public, retailers use this data to determine which communities should get more flu vaccines in stock, when there is a vaccine shortage, and where to direct stock of medications to treat the flu to ensure that enough medication is available when needed.

Retail data uses are clear and within the established context of a customer relationship. Customers are just that, customers – they are not users or products. This context differentiates retail from other industries who collect and use data in ways that are not well understood, anticipated, or desired. Retailers interact directly with customers and the collection and use of personal information is to better meet customer needs.

Retail Privacy Approach

Leading 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 for customers. In designing data management systems, retailers think about the entire data lifecycle management process to determine how to collect, use, share, and protect personal information.

Retailers carefully consider a variety of elements to determine the necessity of data collection as well as the appropriate scope of collection. Some factors weighed by retailers in determining whether to collect data include customer benefits, business purpose of collection, customer insights available from the data, transaction friction, sensitivity and volume of data, and parts of the business that need the data. Retailers frequently evaluate whether a business need can be accomplished by some other means.

After retailers determine whether to collect consumer data, they also continue to reevaluate how that data is being used and stored and with whom it is shared. Leading retailers have invested heavily to protect their customers' data. Keeping personal information private begins with security. Finally, retailers determine the retention period for data to ensure that it is appropriately maintained, according to applicable law, and disposed of properly.

Retail Privacy Public Policy: A Pragmatic Approach

Leading retailers recognize this unique moment. The revelations of Cambridge Analytica coupled with legislative developments in Europe and California have fundamentally reoriented the national conversation on privacy. In today's climate, Democrats and Republicans may not agree on much, but they certainly agree on the importance of a new approach to privacy. Both the Obama[1] and Trump[2] Administrations have recognized the need to address privacy. There is a bipartisan opportunity to create a uniquely American privacy framework that embraces the dynamism of American ingenuity with the fairmindedness of making sure everyone gets a square deal.

A new privacy framework will require choices and artful balancing of interests. RILA believes that a federal privacy framework should be designed to protect consumers and provide clear rules of the road for individuals, businesses, and the government. Retailers are prepared to accept the responsibility of new privacy requirements to create a national framework that applies to all parts of the data ecosystem and inspires consumer confidence.

Retail Privacy Public Policy: Elements
RILA believes there are six critical elements to a pragmatic and workable approach to privacy at scale.

---

[1] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf (last visited Feb 2019).
[2] NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, NTIA SEEKS COMMENT ON NEW APPROACH TO CONSUMER DATA PRIVACY, (2018), https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy (last visited Feb 2019).

1. **Consumer Control, Access, Correction, and Deletion Rights.** Leading retailers believe in respecting 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 control, access, correction, and deletion rights including allowing consumers to limit sharing data with third-parties like advertisers and restrictions on targeted advertising. Retailers believe that which controls to offer, when to offer them, and how they are offered should depend on context. For example, a transaction that includes delivery necessarily includes the transmission of a customer's address to the third-party delivery service. The context of this transaction should not require consent because transferring address information is necessary to meet the customer's desire for delivery. Context may also include a variety of legal, technical, financial, and security requirements that must be correctly weighed. For example, a retailer may need to retain consumer information when it is needed to secure a transaction, prevent fraud, or comply with the law. In addition, retailers believe that policymakers should carefully evaluate the implications of multichannel collection environments by recognizing that all collection is not electronic through easily consolidated data systems, but may include a variety of interactions such as one to one connections through store associates and service professionals. 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 scrutiny by policymakers is required involves data portability. This is an important concept which can, for example, enhance competition in the social media space. However, in other industries porting certain user generated data may ultimately create anticompetitive outcomes. To avoid these unintended consequences, retailers believe that protecting proprietary business methods requires limiting portable data to content generated and submitted by the user, which would exclude data such as inferences drawn by the organization about the user or other data generated by the organization.

2. **National Privacy Framework.** Leading retailers believe a sound privacy policy framework must be national in scope to better protect customers and reduce state-level burdens on interstate commerce. Purchases no longer occur in one place. Consumers may order a product online, that comes from a store or distribution center in another state. Despite these jurisdictions, it is critical that consumers have the same set of rules, safeguards, and protections across the United States that are clear and empower them to make choices and trust that their choices are adhered to, no matter the state jurisdiction. Strong federal preemption is also necessary to prevent a balkanized regulatory landscape and bring uniformity and rationality to myriad potential approaches. We believe a national framework will better protect American innovation and allow companies to implement privacy by design, creating clear and predictable consumer outcomes to meet their expectations.

3. **Accountability for All Ecosystem Parties.** Leading retailers believe that every sector within the data ecosystem should have a responsibility to consumers. As Cambridge Analytica and Equifax have amply shown, third-parties and service providers who are often unknown to consumers must have the same responsibilities as consumer-facing companies. While contracts are certainly

necessary, they should be bolstered by enshrining the responsibilities of all parties to be diligent stewards of consumer data into law.

4. **Risk-based Practical Scope.** Leading retailers believe in a risk-based approach to privacy. The core definition of sensitive personal information should be clearly linked to areas where there is a real risk of tangible harm. Creating a scope that allows companies to draw real boundaries around truly sensitive personal information while enabling non-sensitive data to be used to benefit customers is vital to having a functioning privacy policy framework. Critical to this risk-based approach is a precise and targeted definition of personal information. Overly broad definitions containing data that is publicly available, household level, de-identified, pseudonymous, harmless, or employee data should not be included in such a definition. In addition, data that is not reasonably capable of being associated with an individual should also be excluded. Unrealistic and broad mandates that are untethered to the realities of operating at scale or enhancing privacy should find no home in a federal privacy law.

5. **Incentives for Good Faith Actors**. Retailers support creating incentives for good faith actors to go beyond baseline privacy requirements. For example, policymakers could create legal safe harbors for good faith actors who implement additional privacy enhancements beyond baseline privacy. Retailers believe one challenge to all potential frameworks is the volume, velocity, and complexity of data processing. 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. Incentives will encourage more services and products that are inherently designed to protect consumer privacy and business interests, and adapt as new privacy challenges emerge over time.

6. **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 along with state attorneys general, and that enforcement of privacy laws should be consistently applied based on cases of actual harm. Retailers recognize that beyond enhanced authority, the FTC will require additional resources to robustly enforce a federal privacy law. Retailers strongly believe that enforcement through a single federal expert agency and state attorneys general will create the correct balance between strong consumer privacy and harmful inconsistent enforcement that would occur if alternative mechanisms like private rights of action become widespread.

Retailers are Committed to Protecting Customer Data and Enhancing Consumer Trust

Retailers are encouraged by the Committee's bipartisan commitment to developing a federal privacy standard to protect consumers without stifling innovation, investment, or competition. We are also encouraged that other policymakers, including the Department of Commerce's National Telecommunication and Information Administration and National Institute of Standards and Technology, are working to define an Administration approach and to create a risk-based privacy framework. With both Houses of Congress and the Administration's support, retailers believe a federal privacy bill can become law.

Ultimately, leading 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. Retailers' primary objective is to please customers. Consequently, the industry's guiding principle on consumer privacy is that data should be used responsibly to benefit customers. We encourage policymakers to be guided by that principle and to consider the practical impact a privacy framework will have on consumers. Retailers support this important effort and stand ready to work with policymakers and all stakeholders to continue to advance innovation and consumer privacy.