Statement of the National Automobile Dealers Association
Regarding Data Privacy
Submitted to the Senate Banking, Housing and Urban Affairs Committee
March 15, 2019

Mr. Chairman, thank you for the opportunity to submit comments on the collection, use and protection of sensitive information by financial regulators and private companies. The National Automobile Dealers Association (NADA) represents over 16,000 franchised dealers in all 50 states who sell new and used cars and trucks, and engage in service, repair, and parts sales. Our members collectively employ over 1 million people nationwide, and most of our members are small businesses as defined by the Small Business Administration. In the course of their operations, NADA members have for years taken stringent steps to ensure that consumer data is protected from both a process and technology perspective.

In addition, as "financial institutions" under the Gramm-Leach-Bliley ("GLB") Act, automobile dealers have years of experience complying with strict federal safeguarding and notice requirements under federal privacy laws, such as the GLB, the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act and other federal privacy regimes. As a result, dealers have operated with certain core privacy and data security concepts and are experienced in the implementation of those concepts. Finally, as automotive retailers, dealers are intimately involved in the complicated and important privacy and security issues arising from the changes in connected and autonomous vehicles, which we believe represents a critical component of any federal privacy regime.

(A) A U.S. Privacy Regime Should Ensure Consistency

One primary concern, and a compelling reason for consideration of a broad federal approach (rather than a targeted or limited approach) is that existing international and state privacy regimes already seek to address broad issues and have raised tremendous compliance burdens, costs, and confusion among consumers and businesses alike. The EU's General Data Protection Regulation, along with the California Consumer Privacy Act (and several other comparable proposed state laws) have similarities, but each add their own layer of compliance cost and burden for U.S. businesses without any additional material benefit to consumers. This problem will only be exacerbated if other states enact their own approach. The very nature of data and personal information makes a patchwork privacy approach untenable. Data's non-physical nature, along with the legitimate need for businesses of all types to share and store data around the country and across state lines, makes privacy issues – as a general and practical matter – ill-suited to a patchwork of state regulation.

We urge the Committee to ensure that any federal privacy approach is not only clear and understandable, but also preempts state privacy laws so that businesses can avoid competing and potentially conflicting privacy obligations and instead comply with one national privacy standard. Preemption does not mean that the privacy protections should be weakened, but would instead allow businesses (particularly small businesses) to apply their limited compliance resources to one set of rules and comply with one privacy standard.

(B) Transparency and Consumer Choice Are Critical

We support efforts to provide consumers with both transparency about the data collected about them and with meaningful choices about how that data is used and shared. These concepts, along with the others outlined in the Fair Information Practice Principles[1] ("FIPPs") are the best starting point to guide businesses and protect consumers. While approaches to reaching the goals of these principles vary, the starting point remains the same -- consumers must be able to understand what personal information they are sharing (or is being collected from them), who has access to that information, and how it is used. Transparency is and should be the backbone of any privacy regime. When consumers do not know what information is being collected, or how it is being used, it generates mistrust and heightens the potential for abuse, and that benefits neither business nor consumers.

It is critical in our view that consumers not only have readily-available, standardized access to information about how their personal information is stored, who is storing it and how it is used, but they should also have a clear choice regarding its storage and use, as well as a simple way to exercise that choice. Consumers should be able to exercise that choice not only at the point and time of collection, but in an ongoing manner as well.

(C) Consumer Education is Critical

A related issue we believe will be critical in implementing a federal privacy regime is consumer education. How will consumers be educated so that they understand the choices they have and the implications of those choices? We urge the Committee to consider this question, and to work with interested industry participants and others to ensure that any overall privacy approach includes this important component.

[1] These principles – Notice, Choice, Access, and, Security have been around since the early 1970s, and the FTC has described them as "widely-accepted." The principles were summarized by the FTC in a May 2000 report to Congress (https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf) as follows: (1) Notice - data collectors must disclose their information practices before collecting personal information from consumers; (2) Choice - consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided; (3) Access - consumers should be able to view and contest the accuracy and completeness of data collected about them; (4) Security - data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

(D) Any Technical Requirements Must Be Flexible

General principles and duties are important, but ultimately businesses will need to implement any privacy or security requirements in actual practice. We urge the Committee to ensure that any specific technical requirements be flexible and not prescriptive. This approach is critical: (i) to allow for changes in technology and best practices, and (ii) because reaching the goal is the key, not necessarily utilizing a specific means to do so. In addition, it is critical to remember that any general privacy regime will likely apply to businesses of all sizes and levels of funding and sophistication. Requirements must be clear and flexible so that small businesses with limited technical or compliance resources can comply, along with the largest and most sophisticated businesses.

(E) Enforcement Must Be Based on Clear Objective Standards

Accountability is an important part of any privacy regime; and an important component of "accountability" is regulatory enforcement. We therefore urge the Committee as it goes forward to ensure that privacy enforcement is based on a clear set of well-defined and reasonable rules. Broad standards of "unfairness," or fiduciary-type duties, are likely to be too broad and ill-defined for businesses to ensure compliance and will lead to uneven enforcement without concomitant consumer benefit. Simply put, privacy enforcement cannot be based on whether an activity or disclosure is "unfair" because it fails to provide the legal clarity that businesses and consumers need. Indeed, enforcement under this type of standard often leads to "after-the-fact" enforcement – that is, enforcement based on an *outcome* which, when viewed in hindsight, is "unfair" to consumers, regardless of whether the business took appropriate or reasonable steps before the incident.[2] No business should be allowed to refuse to meet, avoid, ignore, or in bad faith fail to meet clear privacy requirements. However, no reputable business *wants* to suffer a security incident or mishandle their customers' data. Businesses must have clarity to determine how they can meet their obligations.

a. Consider a "Safe Harbor" Approach

One reasonable way for privacy legislation to provide consumer privacy protection, while also providing the needed legal clarity for businesses with respect to consumer data privacy, is to adopt a "safe harbor" approach. In other words, to implement a privacy regime whereby a business who meets or seeks in good faith to meet objective privacy requirements[3] will have "safe harbor" protection, which will account for their efforts even if an event occurs that fails short of the privacy ideal. There are many analogs for such safe harbors under federal law, and this is another context in which this approach is the best balance between privacy ideals and reasonable best efforts in the real world.

[2] Indeed, even many of the most well-funded and sophisticated businesses and federal agencies have suffered data breaches and security incidents.

[3] One possible example would be to provide a Safe Harbor for provisions requiring protection of consumer data to entities that already meet the FTC Safeguards Rule.

(F) Automobiles Present Specific and Important Privacy Issues Because Automotive Data Privacy Impacts Automotive Safety

Lastly, it is important that the Committee be aware of the unique privacy concerns in the automotive context and the inextricable connection between privacy, cybersecurity and safety of automobiles. In short, with cars, any privacy requirements will necessarily implicate vehicle safety, environmental, and other risks. Therefore, the privacy approach to the automotive industry should be more analogous to the aviation industry than to other, less safety-critical industries.[4] NADA, in connection with the FTC/NHTSA connected car workshop[5] , submitted comments that provides additional details on some of the privacy and related cybersecurity issues with the modern automobile and highlights the applicability of some of the privacy concepts in the automotive and dealership context.

Conclusion

Mr. Chairman, we applaud the Committee for its interest in this important topic, and its focus on harmonizing the legal and regulatory landscape. NADA believes that this is a critically important issue for consumers, businesses, and ensuring the competitive posture of the United States. We welcome the opportunity to comment further as the Committee drafts and considers privacy legislation.

[4] See for example NADA's July 2, 2015 letter to House Energy and Commerce Committee outlining some of the cybersecurity issues with automobiles.
[5] Found at https://www.ftc.gov/system/files/documents/public_comments/2017/05/00038-140613.pdf