Connected Cars Workshop and P175403

The Alliance of Automobile Manufacturers (Alliance)[1] appreciates this opportunity to provide input to the Federal Trade Commission (FTC) and the National Highway Traffic Safety Administration's (NHTSA) proposed information collection activities with regard to their review of the consumer privacy and security issues posed by "connected vehicles," including vehicles currently on the road, V2V- and V2I-equipped vehicles, and automated vehicles.

Vehicle connectivity and automation have the potential to play an important and integrated role in crash prevention and congestion mitigation, leading to improved safety, enhanced mobility and reduced fuel consumption, among other benefits. Many of the connected and automated vehicle technologies and services are based upon information obtained from a variety of vehicle systems and may involve the collection of information about a vehicle's location or a driver's use of a vehicle. As reliance on data by these connected and automated vehicle technologies increase, consumer privacy and security continue to be important issues.

Fortunately, automakers, including Alliance members, have already taken proactive steps to ensure that consumer privacy is protected and automotive cybersecurity is maintained. In 2014, the Alliance and Global Automakers issued the Privacy Principles ("Principles"). The Principles provide an approach to customer privacy that Participating Members[2] can choose to adopt when offering innovative vehicle technologies and services. Specifically, they apply to the collection, use, and sharing of information in association with vehicle technologies and services available on cars and light trucks sold or leased to individual consumers for personal use in the United States. This information, referred to in the Principles as "Covered Information," includes identifiable information that vehicles collect, generate, record or store, which is retrieved from the vehicle by the automaker, as well as personal subscription information provided by individuals subscribing or registering for vehicle technologies and services.

The Principles are meant to be flexible so that each company can tailor them to their specific needs, reflecting differences in technologies and other distinguishing or company specific factors. Participating Members may choose to incorporate into their privacy programs elements that are not addressed in the Principles and are free to take additional privacy steps. Regardless of how Participating Members design their privacy programs and implement the Principles, Participating Members affirm the following fundamentals:

- **Transparency:** Participating Members commit to providing owners and registered users with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of Covered Information.

- **Choice:** Participating Members commit to offering owners and registered users with certain choices regarding the collection, use, and sharing of Covered Information.

[1] The Alliance is the leading advocacy group for the auto industry. Its members include BMW Group, FCA US LLC, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America and Volvo Cars North America, and represent about 70 percent of all car and light truck sales in the United States.

[2] All Alliance members are Participating Members.

- **Respect for Context:** Participating Members commit to using and sharing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on owners and registered users.

- **Data Minimization, De-Identification & Retention:** Participating Members commit to collecting Covered Information only as needed for legitimate business purposes. Participating Members commit to retaining Covered Information no longer than they determine necessary for legitimate business purposes.

- **Data Security:** Participating Members commit to implementing reasonable measures to protect Covered Information against loss and unauthorized access or use.

- **Integrity & Access:** Participating Members commit to implementing reasonable measures to maintain the accuracy of Covered Information and commit to giving owners and registered users reasonable means to review and correct Personal Subscription Information.

- **Accountability:** Participating Members commit to taking reasonable steps to ensure that they and other entities that receive Covered Information adhere to the Principles.

In August 2015 the Alliance and Global Automakers worked to establish a proactive information sharing and analysis center, known as the Automotive Information Sharing and Analysis Center ("Auto-ISAC"). The Auto-ISAC is a secure forum that promotes the voluntary sharing of cybersecurity threat and vulnerability information among its members to enhance vehicle security and safety across the industry. Through this mechanism, members of the Auto-ISAC may anonymously submit and receive information to help them more effectively counter cyber threats in real time. Currently, Auto-ISAC members account for more than 99 percent of light-duty vehicles on the road in North America, and now many tier one suppliers. The Auto-ISAC also has global representation from companies in Europe and Asia.

In addition to facilitating voluntary information sharing, the Auto-ISAC is creating and maintaining a series of Automotive Cybersecurity Best Practices ("Best Practices") that expand on the Framework for Automotive Cybersecurity Best Practices ("Framework") completed in January 2016 by the Auto Alliance and the Global Automakers. The Best Practices address the organizational and technical aspects of vehicle cybersecurity, including governance, risk management, security by design, threat detection, incident response, training, and collaboration with appropriate third parties.

Automakers are also working together to address cybersecurity through a collaboration between the Alliance, Global Automakers and DOT known as the Proactive Safety Principles, released in January 2016. The objective of the fourth Principle, "Enhance Automotive Cybersecurity," is to explore and employ ways to collectively address cyber threats that could present unreasonable safety or security risks. This includes the development of cyber best practices through the ISAC to secure the motor vehicle ecosystem.

The auto industry is not waiting for cyber threats to evolve into safety risks for *any* vehicle (connected, automated, or "Level 0") before addressing resilience methods. Likewise, the auto industry is not taking a back seat on addressing increased privacy concerns posed by connected and automated vehicle technologies and services. Alliance members recognize that robust consumer privacy and cybersecurity protections have increasing importance as connected and automated vehicle technologies are

introduced in the on-road vehicle fleet, and they are committed to working together as they have done in the past to proactively address these issues.

Similarly, Alliance members remain committed to working with government agencies on automated and connected vehicle privacy and security issues. The FTC has requested input regarding the role of the FTC, NHTSA and other government agencies with respect to these issues. The Alliance recognizes the importance of this question, as vehicle privacy and cybersecurity topics are often interrelated both on and off the vehicle. As automated and connected vehicle technologies become more prevalent, it is important to delineate responsibilities to the appropriate government agencies in order to streamline processes and provide clear guidance for automakers. The technological needs, benefits, risks, and associated policy considerations likely differ depending on the type of service or function. As a first step to differentiating distinct governing roles in this space, it might be prudent for the FTC and NHTSA to develop a memorandum of understanding (MOU). The MOU could provide a framework for the FTC and NHTSA to determine the best way to limit overlap between the agencies, given that the FTC's focus should remain on privacy and cybersecurity issues that are not connected with the active operation of the vehicle or its features.

The Alliance appreciates the FTC's and NHTSA's consideration of these comments. Please feel free to contact us if you have any questions about the Alliance's position or would like to discuss any aspect of these comments.