Connected Cars Workshop and P175403

Comments of the Association of Global Automakers

FTC and NHTSA Workshop on Privacy and Security Issues Related to Connected and Automated Vehicles

The Association of Global Automakers (Global Automakers)[1] appreciates the opportunity to provide these comments in response to the March 20, 2017 request for input from the Federal Trade Commission (FTC) and National Highway Traffic Safety Administration (NHTSA) on connected and automated vehicles. These technologies hold great promise for vastly improving vehicle safety, mobility and sustainability for consumers, and automakers today are designing these vehicles to address the important privacy and security concerns that are the subject of this workshop.

The automotive industry is in the midst of an unprecedented wave of technological innovation that is redefining how we think about transportation. Advancements in connected and automated vehicle technology promise to enhance mobility, help save lives, improve transportation efficiency, and reduce fuel consumption and associated emissions. Over the past several decades, automakers have made tremendous strides in safety by improving vehicle crashworthiness. Today, manufacturers are deploying crash avoidance technologies to help prevent crashes from occurring altogether. With the introduction of advanced sensors, such as cameras and radar, a number of vehicles on the road today already provide automated functionality through advanced crash-avoidance and convenience features like automatic emergency braking, lane keeping assist, and adaptive cruise control. These systems, which are foundational to the development of more highly automated systems, are designed to provide support to the driver only in certain situations. As these systems become more advanced, a vehicle's capability to operate without active control by the driver will increase.

The next breakthrough in vehicle safety, and a critical technology for realizing the benefits of automated driving, is connected car technology enabled through Dedicated Short Range Communications (DSRC).[2] While cars equipped solely with sensors such as radar, LIDAR and cameras can "see" the immediate, surrounding environment within the line of sight of the

[1] Global Automakers represents the U.S. operations of international automobile manufacturers and automotive suppliers. Our automaker members design, build, and sell cars and light trucks in the United States and abroad, and these companies have invested $56 billion in U.S.-based facilities, directly employ nearly 100,000 Americans, and sell 47 percent of all new vehicles purchased annually in the country. Combined, our members operate more than 300 production, design, R&D, sales, finance and other facilities across the United States.

[2] The term "connected vehicle" can refer broadly to cars and trucks equipped with certain technologies and services that transmit and receive data wirelessly. These vehicles can have the capabilities to connect to the internet via a cellular or other wireless connection, and/or connect to other vehicles, infrastructure, and other road users using DSRC-enabled communications.

sensors, DSRC supports "vehicle to vehicle" (V2V) and "vehicle to infrastructure" (V2I) communications (collectively referred to as "V2X" systems) that enable cars to wirelessly connect to other road users and the surrounding infrastructure to effectively "see" around corners, achieving greater 360-degree situational awareness. DSRC can work alone as a sensor to inform or warn the driver to avoid a crash, or it can work in concert with other sensors and vehicle systems to support automated driving features, such as cooperative adaptive cruise control.

These advanced vehicle systems, as well as modern driver-convenience systems that are prevalent today (such as GPS-enabled navigation systems and infotainment systems that can connect to a driver's handheld device), generate and utilize a tremendous amount of data. Global Automakers supports NHTSA's and the FTC's efforts to gather input from industry stakeholders and the public to better understand the concerns and challenges that arise with respect to protecting that data. These concerns should be addressed in a manner that allows solutions that are flexible and responsive to changes in technology to promote innovation and ensure that consumers realize the maximum benefits from increased connectivity. Global Automakers looks forward to engaging further with NHTSA and FTC as it moves forward in this process.

Data Collection and Use and Effect on Vehicle Functionality (Questions 1 and 2)

Different types of data are generated by motor vehicles in order to satisfy different functional requirements. Much of that data exists temporarily or remains entirely on the vehicle, while some may be transmitted to and from the vehicle in order to perform a vehicle function or provide a customer service.

- Data generated for the operation of the vehicle: During operation, onboard computer systems frequently exchange data to support the normal functioning of the vehicle. This category of information is typically not transmitted outside of the vehicle, nor is it retained in the long-term memory of the vehicle.

- Data transmitted outside the vehicle: Certain data may be transmitted outside of the vehicle to perform a specific function or provide a service for the customer. This category of data includes, for example, automatic crash notification systems that alert emergency responders to a crash scene or vehicle maintenance diagnostics systems.

- Data transmitted into and out of the vehicle: Depending upon the complexity of the design, certain systems provide information back to the vehicle operator. For example, beyond basic route information, some enhanced navigation systems provide the operator with current traffic details and provide alternate directions. With other applications, transmitting data into and out of the vehicle allows consumers greater convenience and understanding by offering features such as remote monitoring of vehicle location, remote start and on-board diagnostics and other information.

- Data legally required to be generated: Some technical information is legally mandated to be gathered and stored on the vehicle, such as certain data elements in the emissions

controls systems. A vehicle event data recorder (EDR) is also required to capture certain data elements, if the vehicle is equipped with such a device.

- Shared Data: Certain data generated by a vehicle may be shared with third parties. For example, information related to the performance, operation and safety of a vehicle is shared with dealers which, in turn, share the information with the manufacturer. In the case of a safety recall, this information is shared pursuant to law. There is also some limited information that may be shared for marketing purposes, which can provide the consumer with information about additional products or services that may be of interest. As described below, information is not shared with third parties without customer consent to do so.

Privacy and Security (Questions 4 and 6)

Global Automakers understands that a number of privacy and security issues may arise with respect to the data that vehicles generate for the operation of advanced vehicle systems. Some of these technologies, which are intended to provide better vehicle safety, performance and convenience, often rely on personally identifiable information, *e.g.*, information regarding the precise locations of vehicles or how drivers operate their vehicles. Accordingly, it is important for consumers to understand how such information is collected, transmitted and shared, and to have confidence that the vehicle data and operation will be protected from cyber-attacks.

With respect to V2Vand V2I communications, NHTSA has correctly concluded that these communication technologies generally do not present a significant privacy risk to individuals since they do not collect or store personally-identifiable information, or information that can be linked to any individual or vehicle. Moreover, to address security concerns, DSRC technology already has layers of security established into its design. Central to these protections is the use of a Security Credential Management System (SCRM) which requires messages to have certificates in order to be "accepted" by others operating within the network. Such certificates are changed frequently to prevent system attacks and apply to messages from an original equipment device or an aftermarket product.

The automotive industry has taken a number of proactive measures to address privacy and security concerns. With respect to cybersecurity, in 2015 the auto industry proactively established the Automotive Information Sharing and Analysis Center (Auto-ISAC) to share intelligence on threats and vulnerabilities among industry stakeholders.[3] In addition, the Auto-ISAC is currently working with experts within the auto industry to develop cybersecurity best practices based on the Cybersecurity Principles Framework published by the auto industry in January 2016.[4]

[3] https://www.automotiveisac.com/

[4] "Framework for Automotive Cybersecurity Best Practices" (2016) (available at http://globalautomakers.org/media/press-release/automakers-develop-framework-for-automotive-cybersecurity-best-practices).

Privacy and security issues may be exacerbated by wireless-enabled aftermarket products that connect to vehicles via on board diagnostics ("OBD-II") ports. While OBD-II is required by law to monitor emissions and provide certain diagnostic capability, these ports were not designed to be used for these aftermarket devices. These products present an opportunity for vulnerabilities and cyber-threats, and have the potential to introduce vulnerabilities by enabling connectivity that may be remotely exploited. Consequently, developers and third party vendors should take appropriate steps to design and manufacture secure products when developing these devices.

Global Automakers recognizes that gaining consumer trust in vehicle communication technologies is key to ensuring public acceptance and procuring the actual use of these beneficial devices. To that end, Global Automakers and its member companies committed to a series of FTC-enforceable privacy protection principles for vehicle technology and services (the "Privacy Principles").[5] The Privacy Principles are rooted in transparency and consumer choice. Under these Privacy Principles, consumers are advised by the automaker of the ways in which data related to the vehicle, owner or authorized user are collected and may be used. The Principles also include heightened protections for personally identifiable information, such as geolocation, driver behavior, and biometric information.

Roles of Industry and Government Stakeholders Related to Privacy and Security (Questions 3 and 8)

While both the FTC and NHTSA have significant roles to play in navigating the connected vehicle landscape, Global Automakers believes the FTC should have the primary role in overseeing data privacy. The FTC is uniquely positioned in this respect as it has been at the forefront of the development of privacy-related policies and best practices. The FTC has the experience and expertise in this subject, having already addressed privacy and data security concerns in multiple other contexts and emerging areas. Global Automakers also believes that it is essential to clarify the roles and responsibilities of the federal agencies involved in managing the security of data in connected vehicles. Further, because the connected vehicle landscape is an evolving one, Global Automakers urges all agencies charged with oversight to work collaboratively with industry stakeholders in creating a balanced policy framework that takes into account the need for safety while permitting innovation.

Consumer Perception (Question 7)

Consumers' understanding of, and trust in, connected and automated technologies is essential. The full safety and other benefits will not be achieved if consumers are afraid of the technology. Consequently, we believe consumer education is paramount. We would also welcome federal actions to encourage the participation of others within the connected car ecosystem, including manufacturers of after-market devices that connect to the vehicle, in order to educate consumers concerning how to properly use such devices so as to minimize any potential cyber vulnerability.

[5] "Privacy Principles for Vehicle Technologies and Services" (2014) (available at http://www.globalautomakers.org/media/papers-and-reports/privacy-principles-for-vehicle-technologies-and-services)

Self-Regulatory Standards (Question 9)

Given the unprecedented pace of technological innovation in the auto industry—innovation that presents enormous opportunities for further enhancing mobility, saving lives, and improving transportation efficiency—it is important to recognize that the traditional regulatory approach may not be best suited for addressing vehicle cybersecurity and privacy. Industry-led initiatives have the distinct advantage of greater flexibility in responding to rapid changes in technology without supplanting regulations where they already exist.

As discussed above, the auto industry has successfully implemented industry-led actions with respect to consumer privacy and cybersecurity. In 2104, automakers issued their Privacy Principles to address the various types of vehicle and driver information that are collected and how this data is used. On the cybersecurity front, automakers formed the Auto-ISAC to share threat information, and leveraged those efforts in the ongoing development of cybersecurity best practices. In January 2016, Global Automakers and the Alliance of Automobile Manufacturers released a Framework for Automotive Cybersecurity Best Practices to serve as the foundation for the development of industry-wide automotive cybersecurity Best Practices, and the Auto-ISAC is currently working with automakers on the development of a series of best practices. The industry has also coordinated with NHTSA, which issued its *Cybersecurity Best Practices for Modern Vehicles* in October 2016 to complement the industries efforts on this issue.