Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of:	)	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	)	Docket No. 160331306-6306-01

COMMENTS OF THE ALLIANCE OF AUTOMOBILE MANUFACTURERS

Jonathan Weinberger
Vice President, Innovation and Technology
Alliance of Automobile Manufacturers

Michael Spierto
Director, Federal Affairs
Alliance of Automobile Manufacturers

June 3, 2016

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of:	)	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	)	Docket No. 160331306-6306-01

COMMENTS OF THE ALLIANCE OF AUTOMOBILE MANUFACTURERS

The Alliance of Automobile Manufacturers (Auto Alliance) welcomes this opportunity to respond to the National Telecommunications and Information Administration (NTIA) request for public comment (RFC) on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things.[1]

The Auto 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, representing 77 percent of all car and light truck sales in the United States.

The members of the Auto Alliance are helping to shape the future of transportation via the development and deployment of new technologies that will potentially improve safety, increase connectivity, expand mobility, and reduce congestion. These technologies and their use raise

[1] Notice and Request for Public Comment, 81 Fed. Reg. 19,960 (April 6, 2016).

policy questions, so we are therefore pleased to offer comments in response to a number of the following questions posed by NTIA in its RFC.

1b. What are the novel policy challenges presented by the IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and approaches address these new challenges, and if not, why?

Much of existing technology policy has been developed and applied in industries and sectors that have had the ability to innovate in a largely unregulated, or at least lightly regulated, environment. The ever-expansive Internet of Things (IoT) is broad and encompasses sectors, such as the automotive and medical device sectors, that, by contrast, have been traditionally highly regulated. An asymmetrical regulatory environment within the IoT could result in an imbalance of innovation, with more lightly regulated sectors potentially able to bring to market new technologies, products, and services more quickly than those which are more heavily regulated.

1c. What are the most significant opportunities and/or benefits created by IoT, be they technological, policy, or economic?

Today's automobile represents the most sophisticated technology owned by most consumers, as more and more vehicles are equipped with connected services, such as automatic collision notification and stolen vehicle locator, and connected infotainment systems, which provide drivers and passengers with more real-time information on traffic and road conditions. Some

vehicle owners are now able to interact with their vehicles from their smartphones to pre-heat their car on a cold day, check to see if they remembered to roll up a window or close the trunk, confirm that they have enough gas to get to work, or find out if their teenage son or daughter is driving safely.

We are also starting to see the deployment of new connected technologies that allow consumers to interact with their homes or communities. In the near future, a driver may be able to lock his or her front door, turn off the lights in the house on the way down the driveway in the morning, pre-heat the oven on the way home from work, or locate and reserve an available parking spot. These services can offer greater convenience and integration to consumers.

Communications technologies are poised to vastly improve the driving experience. In this realm, the potential benefits go beyond economic and societal improvements: they have the opportunity to save lives. For example, emerging vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications technologies have the potential to reduce congestion, enhance mobility, and improve safety. Moreover, such technologies have the potential to enhance the ability of high-level automated vehicles (AV) to perceive their environments.

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: consumer vs. industrial; public vs. private; device-to-device vs. human interfacing?

The term “connected cars” is often used to refer to many distinct types of connectivity. For example, “connected car” may refer to the ability of a vehicle to communicate directly with another vehicle or with the infrastructure around it (vehicle-to-vehicle and V2I communications). Additionally, “connected car” may also refer to the ability of an owner to interact with his or her car from a smartphone or interact with a home from his or her car. More broadly, “connected car” has been described to include in-vehicle services provided to a driver or passenger that are enabled by connectivity.

There are further differences in the functions and features provided by each of these types of connectivity. For example, there may be V2I communication that is focused on preventing crashes and there may be V2I communication that is focused on providing information to local governments on the location of potholes or ice patches. In-vehicle services enabled by connectivity may be a safety-related (such as automatic collision notification) or convenience-related (such as real-time traffic information).

The technological needs, benefits and risks, and associated policy considerations often differ fundamentally depending on the type of service or function. It is important for the government to understand the differences in connected car services and functionality that they can provide, and pursue policies appropriate within the context of their function or service.

6. What technological issues may hinder the development of IoT, if any?

i. Interoperability

For communications technologies to effectively support next-generation crash avoidance systems, it is critically important that all vehicles speak the same language. A vehicle must be able to communicate with vehicles from other manufacturers when it is first sold or leased, but also with vehicles sold or leased many years later. The National Highway Traffic Safety Administration (NHTSA) recognizes the importance of ensuring interoperability for this type of connected vehicle network, and we expect that the agency will issue a Notice of Proposed Rulemaking (NPRM)[2] to provide for that interoperability over the next few months.

ii. Spectrum availability and potential congestion/interference

V2V and V2I technologies rely on Dedicated Short Range Communications (DSRC). These communications are one-way or two-way short-range to medium-range wireless communication channels specifically designed for vehicles to communicate between each other and with infrastructure at a particular frequency. Connected vehicle technologies based on DSRC have the potential to provide multiple societal benefits including saving lives, reducing crashes, increasing mobility, and moving toward a more sustainable transportation system.

V2V communications transmit messages between vehicles about vehicle speed, direction, brake status, and other information with range and detection capabilities that exceed

[2] Federal Motor Vehicle Safety Standard (FMVSS) 150--Vehicle to Vehicle (V2V) Communication. The proposed rule is currently being reviewed by the Office of Information and Regulatory Affairs at the Office of Management and Budget.

sensor/camera/radar-based systems. This longer detection distance and ability to "see" around corners or "through" other vehicles help V2V-equipped vehicles perceive some threats sooner than sensors, cameras, or radar can, and alert their drivers accordingly. DSRC will augment information from on-board sensors, cameras, and GPS to provide greater situational awareness and improve the decisions made by automated vehicles regarding safety-critical situations.

Following over a decade of research and nearly a billion dollars of public and private investment, NHTSA is expected to propose a new Federal Motor Vehicle Safety Standard to require DSRC in all new vehicles to support V2V communication for safety applications[3]. In addition, the U.S. Department of Transportation is leading the development of V2I communication technology using DSRC for safety, automation, mobility, and sustainability applications.

DSRC is uniquely configured to enable continuous, low latency, and secure data exchanges among moving vehicles and between vehicles and roadway infrastructure or mobile devices to support safety-critical applications, as well as automation, mobility, and environmental applications. The Federal Communications Commission (FCC) has allocated 75 MHz of the 5.9 GHz spectrum at 5.850-5.925 GHz to the mobile service for use by DSRC systems operating in the Intelligent Transportation System (ITS) vehicle safety and mobility applications. In making this allocation for DSRC, the FCC noted that DSRC applications are a key element in meeting the nation's transportation needs and in improving the safety of our nation's roadways.

[3] ibid

Sufficient spectrum is necessary to facilitate the development and growth of DSRC applications that are anticipated in the future. V2V crash imminent safety applications, enabled by the planned NHTSA rulemaking, are only the first of the many DSRC applications expected to be widely deployed. Examples of expected future DSRC applications include additional low-latency V2V applications to support automated vehicles, public safety applications for ambulances and other emergency responders, vehicle to infrastructure applications to decrease traffic congestion and vehicle to pedestrian applications to improve urban movement and safety.

The FCC is inquiring about the feasibility of sharing spectrum in the 5.9 GHz band with unlicensed users to ease Wi-Fi congestion. Automakers remain open to sharing this spectrum as long as there is no harmful interference to V2X communication and have been active participants in both the FCC and DOT rulemakings to this end. Efforts to re-channelize the 5.9 GHz band will likely result in interference and will certainly complicate and delay further DSRC deployment, which has already begun.

10. What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?

V2I communication offers important supplemental benefits to V2V communication that should not be ignored. This includes information about stopped vehicles ahead, complicated or sudden lane merges, and upcoming roadway construction, as well as the ability to detect pedestrians or bicyclists. V2I communication also enables communication from the vehicle to the infrastructure, providing a means through which transportation planners and policymakers can

gain important information about when and how roads are being used, potentially aiding efforts to improve transportation efficiency.

We recommend that the federal government look at ways to encourage investment in intelligent transportation infrastructure to support V2I communication in the United States. A commitment to intelligent transportation will encourage automakers to bring new technologies to the U.S. market. Positive activity is underway at both the Department of Transportation and the National Institute of Standards and Technology to develop smart and connected infrastructure in pilot cities; this activity should continue and be expanded. At the same time, the government should pay special attention to ensuring the interoperability of intelligent infrastructure that is deployed as part of these pilot programs in order to assist its universal deployment.

15. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

Government has an important public interest and role to play to facilitate the benefits of technology in a safe fashion. Government policy can either smooth the way for prudent deployment of automation or it can create roadblocks, even if unintentional, that could inhibit the emerging safety, environmental and economic benefits.

Finding the proper public balance that maximizes safety and innovation should be the threshold for government entities when addressing some of the challenges of IoT public policy. Policy consistency and coherence, along with flexibility, are absolutely critical to serve the larger public

interest related to such safety technologies. The Alliance recommends that the government take an approach that encourages innovation and does not impede the adoption of the array of societal benefits at stake. By exercising regulatory restraint, the federal government would be recognizing the limitations of regulation at this juncture, and the potential adverse impacts that over-regulation may have on the introduction of important new technologies.

For the automotive industry, the outcomes of some major policy issues could help to either accelerate or hinder the potential benefits of connected and automated vehicles. Some current and possible future policy areas of consequence to the industry include, among others, burdensome or inconsistent and/or competing federal and state laws and regulations, appropriately preserving spectrum for V2V and V2I use, data privacy, and cybersecurity.

16a. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

The auto industry is aware that connectivity can spawn cybersecurity concerns, and that the cybersecurity risks that exist for other connected devices could also exist in the automotive context. Members of the Auto Alliance remain vigilant against the potential consequences of a successful, real-world cyber attack on a vehicle, and are incorporating modern and robust security protections in vehicle design and manufacturing.

In an effort to further strengthen automotive cybersecurity, automakers have established an Auto Information Sharing and Analysis Center (Auto-ISAC) to enhance the sector's ability to identify and respond to potential cyber threats. The Alliance believes it is an important step for the industry to take to promote the exchange of information about cybersecurity threats to vehicles and their onboard networks and to facilitate the sharing of best practices for how to safeguard against and respond to such threats. Furthermore, the Auto-ISAC's members are currently in the process of creating vehicle cybersecurity best practices.

We believe that voluntary, stakeholder-led efforts like these should be encouraged and supported by the government. However, for the very same reasons that the government has refrained from mandating cybersecurity standards in other sectors, there is a significant risk associated with mandating cybersecurity standards in the IoT or automotive space. In view of the need to protect consumers from cyber threats, which are very dynamic, we believe a flexible and nimble stakeholder-led approach has been the most effective way to address cybersecurity. The threat landscape is constantly changing, with new tools and techniques aimed at circumventing the latest security architectures. Therefore, mandating specific standards or practices for cybersecurity could have the inverse effect of their intentions, and discourage companies from exceeding them or innovating new cybersecurity practices.

17c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

In November 2014, a large group of automakers published the Consumer Privacy Protection Principles for Vehicle Technologies and Services (Privacy Principles), which include meaningful protections on the use of vehicle data and were inspired by the Fair Information Practice Principles. The Privacy Principles include heightened protections on the use of certain vehicle data, including information about a vehicle's location and how someone drives a vehicle. For example, the Privacy Principles say that automakers will not to share this type of vehicle data with third parties for their own use or use this type of vehicle data for marketing purposes without the affirmative consent of the vehicle owner. Additionally, the Privacy Principles describe circumstances in which the government may access vehicle data (such as location information), and permit access only if law enforcement obtains a warrant or court order. The industry chose to formally file the Privacy Principles with the Federal Trade Commission, thereby ensuring they are enforceable under Section 5 of the Federal Trade Commission Act.

The Department of Commerce has promoted and encouraged sectors to adopt these types of privacy commitments in the past and should continue to do so. The Alliance supports granting the Federal Trade Commission the authority to issue safe harbors to industries that adopt and comply with meaningful self-regulatory codes of conduct.

21. What issues, if any, regarding IoT should the Department focus on through international engagement?

Nearly all automakers are global companies, selling products and providing services throughout the world. Different regulatory frameworks in different parts of the world may complicate the

ability to do that. There is value in the government working with other countries to avoid a patchwork of inconsistent or even contradictory national frameworks on the IoT.

27. How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would on overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?

There are a number of Federal agencies that are seeking to oversee, regulate, or influence cybersecurity and privacy practices relating to the IoT. The resulting profusion of agencies, working groups, memorandums, and jurisdictional claims is exceedingly difficult to manage and prioritize. The government and private sector should work together to consolidate these efforts in order to provide clarity around the appropriate roles of both in order to advance policies that balance security and innovation.

Automakers are currently facing a patchwork of state laws and regulation, which could significantly deride both public confidence and industry investment in the deployment of new vehicle technologies. A regulatory regime that changes from one state to the next will dramatically impede the development of automation. For example, when one state requires a steering wheel and foot-applied brakes, while another state does not, the ensuing confusion creates needless obstacles.

Both state and federal rulemaking takes significant time to develop and even more time to adjust to technological advances. For connected vehicles and automated driving technologies, the innovation outpaces the ability of government to impose a traditional regulatory and rulemaking approach. The Auto Alliance contends that the public interest will be dramatically enhanced when policymakers from every dimension of government come together to forge a consistent, coherent and flexible approach to mobility innovation.

***

Thank you again for this opportunity to share the Alliance's views on the IoT, its associated benefits, and relevant policy considerations. We look forward to publication of NTIA's Green Paper and hope we can serve as constructive participants as this process moves forward.

Respectfully submitted,

Jonathan Weinberger
Vice President, Innovation and Technology
Alliance of Automobile Manufacturers

Michael Spierto
Director, Federal Affairs
Alliance of Automobile Manufacturers

June 3, 2016