Additional Questions for the Record

Subcommittee on Consumer Protection and Commerce
Hearing on
"Autonomous Vehicles: Promises and Challenges of Evolving Automotive Technologies."
February 11, 2020

Mr. John Bozzella, President and CEO, Alliance for Automotive Innovation

The Honorable Bobby Rush (D-IL)

1. Mr. Bozzella, as cars become increasingly automated, they will continue to generate even greater amounts of data, a fact that comes with enormous implications. From your understanding, who owns this data? Who can access it and for what purpose? Furthermore, who should own this data?

Automakers are incorporating advanced technology into modern automobiles at an increasing rate, making vehicles safer, cleaner, and smarter. These technological advances provide numerous social and economic benefits, including fewer and less severe crashes, reduced congestion, lower fuel consumption, and increased mobility for older adults and people with disabilities. Connected vehicle technologies also provide new opportunities to integrate features and services that support drivers and provide added convenience for all vehicle occupants.

Many of the connected and automated vehicle technologies and services available today, as well as many under development, rely on information obtained from a variety of vehicle systems. In some cases, data collected may include information about a vehicle's location or how a vehicle is being used. Recognizing that issues around how data is collected, used, and/or made available to third parties are complex, automakers have prioritized efforts to meaningfully address specific concerns and expectations around privacy in order to build trust with consumers around these technologies. That is why over six years ago, 20 members of our organizations took proactive steps to demonstrate their long-held commitment to protecting consumer privacy.

In November 2014, the Alliance of Automobile Manufacturers and the Association of Global Automakers issued the Privacy Principles for Vehicle Technologies and Services ("Principles").[1] The Principles provide a set of privacy fundamentals that Participating Members commit to when offering innovative vehicle technologies and services. Specifically, the Principles apply to the collection, use, and sharing of Covered 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. The Covered Information, under the Principles, includes identifiable electronic information that vehicles collect, generate, record, or store, that is

[1] https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf

retrieved from the vehicle by or on behalf of the automaker, as well as personal subscription information provided by individuals subscribing to or registering for vehicle technologies and services. Geolocation information, biometrics, and driver behavior information are subject to heightened notice and receive additional protections under the Principles, including the requirement to obtain affirmative consent prior to using such information for marketing purposes or disclosing it to unaffiliated third parties for their own purposes.

Built on the Fair Information Practice Principles (FIPPs), Federal Trade Commission guidance, and other recognized privacy frameworks, the Principles are intentionally flexible, so Participating Members may implement the Principles in different ways, allowing for differences in technologies and other distinguishing or company-specific factors. Importantly, the Principles act as a floor, not a ceiling, for privacy practices. 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.

- 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.

The Principles went into effect in 2016 with full implementation required no later than vehicle Model Year 2018. There are 20 Participating Members representing 99.7 percent of car and light duty truck sales in the United States.[2] All Participating Members are subject to enforcement by the Federal Trade Commission (FTC) under its Section 5 authority for unfair and deceptive business practices if they fail to live up to the commitments made in the Principles. Former FTC Commissioners have commented positively in public forums acknowledging the voluntary commitments of the industry towards customer privacy.[3]

In an era of rapid innovation, both within the auto industry and across society, it is important to maintain the trust of consumers and society without stifling the pace of technological advancement. The Alliance for Automotive Innovation recognizes this is a difficult balance. As demonstrated by our adoption of the Principles six years ago, however, we believe it is the right approach to consumer privacy. We and our members remain steadfast in this commitment, especially as vehicle data becomes increasingly relevant to the transportation ecosystem and other stakeholders. We understand and respect the potential opportunities vehicle data may present in our increasingly connected economy and society, but we also recognize our responsibility to put safeguards in place to protect consumer privacy and safety.

The Honorable Doris Matsui (D-CA)

1. When the Alliance for Automotive Innovation was announced in January, you told the press "we don't have a position or a stake in the litigation related to preemption and waivers."

    a. Is that still true?

    Yes.

    b. Does the Alliance intend to participate in the ongoing litigation between the Trump Administration and the State of California over the "One National Program" rule, also known as Part One of the so-called SAFE Vehicles Rule?

    No.

    c. Does the Alliance intend to participate in litigation associated with Part Two, when and if it is finalized?

    Auto Innovators is still reviewing the rule, and we are not in a position at this time to make any commitments concerning whether or not the association will

[2] Full list of Participating Members is available at https://autoalliance.org/connected-cars/automotive-privacy/participating-members/
[3] See, e.g. https://www.hldataprotection.com/2014/11/articles/consumer-privacy/automakers-commit-to-protecting-driver-data/

be participating in any litigation association with the SAFE Part Two rule, and if so in what capacity.

2. Does the Alliance consider tailpipe emissions to be within the scope of a vehicle's design, construction, and performance?

   A motor vehicle's emissions are inherently tied to the vehicle's design and construction, and is an aspect of its "performance." However, we do not view a vehicle's emissions performance to fall within the scope of the preemption provision of the House-passed SELF DRIVE Act, which was focused on the design and performance of highly automated vehicles and automated driving systems.

3. Does the Alliance support preempting State authority over autonomous vehicle design, construction, and performance?

   Auto Innovators supports a unified national approach to the design, construction, and performance of highly automated vehicles and automated driving systems. The United States has long recognized that automobiles are sold in a national market, and that automakers' success rests on the ability to manufacture vehicles that can be sold and operated in all fifty states. We therefore support continued efforts by Congress and the Administration to ensure that there is a consistent national approach to automated vehicle policy, and to clarify the respective roles of federal, state and local governments.

4. Please identify the members of the Alliance for Automotive Innovation

   American Honda Motor Co., Inc.
   APTIV PLC
   Aston Martin Lagonda of North America, Inc.
   BMW of North America, LLC
   BYTON North America Corporation
   Denso International America, Inc.
   FCA US LLC
   Ferrari North America, Inc.
   Ford Motor Company
   General Motors Company
   GM Cruise LLC
   Harman International, Inc.
   Hyundai Motor America
   Intel Corporation
   Isuzu Motors America, LLC
   Jaguar Land Rover North America, LLC
   Karma Automotive, LLC
   Kia Motors America, Inc.
   LM Industry Group, Inc.
   Maserati North America, Inc.

Mazda North American Operations
McLaren Automotive, Ltd.
Mercedes-Benz USA, LLC
Mitsubishi Motors North America, Inc.
Nissan North America, Inc.
NXP Semiconductors USA, Inc.
Panasonic Corporation of North America
Porsche Cars North America, Inc.
PSA North America Inc.
Recreation Vehicle Industry Association
Robert Bosch GmbH
Sirius XM Radio, Inc.
Subaru of America, Inc.
Suzuki Motor of America, Inc.
Texas Instruments Incorporated
Toyota Motor North America, Inc.
Volkswagen Group of America, Inc.
Volvo Car USA, LLC

5. Is the Alliance for Automotive Innovation a member of the Coalition for Sustainable Automotive Regulation?

   No.

6. Please identify the members of the Coalition for Sustainable Automotive Regulation.

   According to court filings, the Coalition for Sustainable Automotive Regulation's members consist of FCA US LLC, General Motors LLC, Mazda Motor of America d/b/a Mazda North American Operations, Mitsubishi Motors North America, Toyota Motor North America, Inc., the Automotive Regulatory Council, Inc., and the National Automobile Dealers Association.

7. What are the Coalition's funding sources? Who is financially supporting the Coalition's participation in the litigation regarding the "One National Program" rule?

   Given that the Alliance for Automotive Innovation is not a member of the Coalition for Sustainable Automotive Regulation, we are not in a position to provide a response to this question.

8. In your written testimony, you stated that "the Alliance for Automotive Innovation was formed to become the singular, authoritative and respected voice of the automotive industry in the United States." Given the ongoing role of the Coalition for Sustainable Automotive Regulation does the Alliance coordinate with or support the Coalition in any way?

The Alliance for Automotive Innovation has not coordinated with the Coalition for Sustainable Regulation in any way.

The Honorable Tony Cardenas (D-CA)

1. What new job opportunities will come from AV manufacturing and deployment?

   We anticipate that there will be new job opportunities that emerge with the manufacturing and deployment of AVs. For example, compared to conventional vehicles, AVs will be equipped with a greater number of sensors and artificial intelligence (AI)-based algorithms to translate raw sensor data into actionable information for the automated driving system (ADS). Thus, the design of such vehicles will require engineers and computer scientists with an understanding of AI and sensors, such as LIDAR, RADAR, ultrasonic and cameras. In addition, during the manufacturing process, trained employees will be required to install the sensors onto the vehicle.

   It is expected that, at least initially, AVs will commonly be operated as part of a fleet. In these cases, fleet operators may be required to oversee the operation of the vehicles and in some cases, provide remote input to the vehicles to assist in the case an emergency. Additionally, as with vehicle fleets today, employees will be required to provide vehicle maintenance and cleaning.

2. How will impacts to existing occupations vary depending on levels of automation?

   We anticipate that there will be varying impacts depending on levels of automation. For example, a Level 3 vehicle may require a human driver to be prepared to take back control of the driving task and a Level 4 vehicle may require a human driver to drive the vehicle outside of the Operational Design Domain (e.g. autonomous operation on highways but human-driven once the vehicle exits the highway and moves to surface roads).

   A recent workforce study by SAFE ("America's Workforce and the Self-Driving Future") projected that the economic benefits of AVs will greatly outweigh any initial job loss due to the increase to productivity, safety and energy efficiency as a result of AV deployment.

3. What occupational barriers must workers overcome to transition successfully to new AV jobs/occupations?

   There should be an emphasis for STEM education, including physics, engineering and computer science. Additionally, training may be required for manufacturing plant workers who will be required to install advanced vehicle sensors.

The Honorable Michael C. Burgess, M.D. (R-TX)

1. Mr. Bozzella, last Congress, Mr. Costello and Ms. Dingell introduced H.R. 3411, a bill to establish an Automated Driving System Cybersecurity Advisory Council to make recommendations regarding cybersecurity for autonomous vehicles. While we are all concerned about ensuring strong cybersecurity protections, if government sets standardized cyber processes, we may end up federally mandating cyber vulnerabilities.

    a. What are your members and industry doing to address cyber concerns?

    Today, cybersecurity is a priority to every industry, including the automotive industry. Automakers understand the realities of a connected world, as well as customer concerns and expectations regarding vehicle security. That is why industry is working proactively to build in security and adopt practices designed to minimize the risk of cyber threats. In fact, the industry is in the final stages of a multi-year effort to develop the first joint, international standard between SAE International and ISO for vehicle cybersecurity, covering the entire lifecycle of the vehicle. An initial draft of this standard was released for comment on February 12 with the final standard estimated to be released later this year.

    That joint effort builds on what the industry has already done. For example, several years ago, the industry proactively created an Information Sharing and Analysis Center (ISAC) in partnership with DHS. The Auto-ISAC now includes more than 50 members and has developed cybersecurity best practices. In addition, in 2014 the industry established FTC-enforceable Privacy Principles, including a specific reference to data security.

    Even with a multi-layer defense against cyber threats, automakers must remain nimble and adaptive to keep pace with the rapid and dynamic evolution of cyber threats. Locking in what seems proactive now may not be so effective when the future demands another approach, which is why the processes, best practices, and standards being developed by automakers, standards bodies, and multi-sector industry partners are so important and reflect the dynamic nature of this emerging risk.

    NHTSA also has oversight and enforcement authority over automakers when it comes to vehicle cyber security matters including those which may pose unreasonable risks to motor vehicle safety.

2. Mr. Bozzella, as the co-chairman of the House Motorcycle Caucus, the safety of motorcyclists is especially important to me. Motorcycle deaths accounted for 14 percent of all motor vehicle crash deaths in 2018, more than double the number in 1997, and nearly two-thirds of all motorcycle deaths involved other vehicles. As passenger vehicles rely more on technology and become autonomous, there are concerns about what this will mean for the safety of motorcycle riders, bicyclists and other non-automobile highway users.

a. How are your members testing to assess how their vehicle advanced driver assistance systems (ADAS) technology interact specifically with motorcycles?

Vehicle manufacturers develop ADAS technologies to rigorous safety and performance specifications which result in the deployment of systems that help improve the safety of the human driver and other road users when used as intended.

In the development of ADAS systems, manufacturers employ a combination of virtual testing (computer simulation) as well as confirmatory track testing to cover a wide range of potential real-world conflict scenarios with other road users including motorcycles.

With each generation of ADAS systems, the object detection and classification capabilities continuously improve, and many of today's Forward Collision Warning, Blind Spot Warning, and Automatic Emergency Braking Systems are designed with the detection of motorcycles in mind.

In addition, Auto Innovators shares some of its members with the Safer Motorcycling Research Consortium (SMRC), whose mission is to "develop strategies to advance and integrate on-road motorcyclist safety through data driven approaches and collaboration with relevant stakeholders." As part of the SMRC's efforts, it has been encouraging NHTSA to conduct research specifically targeted at assessing ADAS effectiveness with respect to motorcycles. In November of last year, NHTSA announced that they were moving forward with a research project to:

- Develop test metrics & procedures to evaluate the ability of light vehicle ADAS technologies to detect, perceive and react to motorcycles
- Assess motorcycle target requirements
- Comparatively assess corresponding Euro NCAP test procedures
- Comparatively test ADAS performance against motorcycles and light vehicles
- Emphasize scenarios/conditions that challenge ADAS capabilities in responding to motorcycles

[NHTSA Docket ID NHTSA-2019-0083-0008]

The SMRC and its shared members with the Auto Innovators look forward to the outcomes of this ADAS research and to additional research in the area of motorcycle safety.

b. Do motorcyclists and other non-automobile roadway users, like cyclists and pedestrians, create unique challenges for this developing technology?

By their very nature, motorcycles and other non-automobile roadway users are less conspicuous than typical passenger cars and light duty trucks. For this reason, human drivers often have difficulty identifying and predicting their presence and intentions. Similar challenges are also present for ADAS systems. Specifically, motorcycles and other Vulnerable Road Users (VRUs) present a physically smaller optical profile as

well as a smaller radar signature. As cameras and radars represent the bulk of ADAS sensors used to detect VRUs, there is a challenge in accurately detecting this population while simultaneously avoiding creating false positives, which present a similar but opposing challenge with sensor perception. However, as ADAS sensors and the associated object detection and classification software capabilities are rapidly improving, further increases in the safety benefit of these systems can be expected for all road users.

c. How will autonomous driving systems (ADS) characterize and operate around motorcyclists and bicycle riders?

Automated driving systems are developed and deployed with specific operating limits characterized by their operational design domain (ODD). Specifically, automated systems are designed to only operate in conditions where adequate levels of safety performance can be assured for road and environmental conditions and other road users that are within the system's ODD. Thus, systems that have ODDs that include exposure to motorcycles, pedal-cyclists, and pedestrians will be equipped with sensors and classification software that can appropriately detect and classify such road users in a manner that will permit safe operation in their presence. Any ADS deployed into the market will have been thoroughly validated through extensive testing, both virtual and physical, to ensure appropriate Object and Event Detection and Response (OEDR) for such VRUs.