ALLIANCE FOR AUTOMOTIVE INNOVATION

June 3, 2020

The Honorable Frank Pallone
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Greg Walden
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, DC 20515

Chairman Pallone and Ranking Member Walden:

On behalf of the Alliance for Automotive Innovation (Auto Innovators), I write to make you aware and seek your assistance to help protect the motoring public regarding the risk of significant motor vehicle safety and cybersecurity vulnerabilities that are being threatened by state-level action. Simply put, Auto Innovators and our members are calling for Congress to reaffirm existing statutory authority and enforcement guidance from the U.S. Department of Transportation when it comes to addressing motor vehicle safety and cybersecurity risks – including misuse of vehicle data that could be used by stalkers to prey on their victims.

Unlike other challenges that the auto sector faces due to the COVID-19 public health emergency, these safety, cybersecurity, and privacy threats facing the traveling public are preventable. However, a ballot initiative being pushed by outside parties in the Commonwealth of Massachusetts would force motor vehicle manufacturers to allow outside parties to be granted real-time, bi-directional access to vehicle data, including a consumer's driving data. This effort is being pursued despite the lack of traction at the state legislative level and has been defeated or failed to gain traction in Rhode Island and California.

This controversial initiative, which is expected to be on the ballot in November, is not just about getting data from a vehicle; it is about mandating real-time, two-way access. Proponents of the initiative not only want to receive data from a vehicle, but also want to be able to send data, including software, to uniquely designed critical vehicle systems – even while a car, or tractor trailer, is driving down the roadway. Not only does this initiative pose cybersecurity, personal safety, and privacy risks to the owner of the vehicle, but it also endangers others on the nation's roadways.

The ballot initiative has been disingenuously presented to voters as a solution for fixing cars. However, this initiative is really about third parties seeking bi-directional remote access to a consumer's driving habits, patterns, and location in real-time. Such a far-reaching mandate risks making personal data readily available to third parties and creates absolutely no safeguards for how consumer information is stored, protected, or used afterwards. Simply put, while manufacturers remain committed to allowing consumers to decide where to take their vehicle for repair and maintenance needs, there is no scenario in which real-time, remote access by third parties would be necessary to diagnose or repair a vehicle.

Each year, automakers spend millions of dollars to take the steps needed to protect consumer information. However, if the Massachusetts ballot initiative passes, third parties will have real-time, bi-directional remote access to consumer driving data and vehicle systems. In fact, the ballot initiative stipulates that, as of January 2021 (Model Year 2022), no vehicles with an operational telematics system in Massachusetts can be sold unless they conform to the bi-directional data access requirement.

Attached you will find a background document that explains the direct conflict between the Massachusetts ballot initiative and both the traditional federal authorities pursuant to the Motor Vehicle Safety Act and the well-established enforcement guidance from the U.S. Department of Transportation that outline steps that automakers are expected to make when it comes to reducing or eliminating vehicle safety or cybersecurity vulnerabilities.

Due to the unique conflicts that automakers are faced with, Congress should act to reaffirm NHTSA's statutory authority and enforcement guidance to protect the motoring public by temporarily establishing a limited five-year preemption regarding access to telematics data that could compromise vehicle safety due to actions at the state level. A five-year preemption provision would enable Congress and NHTSA to work on a longer term solution to ensure that new cybersecurity, privacy and public safety risks are not created.

With your key role on a Committee of jurisdiction, we look forward to following up with you in the coming weeks to schedule a meeting to explain the risks that the traveling public faces under this proposed ballot initiative. With your help, we trust that Congress can affirm the traditional responsibilities that automakers have when it comes to reducing or eliminating such risks.

Sincerely,

David Schwietert
Chief Policy Officer

Cc: All Members of the Committee on Energy and Commerce

Enclosure

About the Alliance for Automotive Innovation

Formed in 2020, the Alliance for Automotive Innovation is the singular, authoritative and respected voice of the automotive industry. Focused on creating a safe and transformative path for sustainable industry growth, the Alliance for Automotive Innovation represents the manufacturers producing nearly 99 percent of cars and light trucks sold in the U.S. The newly established organization, a combination of Global Automakers and Alliance of Automobile Manufacturers, is directly involved in regulatory and policy matters impacting the light-duty vehicle market across the country. Members include U.S. operations of international motor vehicle manufacturers, original equipment suppliers, technology and other automotive-related companies and trade associations. The Alliance for Automotive Innovation is headquartered in Washington, DC, with offices in Detroit, MI and Sacramento, CA.

THE CASE FOR FEDERAL PREEMPTION OF STATE LAWS MANDATING OPEN ACCESS TO VEHICLE SOFTWARE

In a 2015 Report to Congress, NHTSA identified the emerging challenges presented by the increased use of electronics and software to control critical functions in motor vehicles.[1] NHTSA noted:

> "In addition to the challenges regarding electronic components and their ability to function reliably in spite of their complex interactions, NHTSA believes there could also be increasing challenges with regard to the ability of these systems to remain free of unauthorized access or malicious attacks."

The Report noted that there were no automotive-specific cybersecurity standards at the time when the Report was written, but that there were important lessons to be learned from the cybersecurity experience of other industries. The first category identified by NHTSA for priority review was "to harden the design of automotive electronic systems and networks such that it would be difficult for malicious attacks to take place in newer generation systems."[2]

NHTSA identified possible entry points for malicious software on the vehicle, such as the On-Board Diagnostic (OBD)-II port, Universal Serial Bus (USB) ports, CD/DVD players; short range wireless interfaces, such as Bluetooth, Wi-Fi, or Dedicated Short Range Communications (DSRC); and long-range wireless interfaces such as cellular or satellite-based connectivity to the vehicle.[3]

The Report identified several potential solutions to these vulnerabilities, most of which involved strict limits and controls over access to these physical interfaces.

In 2016, NHTSA explicitly warned that software installed in motor vehicles presents unique safety risks, because software often interacts with a motor vehicle's critical control functions, such as braking, steering or acceleration.[4] NHTSA raised particular concerns about the fact that those critical control functions can be substantially altered by after-market updates. The agency cautioned:

> "… [I]f software (whether or not it purports to have a safety-related purpose) creates or introduces an unreasonable safety risk to motor vehicle systems, then that safety risk constitutes a defect compelling a recall."[5]

NHTSA instructed vehicle manufacturers to take steps to mitigate the risks of foreseeable software failures, and pledged to use the full array of enforcement authorities available to the agency to ensure that manufacturers step up to this responsibility.

Shortly thereafter, NHTSA published a report recommending best practices for protecting against cybersecurity risks to safe motor vehicle operation, which compliments the work of the Auto ISAC.[6] First among

---

[1] NHTSA. (2015, December). Electronic systems performance in passenger motor vehicles: Report to Congress.
[2] Id. at 18.
[3] Id.
[4] NHTSA Enforcement Guidance Bulletin 2016–02: Safety-Related Defects and Automated Safety Technologies, 81 Fed. Reg. 65705, 65709 (September 23, 2016)
[5] Id.
[6] National Highway Traffic Safety Administration. (October, 2016). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333).

several recommendations was to take explicit steps to design vehicle systems to be free of unreasonable risks from potential cybersecurity threats and vulnerabilities through the entire life-cycle of the vehicle.

Under the category of "Fundamental Vehicle Cybersecurity Protections," the first recommended practice is to limit access to Electronic Control Units (ECUs) in vehicles to authorized privileged users.[7] With respect to the need to access ECUs and other vehicle systems for diagnostic purposes, NHTSA cautioned:

> "Diagnostic features should be limited as much as possible to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature. **Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they are misused or abused outside of their intended purposes.**"[8] (emphasis added)

Additional recommendations were to limit the ability for a third party to modify firmware,[9] to limit access to network servers through vehicle ports,[10] use segmentation and isolation techniques in vehicle architecture design to control pathways to critical systems,[11] and to control internal vehicle communications about critical safety messages to deter interfacing between insecure aftermarket devices and vehicle networks.[12]

With respect to serviceability, NHTSA noted the need for third party repair services to be able to have access to certain vehicle systems to provide service, but cautioned that such access must be balanced with strong cybersecurity protections to ensure public safety.[13]

In the context of the rapidly emerging market for automated driving systems in vehicles, which are particularly vulnerable to cybersecurity risks, NHTSA addressed the need for designing components to minimize safety risks from cybersecurity threats and vulnerabilities.[14] A year later, the Department of Transportation reiterated that it is the responsibility of vehicle manufacturers and other stakeholders to manage cyber risks in designing automated driving systems in vehicles.[15] **More recently, DOT announced that NHTSA is conducting research to promote a layered approach to cybersecurity by focusing on a vehicle's entry points, both wireless and wired, which could be potentially vulnerable to a cyber-attack, in anticipation of updating its 2016 Cybersecurity best practices**.[16]

Against these strong warnings from NHTSA, the State of Massachusetts will have an initiative on the ballot in November 2020 to require auto manufacturers to grant third parties ***bidirectional access*** to vehicle systems in real-time, even when the vehicle is being driven. This means that a third party could not only download information from a vehicle (which is already permitted), but could also upload unauthorized information, including software, into the vehicle that could compromise the safety of critical systems such as braking, steering and acceleration. This initiative , which would take effect in January 2021, extends beyond light duty vehicles to include tractor-trailers and other heavy-duty vehicles, will jeopardize the safety and the security of the motoring public and those who share the street with motor vehicles, including pedestrians, bicyclists and other micromobility riders.

---

[7] Id. at 17.
[8] Id. at 17.
[9] Id. at 18.
[10] Id. at 19.
[11] Id. at 19.
[12] Id. at 19.
[13] Id. at 21.
[14] Automated Driving Systems 2.0: A Vision for Safety (September 2017)(Report No. DOT HS 812 442) at 11.
[15] Automated Vehicles 3.0: Preparing for the Future of Transportation (October 2018) at 32.
[16] Automated Vehicles 4.0: Ensuring American Leadership in Automated Vehicle Technologies (January 2020) at 18.

If this initiative is enacted into law, auto manufacturers will be placed in the dilemma of redesigning vehicles in a manner that is contrary to all of the NHTSA guidance summarized above. NHTSA's guidance is not simply a set of suggestions; it is an explanation of NHTSA's view of the industry's legal obligations under the National Traffic and Motor Vehicle Safety Act, as described prominently in the first paragraph of the *Cybersecurity Best Practices* guidance document.[17]

NHTSA has shown that it has adequate tools through its safety defect authority to protect the public against unreasonable cybersecurity risks, and it will not hesitate to use those tools. However, the Massachusetts initiative threatens the policies that NHTSA has established and expands the likelihood of consumer harm from cyber-attacks.

If NHTSA had established these policies through a Federal Motor Vehicle Safety Standard (FMVSS), the Massachusetts initiative would be preempted by federal law. The federal policies informed by Vehicle Safety Act authorities should enjoy no less protection from State law conflicts, simply because the agency chose to announce them through an enforcement policy and guidance versus an FMVSS that would be rigid and unable to keep pace with technological changes and security vulnerabilities.

Congress should act to reaffirm NHTSA's authority and protect the safety of the motoring public by temporarily establishing preemption in this limited circumstance for five years. NHTSA is expected to complete the updating of its Cybersecurity Best Practices later this year. In that context, NHTSA could evaluate the risks posed by the Massachusetts initiative and report to Congress on potential resolutions of these risks through rulemaking or other actions. Effectively, the five year preemption provision would enable Congress and NHTSA to work on a longer term solution to ensure that new cybersecurity, privacy and public safety risks - including misuse of vehicle data that could be used by stalkers to prey on their victims – are not created.

[17] National Highway Traffic Safety Administration. (October, 2016). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333) at page 5.