# Comments of the

# Ad-Hoc HAV Data Access Coalition

# To the

# U.S. Department of Transportation

# Federal Moto Carrier Safety Administration's

# "Request for Comments Concerning Federal Motor Carrier Safety Regulations (FMCSRs) Which May Be A Barrier to the Safe Testing and Deployment of Automated Driving Systems-Equipped Commercial Motor Vehicles on Public Roads"

# Docket No. FMCSA-2018-0037

May 10, 2018

(83 Fed. Reg. 12933 (March 26, 2018))

The Ad-Hoc HAV Data Access Coalition ("Coalition") is pleased to respond to the Federal Motor Carrier Safety Administration's ("FMCSA") "Request for Comments Concerning Federal Motor Carrier Safety Regulations (FMCSRs) Which May Be A Barrier to the Safe Testing and Deployment of Automated Driving Systems-Equipped Commercial Motor Vehicles on Public Roads."

The Coalition is a voluntary group of diverse stakeholders – consumer protection and privacy advocates, vehicle fleet owners (both light- and heavy-duty), vehicle

equipment suppliers and repair facilities, insurance companies and others – united by our common belief that vehicle owners control access to, and the use of, the personal information and vehicle data generated and stored by all motor vehicles.

As we collectively move towards the deployment of more automated driving system-equipped vehicles – both light- and heavy-duty – in the coming years and decades, this issue of data access and control by vehicle owners and other parties will of necessity become more important. And this issue of data access and control takes on even greater importance when the automated driving system-equipped vehicles involved are larger commercial motor vehicles ("CMVs"). The Coalition welcomes this opportunity to provide input to FMCSA on these important issues and looks to working with Department of Transportation Secretary Chao and the leadership of FMCSA in the coming months and years on automated driving system-equipped vehicle data access issues.

There are three key issues with respect to data access involving automated driving system-equipped CMVs that the Coalition urges FMCSA to address actively as it considers regulatory changes or updates: (1) communication and interoperability; (2) safety; and, (3) cybersecurity.

First, with respect to communication and interoperability, all vehicles are undergoing revolutionary changes with respect to how they communicate with other vehicles on the road, with the transportation environment surrounding them, and with vehicle owners and their representatives, drivers and passengers both inside the vehicle and at a remote location. The Coalition's focus is on access to, and control of, the data being generated and stored by, and transmitted from, the automated driving system-equipped CMV. However, without interoperability, that access and

control will not be meaningful; seamless communication between vehicles, infrastructure and the overall transportation environment (including governmental oversight and regulation) are essential. Given the very nature of the CMVs, the communication and interoperability of vehicle data, as well as the access to and control of that data, are a core consideration for federal regulators.

The Coalition strongly supports maintaining the current uniform regulatory construct that the owners of motor vehicles, as well as parties to whom the owners give informed and advance permission, control access to the data generated and stored by automated driving system-equipped CMVs. This communication can relate to the location of the CMV, the cargo transported, the operation of the vehicle, the weather at the vehicle's current location or along its planned route, and numerous other interactions between the vehicle, its driver and/or passengers, and individuals at remote locations (dispatchers, logistics and safety experts, first responders, and customers). All of these individuals need real-time and accurate communication with all vehicles operating in an autonomous mode, particularly if those vehicles are CMVs.

Second, with respect to safety, the Coalition anticipates that data on CMV cargos will be communicated increasingly through data and the airwaves, rather than through placarding and manifests. As a result, first responders and law enforcement will be able – and must be able -- to access real-time, accurate and detailed information about a cargo electronically. Such real-time data exchange could well save lives and limit property damage in the event of an incident or an accident – underscoring the importance of real-time data access by vehicle owners and other authorized parties. Again, maintaining data access and control by vehicle owners – who have the accurate information on the freight being transported – and their

authorized third parties – is vital to assuring real-time responses to incidents to avoid safety risks.

Third, cybersecurity has become a focus of automated driving system-equipped CMVs, including the potential for hackers to disrupt communications between vehicles or take over control of a CMV. Some stakeholders have gone so far as to assert that the sole method of addressing cybersecurity concerns in automated driving system-equipped CMVs is to shut down or limit access to the data generated by a motor vehicle for anyone other than the manufacturer of the vehicle.

The Coalition strongly disagrees with this position assertion and asserts that basic cybersecurity tenants support that proprietary and closed data systems are actually the most vulnerable to catastrophic failures. Accordingly, the Coalition urges FMCSA to resist the adoption of such an approach to automated driving system-equipped CMV cybersecurity and data access. The Coalition suggests that FMCSA promote a regulatory framework that insures that vehicle data access is: (1) open, secure, and neutral; (2) protected against hacking through recognized principles of data security by design; and, (3) accessible without charge to the vehicle owner and, should the vehicle owner provide informed advance consent, to authorized third parties.

Congress has signaled its interest in the autonomous vehicle data access and control issue through its unanimous adoption of a bi-partisan autonomous vehicle data access amendment to the Senate autonomous vehicle bill. This data access amendment, sponsored by Senators Inhofe (R-OK) and Baldwin (D-WI), would create a data access advisory committee comprised of a wide spectrum of stakeholders, including the Department of Transportation and the National Highway

Traffic Safety Administration. The Inhofe/Baldwin Amendment was adopted by the Senate Commerce Committee unanimously in October 2017 and its inclusion of all legitimate stakeholders with an interest in autonomous vehicle data access should form the foundation for all future discussions of data access and control of vehicle and personal data by vehicle owners – whether by PHMSA or other federal agencies. The Inhofe/Baldwin Amendment does not apply to CMVs over 10,000 gross vehicle weight, but there is no reason to anticipate that Congress would adopt a different set of data control and access standards for heavy-duty vehicles than would be applied to light-duty vehicles.

Thank you for the opportunity to provide these comments from the Ad-Hoc HAV Data Access Coalition. The Coalition looks forward to working with FMCSA and all stakeholders to address the issues of automated driving system-equipped CMV data access, vehicle owner data control rights, and cybersecurity in the near future.

If the members of the Coalition can be of assistance to FMCSA, please do not hesitate to contact me at 202-297-5123 or at gscott@merevir.com.

**MEMBERS OF THE AD-HOC HAV DATA ACCESS COALITION**

American Automotive Leasing Association
American Bus Association
American Car Rental Association
Auto Care Association
Automotive Service Association
Consumer Action

NAFA Fleet Management Association

National League of Cities

National Motor Freight Traffic Association

Property Casualty Insurers Association of America

Geotab, Inc.

Jack Cooper Logistics, LLC

Safelite Group, Inc.