Comments of the
U.S. HAV Data Access Coalition
To the
Subcommittee on Communications and Technology
Of the
House Committee on Energy and Commerce
Hearing on
"Protecting Consumer Proprietary Network Information in the Internet Age"

July 11, 2018

Good morning, Chairman Blackburn, Ranking Member Doyle, and Members of the Communications and Technology Subcommittee. The U.S. HAV Data Access Coalition ("Coalition") is pleased to present this statement to the Subcommittee with respect to your hearing on "Protecting Consumer Proprietary Network Information in the Internet Age." The Coalition respectfully asks that this statement be made a part of the official record of this hearing.

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, telematics and fleet management companies, insurers and others – united by our common belief that vehicle owners must control access to, and the use of, the personal information and vehicle data generated and stored by the motor vehicles they own.

As we collectively move towards the deployment of more connected and automated driving system-equipped vehicles – both light- and heavy-duty – in the coming

years, the importance of data access and control by vehicle owners, and other parties, will only increase. The Coalition commends the Subcommittee for calling this hearing and urges its members to focus your collective attention on the issue of data access as you consider broader policy issues of protecting consumer proprietary information in the internet age.

There are three key issues with respect to data access involving connected and automated driving system-equipped motor vehicles that the Coalition urges the Subcommittee to address: (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 remote locations. The Coalition's focus is on access to, and control of, the data being generated by, and transmitted from, connected and automated driving system-equipped motor vehicles. 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 motor vehicles, the communication and interoperability of vehicle data, as well as the access to and control of that data, are a core consideration for federal legislators and regulators.

The Coalition strongly supports guaranteeing that the rights of motor vehicle owners are not eroded through the introduction of new technologies. Owners of motor

vehicles, as well as parties to whom the owners give informed and advance permission, must control access to the data generated and stored by connected and automated driving system-equipped motor vehicles. This data can relate to the location of the vehicle, 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 a connected and/or autonomous mode.

Second, with respect to safety, the Coalition anticipates that data on the freight, cargos and packages being transported by commercial motor vehicles – particularly medium- and heavy-duty trucks -- 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 vehicle's cargo electronically. Such real-time data exchange could save lives and limit property damage in the event of an incident or an accident as well as actually preventing incidents and accidents – 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 connected and automated driving system-equipped motor vehicles, including the potential for hackers to disrupt communications between vehicles or take over control of a vehicle. Some

stakeholders have gone so far as to assert that the sole method of addressing cybersecurity concerns in connected and automated driving system-equipped motor vehicles 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 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 legislators and regulators to resist the adoption of such an approach to connected and automated driving system-equipped motor vehicle cybersecurity and data access. The Coalition suggests that legislators and regulators promote a policy 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 connected and 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 connected and 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 the

Subcommittee, by the full Committee, by other congressional committees, or by federal vehicle, consumer protection and privacy regulators.

Thank you for the opportunity to provide these comments from the U.S. HAV Data Access Coalition. The Coalition looks forward to working with the members of this Subcommittee and all stakeholders to address the issues of connected and automated driving system-equipped motor vehicle data access, vehicle owner data control rights, and cybersecurity in the near future.

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

MEMBERS OF THE U.S. HAV DATA ACCESS COALITION

American Automotive Leasing Association
American Bus Association
American Car Rental Association
Auto Care Association
Automotive Service Association
Coalition for Smarter Transportation
Consumer Action
NAFA Fleet Management Association
National Consumers League
National League of Cities
National Motor Freight Traffic Association
Owner Operator Independent Drivers Association
Property and Casualty Insurers Association of America

Geotab, Inc.
Recall Masters, Inc.