NAFA®
Fleet Management Association

Fleet Solutions
for Fleet Professionals

June 22, 2017

Office of the Secretary
Federal Trade Commission
Suite CC-5610 (Annex A)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Connected Cars Workshop P175403

Dear Secretary:

NAFA Fleet Management Association (NAFA) submits the following comments in response to the Notice seeking comments on the FTC/NHTSA Connected Cars Workshop scheduled for June 28, 2017.

NAFA is the association for professionals who manage fleets of sedans, public safety vehicles, trucks, and buses of all types and sizes, and a wide range of military and off-road equipment. NAFA's members are responsible for the specification, acquisition, maintenance, repair, fueling, risk management, and remarketing of more than 4.6 million vehicles that drive an estimated 50-billion miles each year. NAFA's members control assets and services well in excess of $100-billion each year.

A fleet vehicle may be an automobile driven by a pharmaceutical salesperson; a service vehicle, such as a cargo van, driven by a technician; or a pickup truck driven by a repair person. In many cases, the employer may permit a vehicle to be driven for personal as well as for business use, subject to applicable tax requirements.

While most of the connected vehicle discussion has focused on the consumer, the connected vehicle also provides promise and challenges for fleets – the companies, government agencies, utilities and educational institutions that own or lease vehicles to carry out their mission. As of January 1, 2016, there were 3 million cars and Class 1-5 trucks in commercial fleets, and 1.52 million cars and Class 1-5 trucks in government fleets.[1] [This data does not include rental or taxi vehicles.]

With vehicles becoming more and more dependent on technology, performance and convenience features, automakers are growing increasingly concerned with cyber hackers and vulnerabilities in their line-ups. These vulnerabilities present challenges for fleet management in being able to

[1] 51st Annual Fact Book Guide 2016-2017, Automotive Fleet

125 Village Boulevard, Suite 200 • Princeton Forrestal Village • Princeton, NJ 08540
Tel: (609) 720-0882 • Fax: (609) 452-8004 • www.nafa.org

continue utilizing new technology, while also ensuring that the fleet is protected from malicious or criminal activity. As vehicles become increasingly connected and autonomous, the security and integrity of automotive systems has become a high priority for fleet management.

Privacy

Today's vehicles collect personal information through in-car technologies. Sensitive information, such as geolocation and driver behavior information, merits heightened protections.

The driver of a vehicle has an expectation of privacy. Yet, there is an important distinction between the expectation for a driver of a consumer vehicle and the driver of a fleet vehicle. The driver of a fleet vehicle is responsible for the operation of an asset owned or leased by the employer, while the consumer is responsible for his or her own vehicle. There is a distinction between privacy expectations for the consumer and the privacy expectations for the driver of a fleet's asset.

Fleet managers should recommend that employers develop a policy governing the collection and use of driver behavior data, such as geolocation and vehicle operation information, speed and braking, and other aspects. The policy should be fully transparent and shared with the driver of the employer-provided vehicle.

The privacy policy should specify the types of information that will be collected, how such information will be used and stored, and under what circumstances the information can be retrieved. If personal use of the vehicle is permitted, the privacy policy should distinguish between privacy expectations for business and personal use.

Because driver behavior data may be discoverable in a court of law or subject to freedom of information requests in public fleet cases, the fleet manager should make the employer aware of the information collected and stored and advise the employer of the need to assess its tolerance for risk.

Because disclosure of vehicle specific information, such as geolocation, could impede the ability of certain government agencies to conduct necessary business, Federal and state laws and regulations should provide limitations on the access to and disclosure of such information for purposes of law enforcement, national security, and public health and safety.

Ownership and Collection of Data

The connected vehicle generates and transmits large amounts of data. The owner of the vehicle is the rightful owner of data generated and transmitted by the vehicle. In the case of a leased vehicle, collection, storage and use of data from the vehicle should be reflected in the lease agreement.

Some of this data is properly collected by OEMs to monitor operating history and vehicle performance. The OEM should have unrestricted access to information from the vehicle's operating system for warranty and safety purposes provided this is disclosed to the owner. Fleets

need to collaborate with the OEMs to determine what information is transmitted by the vehicles to the manufacturer and how that information is analyzed and stored.

The owner of the vehicle should opt-in before data can be transmitted and collected by the OEM. Exceptions regarding an opt-in requirement need to be allowed for safety and identified vehicle operation needs. NAFA will collaborate with the OEMs to develop a transparent list of exceptions.

Telematics

The technology of telematics will improve exponentially over the next several years. Public policy adopted today must be forward looking.

There is a need to clearly define that the information extracted from a vehicle's telematics system is the property of the vehicle owner and cannot be accessed, transmitted, collected or stored by others, including the vehicle manufacturer, without prior approval from the vehicle owner.

The vehicle manufacturer should clearly disclose to the owner and lessee the exact types of information capable of being transmitted and collected by the manufacturer from the vehicle's telematics system. Such information should be available as read only.

Vehicle manufacturers should build telematics systems with the capability to communicate data for fleet purposes using a standardized interface, such that the information can be directly transmitted, read, and used for fleet management.

Security

The on-board diagnostic (OBD) port was designed to collect emissions data, but is now used by fleets for telematics and vehicle diagnostics. For a fleet maintenance facility, access to the electronic control module of the vehicle is needed for both diagnostics and repair. Aftermarket telematics devices that depend on access to the OBD port offer fleet managers a range of advantages, including safety, reduced cost of ownership, and environmental protection. Fleet managers should have policies in place to ensure that only secure devices are connected to the port.

NAFA is eager to collaborate with vehicle manufacturers and other stakeholders on alternatives to the OBD II port, provided that such alternatives guarantee the same level of access to data for fleet management.

***

NAFA is ready to work with all stakeholders to develop the solutions needed to take advantage of connected vehicle technology while protecting the integrity of the vehicle. We appreciate your consideration and look forward to being a part of this important process. If you have any

questions, or need additional information, please feel free to contact me or Patrick O'Connor, NAFA's U.S. Legislative Counsel, at (703) 351-6222.

Sincerely,

Phillip E. Russo, CAE
Chief Executive Officer

125 Village Boulevard, Suite 200 • Princeton Forrestal Village • Princeton, NJ 08540
Tel: (609) 720-0882 • Fax: (609) 452-8004 • www.nafa.org