The Auto Care Association appreciates the opportunity to comment on the draft Guidelines issued by the European Data Protection Board entitled “Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications”.

Auto Care has three core values in regards to control and access to in-vehicle data:

- Vehicle owners/users should be clearly informed about the data being transmitted by their vehicle.
- Owners/users should have direct and secured access to that data.
- Owners/users should have the ability to control where that data is sent and how it is used.

As stated in item 4 of the Introduction to the Guidelines:

“Thus, the challenge is, for each stakeholder, to incorporate the protection of personal data dimension from the product design phase, and to ensure that car users enjoy transparency and control in relation to their data. Such an approach helps to strengthen user confidence, and thus the long-term development of those technologies.”

While cyber protections for vehicles are critical, it is imperative that these protections are not used by vehicle manufacturers in a way that mitigates the rights of car owners to be aware of data being generated by their vehicle or their ability to control access to their data. Auto Care strongly supports efforts by the European Commission to provide increasing transparency and real time control of data. In fact, Auto Care has worked in partnership with international and European standards organizations to create a standardized, secure design for vehicle data to be shared with third parties at the owner’s discretion that, if adopted by manufacturers, would provide for a secure and transparent framework for the control of vehicle data. This standards-based approach, known as the Secure Vehicle Interface (SVI), is a solution that provides security, privacy, consumer choice, safety and a level playing field for the marketplace. We have included these references in the following comments.

1.5.1 Lack of control and information asymmetry

It is critical that users have real time control of the data generated by their vehicle. Currently vehicle manufacturers are obtaining blanket permissions from new vehicle purchasers to collect data from vehicles. In many cases, the owner can opt out of permitting the manufacturer from sharing personally identifiable data with third parties, but they have no control of who the manufacturer choses to share that data with. Further, the owner is prevented from sharing their data with other third parties of their choice. In short, under the current vehicle data landscape, the owner/operator of a vehicle has virtually no control of the data generated by their vehicle and is reliant on the manufacturer of that vehicle for any access.

1.5.2 Quality of the user’s consent

As stated previously, the consent currently obtained from owners is extremely broad and provides little if no specifics as to what data will be shared, or how it will be shared. Further, since that consent occurs during the purchase of

that vehicle, there is no consent once the vehicle is on the road or if the vehicle is sold to a second or third owner. We agree with the comment under item 46 of the Guidelines that "Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car. Consent must be as easily withdrawn as it is given." It is important to note that as long as the manufacturer is the center of the data access environment, they will be able to determine the extent and terms of that access. This will mean limitations on competition and privacy.

1.5.3 Further processing of personal data

No comments.

1.5.4 Excessive data collection

We agree that there are an ever increasing number of sensors on connected vehicles and this does risk excessive data collection. However, there are industry standards that have been developed under C-ITS that could mitigate this scenario and provide the ability for owner/users to securely retain control of their data.

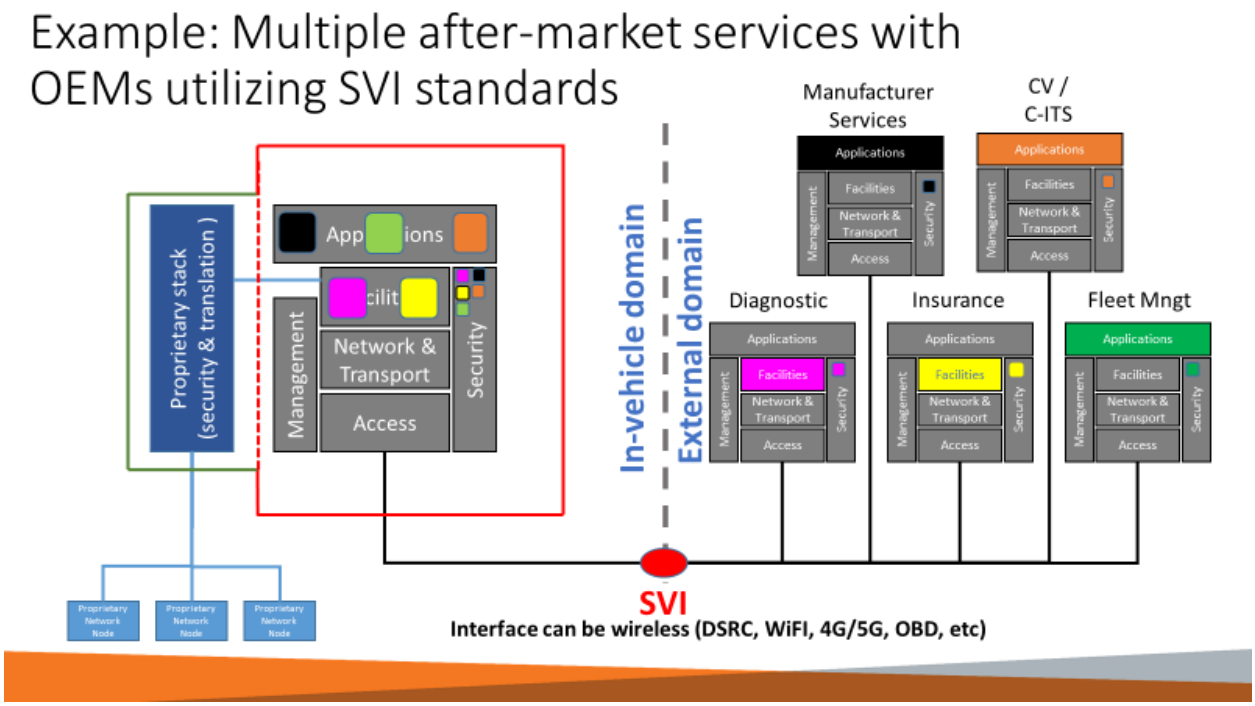
This collection of standards (ISO.EN 21184/ISO.EN 21185/ISO.EN 21177) is known as the Secure Vehicle Interface (SVI) and is intended to permit car owner/user control of data and to make a limited set of data available to third parties providing services to the vehicle owners. Through use of digital certificates that can be transmitted between trusted entities, there can be secure communications of specified data for specified use cases. Such action would extensively limit the availability of the collection of data not authorized by the vehicle owner and not needed by the entity collecting the data for a specified purpose.

Below is a brief description of the standards that comprise SVI:

- ISO.EN 21184 Cooperative intelligent transport systems — Global transport data management (GTDM) framework
- ISO.EN 21185 Intelligent transport systems — Communication profiles for secure connections between trusted devices
- ISO.EN 21177 Intelligent transport systems — ITS-station security services for secure session establishment and authentication between trusted devices.

1.5.5 Security of personal data

As illustrated below, the Secure Vehicle Interface (ISO.EN 21184/ISO.EN 21185/ISO.EN21177) provides a means for controlling what data is authorized for which use cases. Therefore, in the instance of a repair workshop, as referred to in item 57 of the Guidelines, digital certificates provided to a technician would only authorize access to the data needed to provide repair and maintenance services for the owner. Other data that could be either personal or security related would be protected from access through the use of digital certificates which limit data access and provide a means to track use of that data.



2 General Recommendations

2.1 Categories of data

While we do not have any comment on the categories discussed under this section, we should note that permitting the data to be available from the vehicle specified by use cases will minimize access to personal data where it is not necessary. For example, while an owner might want to activate the availability of location data on their vehicle if they need to be towed or in an emergency, using a certificate based system would prevent access to location data for entities that seek to provide services for a vehicle that do not require location access.

2.2 Purposes

We agree with this section.

2.3 Relevance and data minimisation

See comments under 2.1

2.4 Data protection by design and by default

Vehicle manufacturers should be required to design their vehicle in such a way as to prevent open and uncontrolled access to an owner's personal data. SVI, as previously described in these comments, would allow for data to be processed, locally, on-board the vehicle, such that only the data needed by a certain use case would be sent by the vehicle to the entity that has been directed by the owner to receive the data. The determination of what data is permitted to be sent for each use case should be collaborative between the manufacturers and entities that would use the data. However, it is critical that owner/user be provided with full control of where their data is being directed; and clear information from the entity receiving the data, as to what data is being used and for what length of time the data will be needed to complete the task.

2.5 Information

No comments

2.6 Rights of the data subject

We agree with this section that the owner/operator of the vehicle should have the ability to directly control access to their vehicle data in real time. The challenge in the motor vehicle space is that the owner or user of a vehicle is likely not the same person who purchases the vehicle from the manufacturer. Therefore, it is critical that control and authorization for the collection of data from a specific vehicle must be accomplished in real time and cannot simply be completed at the time of the purchase of a vehicle and should not be under the control of the manufacturer who has limited to no knowledge of the identity of either the owner or driver.

2.7 Security and confidentiality

While we are strong proponents of installing measures that guarantee the security and confidentiality of processed data and to prevent access by unauthorized persons, we are concerned that manufacturers will use this process to prevent, restrict or increase the difficulty of independent vehicle workshops needing access to vehicle data in order to provide repairs for owners and users of vehicles. Specifically, while access to a vehicle data should secured, it is critical that the access point not be controlled by the manufacturer. Instead, the EU is urged to establish an independent certificate authority to ensure that control and access to data is secure, but also that it remain competitive, permitting innovative services to be developed and for owner/operators of vehicles to determine who has access to specific data.

2.8 Transmitting personal data to third parties

No comments

2.9 Transfer of personal data outside the EU/EEA

No comments.

2.10 Use of in-vehicle Wi-Fi technologies

No comments

About the Auto Care Association

The Auto Care Association is the voice of the American independent repair and maintenance industry.

The 533,000 businesses in the United States (US) auto care industry form a network of independent manufacturers, distributors, repair shops, marketers and retailers small and large. At its core, this integrated grid of professionals is dedicated to providing the quality parts, products and vehicle service and repair for all 280 million cars and trucks on American roads today.

Several Auto Care Association members have operations across the globe, including in the European Union (EU). The Auto Care Association wishes to develop a positive and constructive dialogue with the EU institutions, especially considering Europe's leading role in shaping the future of the automotive industry at global level.