European Automobile Manufacturers Association

ACEA

ACEA Position Paper

Access to vehicle data for third-party services

December 2016

INTRODUCTION

Today's vehicles are increasingly 'connected' in the sense that they can exchange information wirelessly with the vehicle manufacturer, third-party service providers, users, infrastructure operators and other vehicles. This increases comfort and convenience for customers, improves products and services, and contributes towards achieving societal goals such as improving road safety, reducing fuel consumption, and facilitating traffic management and parking.

This development is generating increasing demands from third parties to access and use in-vehicle data. This paper presents the view of the European automobile manufacturers as to how such data access can occur for third-party services in a manner that strikes a fair balance between the legitimate market-driven needs of service providers, the interests of consumers and the need to protect their personal data and privacy, as well as the protection of road safety, security and intellectual property rights.

BASIC PRINCIPLES

Vehicle manufacturers are prepared to make vehicle generated data available for third-party services in a manner that ensures the protection of the vehicle user's personal data, does not endanger the safe and secure functioning of the vehicle and does not undermine the liability or intellectual property rights of the vehicle manufacturer. This implies:

- **Customer choice:** Vehicle users can obtain services from the vehicle manufacturer, his network of authorised repairers, independent aftermarket operators or any other service provider that has concluded a B2B agreement with the vehicle manufacturer.

- **Fair competition:** Repair and maintenance information that is made available to the vehicle manufacturer's network of authorised repairers will be made available to independent aftermarket operators on non-discriminatory conditions (type, amount and quality of data, delivery time, price) in accordance with EU law.

  Other service providers will have access to a defined dataset to offer their services in accordance with the B2B agreement concluded with the vehicle manufacturer.

- **Privacy and data protection:** In accordance with EU and national data protection and privacy laws, personal data of vehicle users will be made available to service providers only with the consent of the vehicle user except where a legal requirement or a contract exists. Service providers shall use this data only for the purpose(s) for which the vehicle user gave his or her consent.

- **Safety, security and liability:** With the exception of regulated access to data for emissions control, diagnosis, repair and maintenance, data access must occur only through off-board means since direct third-party access to vehicular electronic systems would jeopardise safety, (cyber)security and vehicle integrity. Having regard to the vehicle manufacturer's obligations under product liability law, the responsibility for ensuring secure end-to-end communication between the vehicle and the off-board facility must remain exclusively with him.

- **Interoperability:** The means of access and the interface(s) must be standardised to ensure interoperability. The ISO standard 20078 is being developed specifically for this purpose. It provides for web service access to the 'extended vehicle' as defined in ISO standard 20077-1. The extended vehicle consists of a physical road vehicle with external software and hardware extensions that are developed, implemented and managed by the vehicle manufacturer.

- **Return on investment:** Service providers who use vehicle data for commercial purposes shall compensate vehicle manufacturers for all costs incurred, for example in generating the data and in developing, operating and maintaining the access facility and, where appropriate, for the market value of the data.

AVAILABLE DATA

VEHICLE GENERATED DATA

The data that can be made available is 'vehicle generated data' or 'operating data'. It excludes data imported by vehicle users (eg mobile phone contact list, selected destinations for navigation) and data received from external sources (eg information transmitted by roadside units, other vehicles or vulnerable road users).

Vehicle generated data is created within vehicle control units and helps ensure the safe operation of the vehicle, checks its proper functioning, identifies and corrects errors and refines and optimises vehicle functions.

It also documents the system status for certain events (eg component malfunction, airbag deployment, stability control) and records the relevant information for the function (eg number of revolutions, acceleration, speed, air temperature, fuel level or brake pad wear). This operating data varies according to manufacturer, vehicle type and equipment.

This data can be used for a wide variety of purposes such as:

- Repair and maintenance
- Road safety and traffic management
- Fleet management
- Quality management and product development
- Non-automotive usage (eg insurance, car rental, car sharing)

USE CASE CATEGORIES AND DATA ACCESS CONDITIONS

Access to this 'vehicle generated data' or 'operating data' will be granted taking into account the type of use case (purpose for which it is used), the nature of the usage (public interest or commercial interest) and the type of data (personal or non-personal). On this basis, we distinguish the following use case categories:

- **Road safety**

Example: Local hazard warning.

As the availability of this data is in the public interest, vehicle manufacturers are prepared to make this data available in an anonymised manner to public authorities (or private operators entrusted with a public task such as road operators) on a reciprocal basis. Private operators using this data for a commercial purpose (developing apps, for example) can obtain this data on the basis of a B2B agreement with the vehicle manufacturer.

- **Cross-brand services**

Example: Road sign recognition, on-street parking.

This data will be made available on the basis of a B2B agreement.

- **Personalised services**

Example: 'Pay how you drive' insurance, electric vehicle infrastructure routing for charging (pay and charge).

Except where a legal requirement or a contract exists, personal data will be made available to service providers only with the consent of the vehicle user. Service providers shall use this data only for the purpose(s) for which the vehicle user gave his or her consent.

- **Brand-specific services/component monitoring**

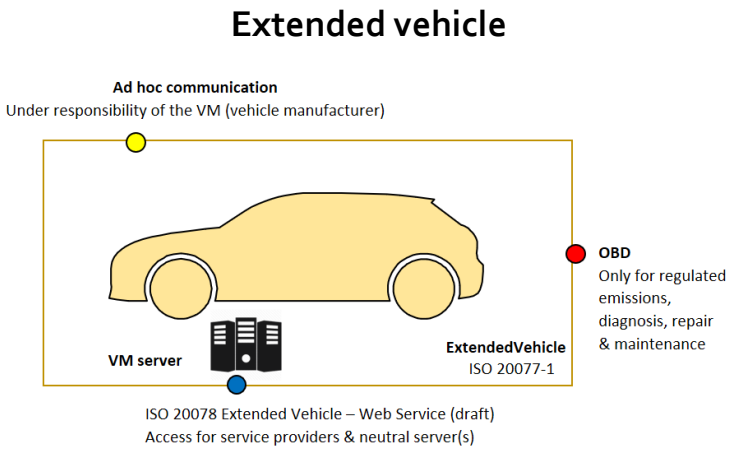
Example: Control unit monitoring.

This data will not be made available to third parties since it contains trade secrets, know-how or information covered by intellectual property rights that should not be disclosed to actual or potential competitors.

MEANS OF ACCESS

The extended vehicle concept (ISO standard 20077-1) makes it possible to access vehicle data through a number of interfaces that can be used depending on the purpose for which access is sought:

1. OBD interface for regulated emissions control, diagnosis, repair and maintenance;
2. Ad hoc communication interface under the responsibility of the vehicle manufacturer (eg applications in the field of cooperative intelligent transport systems); and
3. Web interface for all other third-party services (eg remote diagnostic support).



OFF-BOARD ACCESS

A motor vehicle is not a business or communications platform nor a smartphone on wheels. It is a means of transport, the primary function of which is to bring people and/or goods safely from one place to another. It is the vehicle manufacturer's responsibility that the vehicle operates in a safe and secure manner.

This is why any risk of attack on or access to the vehicle's security electronics through external systems or software programmes that are not under the control of the vehicle manufacturer must be avoided. Even uncontrolled third-party access to vehicle functions or data that are not directly security-relevant could lead to risks through networking: enabling vehicle theft and remote door unlock, for example, as well as creating opportunities for fraud, such as mileage manipulation, improper creation and misuse of movement profiles or sale of personal data. Similarly, it must be avoided that critical safety functions such as braking would be affected negatively by the use of in-vehicle resources for third-party applications.

To limit such risks, third parties shall not have direct in-vehicle access to data. Instead, vehicle manufacturers will communicate the relevant vehicle data in a secure manner to an off-board facility from where third parties can access the data.

Access to the data and the creation of functionality inside the vehicle using the data shall require a B2B agreement between the service provider and the vehicle manufacturer. The latter will not monitor data access except to prevent unauthorised access and system attacks, and to the extent required for quality management, compliance with data protection legislation and to enable payment. The anonymity of the party accessing the data shall be supported to the extent permitted by data protection legislation.

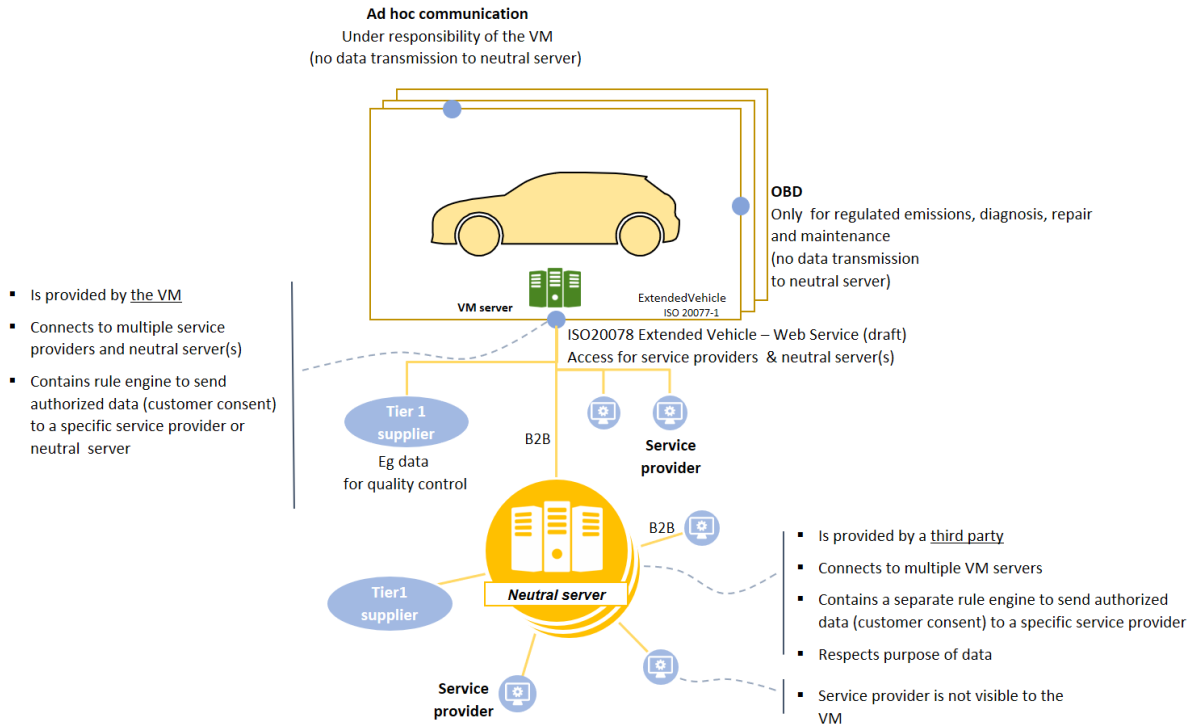
NEUTRAL SERVER

To promote competition, service providers should have the choice between accessing data directly through the vehicle manufacturer's server or via 'neutral' servers that would gather the data from vehicle manufacturers' servers. Therefore, each vehicle manufacturer will offer the possibility to independent third parties to operate such a neutral server. The neutral server operator(s) will be required to have a B2B agreement with the vehicle manufacturer and to implement state-of-the-art security and data protection measures. The vehicle manufacturer will not be responsible for operating or financing the neutral servers.

The data made available to the neutral servers will be of the same quality as the data available on the vehicle manufacturer's server and will be delivered without undue delay.

The neutral server operator(s) can negotiate the inclusion of additional data fields with the vehicle manufacturer and make these available on the neutral server(s) without revealing their usage or the requesting provider, thereby enabling the development of new business models independently from the vehicle manufacturer. The availability of the neutral servers should facilitate data access in particular for small and medium-sized companies by offering multi-brand data access on one server rather than obliging them to use multiple servers of individual manufacturers.

Extended vehicle, service providers and neutral server(s)



ADDITIONAL SAFETY AND SECURITY CONSIDERATIONS

OBD INTERFACE

Vehicle manufacturers will continue to grant access to vehicle data required for diagnosis, repair and maintenance by means of the OBD (on-board diagnosis) interface when the vehicle is stationary, in accordance with EU law.

Considering the risks of cyber attacks and the increasing threat to vehicle safety and security caused by connected plugs (so-called 'dongles') developed by third-party service providers, vehicle manufacturers reserve themselves the right to limit the data accessible via the OBD interface to those required for diagnosis, repair and maintenance.

OVER-THE-AIR ACCESS WITH WRITE FUNCTIONALITY

Similarly, for reasons of safety, security and product liability, third parties will not be permitted to perform any over-the-air writing in the vehicle.

THIRD-PARTY APPS

For safety, security and liability reasons, third-party applications that interact with the vehicle or with the driver via the vehicle display must continue to be developed and approved only in cooperation with the vehicle manufacturer on the basis of a B2B agreement.

Third-party applications running on mobile devices and using allocated vehicle data must remain under the responsibility of the relevant service provider.

European Automobile Manufacturers Association

ABOUT ACEA

- ACEA represents the 15 Europe-based car, van, truck and bus manufacturers: BMW Group, DAF Trucks, Daimler, Fiat Chrysler Automobiles, Ford of Europe, Hyundai Motor Europe, Iveco, Jaguar Land Rover, Opel Group, PSA Group, Renault Group, Toyota Motor Europe, Volkswagen Group, Volvo Cars, and Volvo Group.
- More information can be found on www.acea.be or @ACEA_eu.

ABOUT THE EU AUTOMOBILE INDUSTRY

- 12.2 million people - or 5.6% of the EU employed population - work in the sector.
- The 3.1 million jobs in automotive manufacturing represent 10.4% of EU manufacturing employment.
- Motor vehicles account for over €400 billion in tax contributions in the EU15.
- The sector is also a key driver of knowledge and innovation, representing Europe's largest private contributor to R&D, with €44.7 billion invested annually.
- The automobile industry generates a trade surplus of €100.4 billion for the EU.

European Automobile Manufacturers' Association (ACEA)
Avenue des Nerviens 85 | B-1040 Brussels | www.acea.be
T +32 2 732 55 50 | F +32 738 73 10 | info@acea.be | @ACEA_eu