November 2021

ACEA Position Paper

Access to in-vehicle data

EXECUTIVE SUMMARY

This document presents the views of the European Automobile Manufacturers' Association (ACEA) on a European regulatory framework for in-vehicle data access and sharing.

Our industry believes that the primary objective of this framework should be to achieve the creation of an ecosystem in which customers benefit from innovative services which improves their driving experience while ensuring their safety and security above all other concerns. This ecosystem should therefore ensure that providers of services to a connected vehicle can use the vehicle data that is required to provide the services that customers want and need while preserving customer choice over what data is shared, with whom, and for what purpose.

To that end, our industry recommends that this framework be articulated around a principle of fair and non-discriminatory access that will act as its cornerstone. Under this principle, providers of service to a connected vehicle would be granted access to the data and the resources that manufacturers use to offer services to their customers, and which their customers have agreed to share.

To enable the principle of fair, reasonable, and non-discriminatory access to in-vehicle data and resources, vehicle manufacturers suggest additional and specific **policy recommendations** that could be implemented in the upcoming regulation. The industry's recommendations are grouped in two clusters: access to in-vehicle data (I) and access to vehicle resources (II). The recommendations regarding **access to in-vehicle data** will ensure transparency and predictability for all stakeholders active on downstream markets:

- The catalogue of available data published by each manufacturer will provide a clear and precise overview of the in-vehicle data that can be licensed to service providers to provide the service that their customer requested.
- Defining a common framework for the description of vehicle data in an open standard will streamline data sharing and facilitate the activities necessary for their proper sharing with and use by all actors of the ecosystem.
- Within the common framework, establishing common sets of data will ensure that service providers can provide services to their customers across different brands and models of vehicles.
- Initiating a structured forum to discuss available data will provide manufacturers and data access seekers with the opportunity to help shape the data economy and the digital market, by ensuring that the latter can

voice their needs regarding the range and characteristics of the data delivered to the market.

- The publication of Service Level Agreement standardisation guidelines will foster the development of a common terminology to share the definition of the data and use cases and a common understanding of the data sets and APIs provided by manufacturers.
- Finally, the enactment of a principle of non-monitoring of data flows will provide additional trust by guaranteeing to all relevant parties that manufacturers do not monitor the commercial usage of data.

The industry's recommendations regarding **access to vehicle resources** will ensure that all market actors are equipped with the same tools to offer innovative and competitive connected services to vehicle users:

- The publication of guidelines for the deployment of third-party applications will ensure that service providers can offer the means for their customers to deploy applications in their vehicles in a safe and secure way.
- The enactment of a principle of equal right to write access for all relevant service providers will ensure that all market participants have access to the same abilities to offer competitive services to their customers, in compliance with conditions of safety, security, data protection and privacy and homologation.

ACEA and its members believe that these recommendations will ensure that all market players seeking to provide services to connected vehicles are equipped with the same tools and have access to equivalent input. This will allow them to compete fairly and on equal grounds and continue to innovate in a way that will broaden consumer choice, strengthen the European data economy, and benefit society at large.

Finally, we emphasise three important caveats when talking about data access and sharing:

- A vehicle is a device and tool to move people and goods. It cannot be compared to a software platform, a computer, or a smartphone. Safety and (cyber) security of the vehicle and its occupants and goods are paramount.
- The data market is a relatively new ecosystem for our industry. This is a highly competitive market in which European vehicle manufacturers not only actively compete against one another and against non-European manufacturers, but also with an increasing number of service providers, including very large international players. The market should be assessed while considering this competition and with a view to preserving and fostering the innovative power and competitiveness of our industry.

- A large portion of data are personal data. We value the customer's choice and deem it essential to provide transparency and preserve customer choice over what data is shared, with whom, and for what purpose. To enable customers to exercise their rights, the means of consent management must be centralised, consistent, and easy to understand and to use.

CONTENTS

INTRODUCTION

Today, vehicle customers want to use their added value services on their smartphone and integrate them in their vehicles. Use cases from vehicle data exchange can increase comfort and convenience for customers, improve products and services, and contribute 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. Many of those use cases are already utilised by customers.

The purpose of a vehicle is to safely transport people and goods. It is not a software platform, the primary purpose of which is to generate, share and receive data, and it should not be compared to personal computers or smartphones. For that reason, **ACEA's members make vehicle generated data available for third-party services in a manner that meets customer usage choices while also ensuring the protection of their personal data, that does not endanger the safety and (cyber) security of the vehicle and its occupants and does not undermine the liability or intellectual property rights of the vehicle manufacturer.**

Vehicle manufacturers showcase this with **tangible results** across the automotive value chain and beyond, be it in the B2B, B2G or B2C segment. Vehicle manufacturers also share data to protect pedestrians and cyclists. For example, manufacturers share data for repair and maintenance purposes, tailor made insurance coverage, mobility planning and traffic management, road safety (eg the Data for Road Safety ecosystem with member states' road authorities and service providers[1]).

The market has therefore evolved and grown, and the emergence of data marketplaces providing new and innovative offers to a growing number of players illustrates that this business is flourishing.

Vehicle manufacturers make vehicle generated data available to third-party in compliance with the following **basic principles**[2]:

- Customer choice
- Privacy and data protection
- Safety, security and liability

---

1 See www.dataforroadsafety.eu

2 See ACEA Position paper on access to vehicle data for third-party services, available at: https://www.acea.auto/files/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf

- Fair competition
- Interoperability
- Return on investment

In the context of the upcoming legislation on access to in-vehicle data, we suggest that the European Commission should limit itself to laying down the basic principles according to which data should be made available.

Each manufacturer should **remain free to adopt its own strategy** to participate in the European digital economy. They should thus remain able to define what data should be generated by the vehicles they manufacture and put on the market, based on their own economic and technical considerations, and to guarantee that the data access means that they deploy will not jeopardise the safety and security of the vehicles they put on the market – which is crucial to the manufacturer's liability – and protects the privacy of their customers and their customers' data.

Manufacturers, as data providers in this context, are at the lower end of the value chains, while service providers are at the higher end. Service providers currently benefit from a higher business potential due to their position in the value chain, while manufacturers are in a more vulnerable business position due to their traditionally low margin core business (ie the sale of vehicles) and lower service business potential. Yet, many stakeholders repeatedly ask for more; some still ask for more data access while some demand direct access to data so that they can bypass manufacturers entirely, and thus exclude them from the value chain, and ultimately from the market.

Manufacturers cannot be considered dominant undertakings on their primary market, nor can the data of connected vehicles be assimilated to an 'essential facility' under competition law.[3] Furthermore, manufacturers are subject to strong incentives that naturally leads them to share their data with other market players that are likely to bring them the know-how that they may lack today. They know and acknowledge that adopting an aggressively restrictive policy regarding data sharing will likely mean that they will be penalised by the market.

An ex-ante regulation has the potential to cause major adverse effects for the European automotive industry. It would notably restrict manufacturers' choice of economic model, thereby strongly limiting their **incentives to invest**, thus compromising the **dynamics of innovation** at a time when the automotive market is changing and the market for data and related services is **emerging**.

[3] See D Geradin, Access to In-Vehicle Data by Third-Party Service Providers: Is there a Market Failure and, if so, How Should it be Addressed? (February 28, 2020). TILEC Discussion Paper No 041, available at SSRN: https://ssrn.com/abstract=3545817 or http://dx.doi.org/10.2139/ssrn.3545817

The EU principle of proportionality should therefore prevail. This implies that the legislation should strike a fair balance between the requirements for vehicle manufacturers and the needs of other stakeholders.

This principle complements the principle of non-discrimination and equally suggests that vehicle manufacturers should not be obliged to make available data that they do not have or that they do not use themselves.

It also means that the vehicle data concerned should not be standardised since this would impose a huge technical and financial burden on manufacturers without being indispensable for independent operator. Rather, the definition of **a common framework for the description of vehicle data** is recommended.

We agree that the purpose of the regulation should be to **stimulate fair competition** on downstream markets **without deterring or impeding competition between vehicle manufacturers**. It would be fair to extend the basic principles of EU law that currently govern physical access to repair and maintenance information (RMI) to the sharing of in-vehicle data. Vehicle manufacturers are engaged in data sharing today with many parties such as suppliers, road agencies and operators, repair shops, insurers, fleet managers, mobility providers.

ACEA and its members offer to share their experience on these promising market developments and to sustain a constructive dialogue with the Commission services to achieve a balanced approach in the policy outcome. **To that end, we propose that the following principles and policy recommendations be enshrined in European law.**

I. PRINCIPLES

A. FAIR AND NON-DISCRIMINATORY ACCESS

To ensure fair and undistorted competition on the market, a level playing field must exist between vehicle manufacturers and third-party service providers active on the same relevant market. To enable this, the upcoming regulation could mandate that **manufacturers provide fair, reasonable, and non-discriminatory access to in-vehicle data and resources (FRAND)**. A possible definition of what is understood under this FRAND concept could be that licensing terms be negotiated in good faith, allowing access to essential technologies and / or data in exchange for a fair reward, under the same or similar terms as determined with other licensees.

To implement this principle in a clear and concrete way, the Commission could enshrine the following requirements in the upcoming regulation on access to in-vehicle data:

- **Third parties are given access to the same vehicle-generated data** as manufacturers use to offer their customer services. The data will be of the same quality and accessible at the frequency implemented and used in manufacturers' customer services.
- **Third parties are given access to the same resources**, at the same time and to the same extent as granted to the manufacturer itself to provide its connected services, **but only where it is safe and sound to do so**.

  '**Resources**' is understood as a function of the Extended Vehicle, designed by the manufacturer of the product. These are made accessible to third parties who can interact with them from a connected service. This includes, for example, the possibility of displaying messages on an HMI display, activating a function such as the preheating system, or opening the boot remotely (see description below).

B. CUSTOMER CHOICE, DATA PROTECTION AND PRIVACY

A large portion of data are qualified as personal data. Manufacturers believe it is essential to provide transparency and preserve customer choice over what data is shared, with whom, and for what purpose. This is necessary to retain the trust of customers and to allow all stakeholders in the ecosystem to comply with their respective obligations under relevant privacy legislation (including the GDPR).

In-vehicle data sharing is limited by privacy and data protection rules. Data sharing must therefore be based on clear terms and conditions and privacy notices ensuring that consumers know what data they share and with whom, in full compliance with these rules. Customers must give permission for third parties to access their data, and we strongly believe that they must remain in control of data sharing at all times.

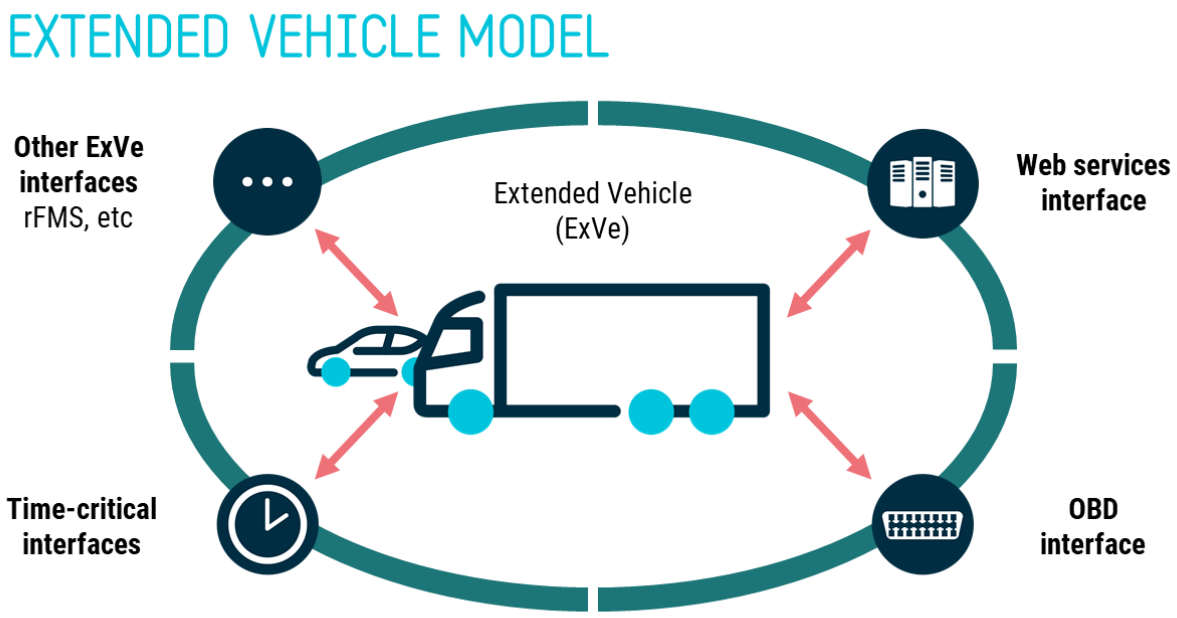
To enable customers to exercise their rights, the means of consent management must be centralised, consistent, and easy to understand and to use (contrary for example to website cookie banners). Therefore, an end-to-end use case-based data processing and consent management by the manufacturer is the only viable option.

The principles of legitimate data use and of data minimisation state that data collected and processed should not be held or further used unless it is essential, for reasons that were clearly stated in advance to support data privacy. This prevents manufacturers from transferring data without a clear use for it.

C. MEANS OF ACCESS

The means by which in-vehicle data will be accessed should not be regulated.

Vehicle manufacturers already deploy the Extended Vehicle model and believe that the choice of the technology used to access data is based on the best practices in the industry, underpinned by the key principles of safety and security of the driver. We believe that the ISO Extended Vehicle model satisfies the FRAND principle.



The Extended Vehicle[4] 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. On-board Diagnostics (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).
3. Web interface for all other third-party services (eg remote diagnostic support).

The customer determines whether they wish to share their personal data. Each vehicle manufacturer determines which technology will be used to make that data available to third parties on a non-discriminatory basis.

In addition, manufacturers can innovate and switch to future oriented technologies where needed while keeping the customer in mind. It is not recommended that legislation prescribes a specific technology given the need for continuous innovation in Europe. By applying this principle, the regulator would avoid making technology choices that are normally best made by economic operators.

Service providers can access vehicle data through the same Extended Vehicle interface by which the manufacturer, acting as a service provider, accesses that data.

Manufacturers may also provide access to in-vehicle data via marketplaces that they manage, which ensure data privacy for customers through consent management and end-to-end use case-based data processing.

Manufacturers may also make data accessible to data marketplaces, including **Neutral Servers**, that:

- Are connected to one of the Extended Vehicle's interface, as agreed with the manufacturer.
- Provide access to the in-vehicle data that they hold to third parties.
- Are neither operated nor financed by vehicle manufacturers.
- Implement state of the art cybersecurity systems.
- Comply with all relevant legislation on data protection and privacy.

Data made available to data marketplaces is of the same quality as the data available on the manufacturer's interface and is delivered without undue delay. This

[4] ISO 20077-1: Road Vehicles – Extended Vehicle (ExVe) methodology – Part 1: General information; ISO 20077-2: Road Vehicles – Extended Vehicle (ExVe) methodology – Part 2: Methodology for designing the Extended Vehicle.

fact was demonstrated by vehicle manufacturers and Neutral Server operators in the framework of the User Group on the Extended Vehicle organised by ACEA, CLEPA, AFCAR, Insurance Europe, HERE Technologies and TomTom in 2018. Furthermore, service providers and Neutral Servers can negotiate the inclusion of additional data fields with vehicle manufacturers.

To enable the principle of fair, reasonable, and non-discriminatory access to in-vehicle data and resources, vehicle manufacturers suggest additional and specific **policy recommendations – described in detail in the sections below –** regarding the access to the vehicle's data (II) and resources (III) that could be implemented in the upcoming regulation.

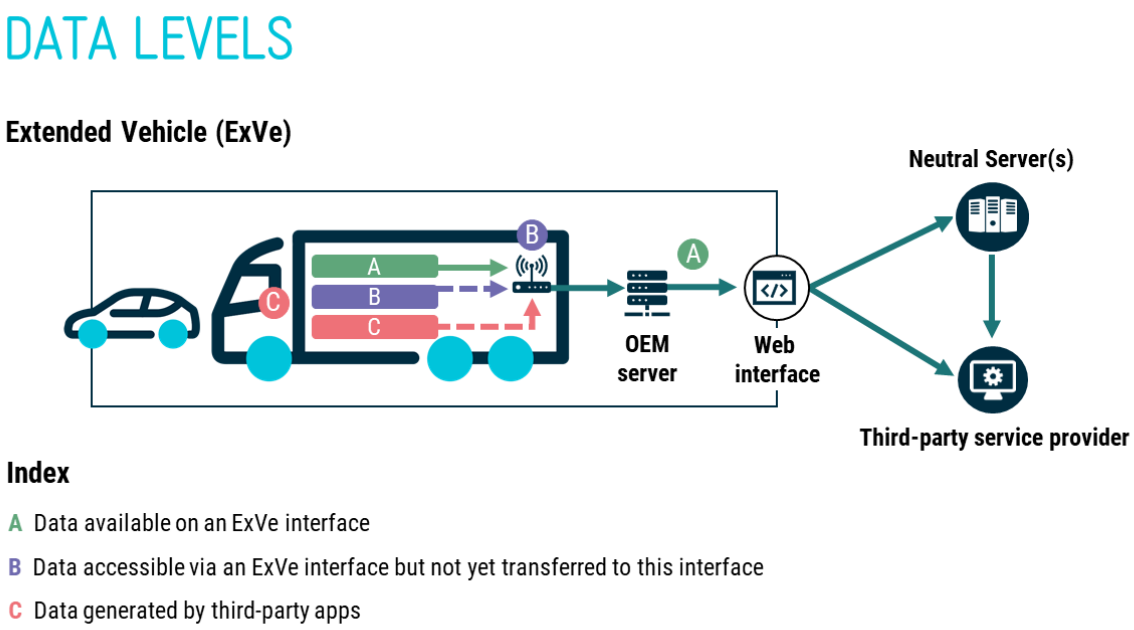
II. ACCESS TO THE VEHICLE'S DATA

A. DESCRIPTION AND CURRENT STATUS

A regulation on access to in-vehicle data should be based on a clear and accurate understanding of the functioning of a vehicle, of how data is generated and how it is made available for access on a vehicle interface, regardless of the data level considered.

1. Levels of data

Available data points differ depending on the vehicle manufacturer and the equipment level of each customer vehicle. Bearing this in mind, the following scheme describes approaches to enable access to relevant data depending on the requests of the third party.



2. Description of levels of data

A. LEVEL A – AVAILABLE DATA

Data in the vehicle is available on the vehicle manufacturer's (OEM) backend via the Extended Vehicle interface selected by the manufacturer.

Level A data is data that is already available through an Extended Vehicle interface because the customer already avails of a service that requires the transfer of that

data. Level A data can be accessed by third parties, including Neutral Servers, via the Extended Vehicle interfaces selected by the manufacturer. The customer controls the transfer and use of this data and their agreement is required to transfer level A data from their vehicle to the OEM server.

Further consent from the customer is required for the manufacturer to transfer level A data from the OEM server to the third party of their choice. Level A data can be accessed at the frequency and resolution used by the manufacturer to provide customer services.

Customer data can only be transferred where end-to-end use case-based data processing is ensured, and the data quality is validated. This means that the customer controls their data through the manufacturer's customer management process from beginning to end.

B. LEVEL B – ACCESSIBLE DATA

Level B data is data that can be made accessible via an Extended Vehicle interface but that has not yet been transferred to this interface.

Manufacturers only extract data that is necessary to provide a service which the customer avails of. In order to foster the development of the digital market, manufacturers are willing to provide access to additional data fields if the customer has availed of a third-party service for which this data is necessary, provided that such a transfer is technically feasible and has been implemented by the manufacturer. On this basis, the service provider and the manufacturer can discuss and define access to additional data fields through a transparent and user-friendly process, standardised at ISO[5] or as part of an open standard (see description below).

For a third party to access Level B data, a B2B agreement with the manufacturer will be required. Manufacturers can only transfer data for specific purposes, when the customer consents to it, and subject to the technical limitations described below. The data will be transferred specifically for that third party's usage and for specific purposes pre-agreed to by the customer. The data will then be channelled to the third party via an Extended Vehicle interface. Neutral Servers can also request access to Level B data from manufacturers, that they will then make available to third parties.

[5] ISO 20077-3 Road Vehicle – Extended Vehicle (ExVe) - Upstream process to develop services. This standard is currently under development.

C. LEVEL C – DATA GENERATED BY APPLICATIONS

Data that is generated by applications hosted in a vehicle's electronic control unit (ECU). These applications can be used to aggregate and process data on-board.

A B2B contract will be required between the manufacturer or its subcontractor (eg Android Automotive) and third parties wishing to develop, integrate, test, and deploy applications. Such practices exist today in various service segments such as insurance, roadside assistance, etc.

Access to vehicle resources, and the transfer of data generated by third-party applications is governed by the B2B contract. Any data generation and data transfer must meet compliance requirements and ensure cyber security.

3. Limitations

There are inherent limitations to the amount of data that can be processed in a vehicle and transferred to an interface.

Over the years, vehicles have become marvels of technology, bringing increasing intelligence and functionality to the benefit of customers and society. This was and continues to be achieved through the gradual and careful inclusion of state-of-the-art information and communication technology, and the widespread use of computing power and ECUs. Yet with this added capability also comes the inevitable complexity and vulnerability of such systems.

Vehicle manufacturers relentlessly work towards building safe and robust systems that offer customers new functionality while safeguarding their safety and protecting the vehicle's integrity. The safety and security of the vehicle's occupants is their overriding priority.

A vehicle is not a smartphone on wheels, nor is it a personal computer that can be rebooted if a problem occurs while driving. Furthermore, it is not a software platform the primary purpose of which is to generate, process, share and receive data. A vehicle is a means of transport, the primary function of which is to bring people and goods safely from one place to another. It therefore requires much higher standards in safety, security and privacy compared with smartphones or other consumer devices, and components must work under extreme 'automotive grade' conditions.

From a technical point of view, transferring additional data points requires deep modifications of the physical architecture and the software of the vehicle, which in turn will require oversizing the computing power of the vehicle. Such measures have a significant impact on the total cost, resources optimisation and on the environment.

To access more vehicle data, it would be necessary to physically bring that data to an Extended Vehicle interface through the networks. In order to transfer this data, each ECU in the chain would need to be modified, from the point where the data was generated up to the telematics unit, which would affect multiple networks and ECUs. Currently, in-vehicle networks are based on a combination of several different data networking protocols. Additional information will increase traffic to the vehicle's networks, which will require modifying the vehicle's electric and electronic (E/E) architecture.

Such modifications can be made to future vehicles in general and may be made on specific models or versions of models of vehicles. However, such modification must reflect and respect the customer's expectations and wishes, and they must be willing to cover the development (capital investment) and connectivity (operational costs) costs when they decide to purchase such a vehicle.

Any policy initiative regarding access to vehicle data for third party services must take these limitations into consideration, and the consequences they may have on a customer's ability to choose a vehicle which best suits their needs.

4. Data access request process

When a stakeholder seeks to provide a service using vehicle data or resources over the air, it is necessary to provide a clear process for this provider to submit its request to the relevant vehicle manufacturer. To that end, ISO (TC22/SC31/WG 6 Extended Vehicle) is finalising a draft Technical Report entitled 'Road vehicle - Extended Vehicle – Upstream process to develop services'.

This Technical Report describes a process to **initiate and facilitate the communication between service providers and vehicle manufacturers**, whereby service providers express their request to access data and resources from the Extended Vehicle interfaces for the purposes of developing services.

B. POLICY RECOMMENDATIONS

To ensure that all stakeholders get access to the vehicle generated data they need to provide the services that their customers have booked, the following policy recommendations regarding access to data could be implemented as part of a regulation on access to vehicle data.

1. Catalogue of available data

To provide additional transparency and ensure that service providers have access to the information that they need regarding vehicle generated data available on the market, the upcoming regulation could require that vehicle manufacturers publish a **catalogue of available data**.

This catalogue would provide a list of the data available on the vehicle manufacturer's server via the Extended Vehicle web services interface or other available interfaces (level A data).

This regulation could further require that this catalogue be readily available in electronic format, prominently displayed on the website of the vehicle manufacturer.

2. Common framework for the description of vehicle data

Vehicle manufacturers believe in the need to define a common terminology to share the definition of the data and associated use-cases and to ensure that data access seekers understand the data sets licensed by vehicle manufacturers. Such a common terminology would streamline data sharing and facilitate the activities necessary for their proper sharing with and use by all actors of the ecosystem.

Vehicle manufacturers **believe that the standardisation of in-vehicle datasets and the standardisation of the format of in-vehicle data are not appropriate measures** to achieve this objective.

Defining a common data format would impose a huge burden on manufacturers without being indispensable for independent operators. It is important to consider that different vehicle architectures are the result of decades of significant investments in research and development, and engineering efforts driven by competition in the automotive industry.

Therefore, an imposed standardisation of vehicles' architecture would not only force manufacturers to incur significant unforeseen costs but would also affect their leverage for differentiation, and thus severely impede their ability to innovate as it would prevent the evolution of future vehicle architectures. Such a forced standardisation will also deprive the customer from reaping the benefits that this evolution and this innovation would have brought.

The Extended Vehicle provides inter alia for a standardised web interface to the vehicle manufacturer's server. It does not standardise the relevant vehicle data. Instead, **metadata description** that enables data to be understood in a consistent manner is available on the vehicle manufacturer's back-end server, upon request from a service provider, to ensure interoperability. Metadata descriptions promote

interoperability without imposing the burdens raised by the standardisation of in-vehicle data.

Vehicle manufacturers believe that a standardised description of the characteristics of in-vehicle data will facilitate their use by various actors of the ecosystem and foster innovation. This would streamline data sharing and facilitate the activities necessary for their proper use. The industry therefore recommends defining **a common framework for the description of vehicle data**.

To that end, vehicle manufacturers, together with representatives of the entire automotive supply chain, are currently working in ISO[6] on a common metadata description.

An open standard co-developed by industry players in the automotive domain would provide standardised data characteristics in various domains such as fleet management and address the need for emerging use cases to evolve over time.

An example of such an open initiative to establish standardised data and interfaces description is the Common Vehicle Interface Initiative (CVII) jointly hosted by GENIVI Alliance and W3C.

To further enable the efforts of the industry in this area, the upcoming regulation could support the development of an open standard for metadata description.

3. Common sets of data within the common framework and interoperability

To ensure that service providers can provide services to their customers across different brands and models of vehicles, stakeholders require that common sets of data are established that would be made available to third parties.

Such **data sets should be elaborated by the industry to reflect the needs of the market** and should be discussed with relevant access seekers in a structured forum (see description below). These data sets **would be defined with the common framework for the description of vehicle data** (see above) and **focus on data that are essential to fulfil clearly identified use-cases currently offered on the market and subscribed to by customers.**

These data sets would be made available to third parties to the extent that they can be generated and be made accessible via an Extended Vehicle interface for a given vehicle (level B data). They would be made available in addition to the data that individual manufacturers already make available to third parties (ie level A data).

These data sets would be licensed on an individual basis and be subject to terms and conditions for usage.

[6] ISO TC 22/SC31/WG6 “Extended Vehicle/Remote Diagnostics”

4. Structured forum to discuss available data

To ensure that data access seekers have an opportunity to help shape the data economy and the digital market, they should have the ability to voice their needs regarding the range and characteristics of the data delivered to the market.

The number of available data points will increase over time as vehicle software is updated and new models and vehicle types are deployed. There are four steps that must be followed to expand the set of available data:

1. **Data basis**: the basis for data is defined by the underlying platform and depends on the availability of data (eg from sensors). Significant expansion of the data base will happen with the introduction of the new vehicle platforms and will lead to an increase in the availability of data for future third-party use cases.
2. **Data availability**: It requires use cases to obtain data, establish necessary processing and perform quality checks. These use cases can be proposed by any interested party. Based on these use cases, the set of available data will grow with as the number of new vehicles featuring new platforms increases.
3. **Data privacy**: A prerequisite for the transfer of data to third parties is that the data is transferred for a specific purpose – namely use cases based. The manufacturer provides the corresponding consent management.
4. **Data accessibility**: The set of available data will be expanded step by step for further roll-out of services on various vehicle platforms in the future, thereby making more data for third parties easily accessible.

To ensure this, the upcoming regulation could set up a **structured forum in which relevant stakeholders could participate to discuss the range and characteristics of in-vehicle data generated by future generations of vehicles, based on the four steps** described above.

For efficiency purposes, to ensure a healthy dialogue between stakeholders and guarantee that the discussions that will take place in this forum are set at the right level and can deliver demonstrable results, **this forum should exclusively involve individual vehicle manufacturers and in-vehicle data access seekers**.

This forum could be organised and moderated by a neutral entity, such as the Commission or a consultant it would appoint. The forum would act as a facilitation and advisory body that could, where relevant, make policy recommendations to the Commission.

Nevertheless, decisions reached by this forum should not impede innovation by imposing requirements regarding the architecture of the vehicles produced by

manufactures, nor should it prevent manufacturers from providing model-specific data.

5. Service Level Agreement standardisation guidelines

The automobile industry supports a process for the analysis of an access request that is known and shared. It begins at a manufacturer's entry point and allows for a request to be processed in a way that guarantees to both parties – access seeker and manufacturer – a collaboration under equitable, fair, and reasonable conditions, and which will factor-in their respective interests.

To that end, the industry notes that the existence of a common terminology to share the definition of the data and use cases and to understand the data sets and APIs provided by manufacturers would be advantageous.

With a view to ensuring additional certainty to data access seekers when seeking access to in-vehicle data from vehicle manufacturers, the upcoming regulation could provide for the publication of a set of **guidelines on the standardisation of service level agreements for in-vehicle data providers**[7].

These guidelines would be drafted by an expert group involving the industry, appointed by the Commission and under its supervision. They could provide definitions of the technical terms used in Service Level Agreements (SLAs), as well as specific Service Level Objectives (SLOs) designed to achieve standardisation for several aspects of SLAs. The guidelines could provide specific SLOs for example in terms of codes of conduct, standards and certification mechanisms, data minimisation, limitations on the use, retention and disclosure of personal data, security, openness and transparency, and interoperability.

6. Principle of the non-monitoring of data flows

Vehicle manufacturers commit **not to monitor the commercial usage of data** flowing between Extended Vehicle interfaces and third-party service providers, OEM marketplaces or, where applicable, Neutral Servers. There will be no monitoring of outbound data to a third-party service provider, OEM marketplace or, where applicable, a Neutral Server.

Nevertheless, some monitoring will be required for legal, contractual or security purposes, to enable the optimisation of the vehicle and its technical development, the optimisation of the data transfer between the vehicle and the manufacturer's server

[7] A similar initiative was recently published for cloud services. See Cloud Service Level Agreement Standardisation Guidelines, available on the Commission's website at https://digital-strategy.ec.europa.eu/en/news/cloud-service-level-agreement-standardisation-guidelines

and to enable customer consent management. The manufacturer will not use the data that flows between the server and the third-party service provider or Neutral Server to analyse third-party services.

To provide additional trust to data access seekers, this principle could be enshrined in the upcoming regulation on access to in-vehicle data. Additionally, the regulation could provide that the examination of the corresponding implementation be part of a process of external audit by an independent entity.

III. ACCESS TO THE VEHICLE'S RESOURCES

A. DESCRIPTION AND CURRENT STATUS

As explained above, '**resources**' is understood as a function of the Extended Vehicle, designed by the manufacturer of the product. These are made accessible to third parties who can interact with them from a connected service. This includes, for example, the possibility of displaying messages on a human machine interface (HMI) display, or activate a function such as the preheating system, or to open the boot remotely.

1. Access to the vehicle's display

The ability for a service provider to exchange information with its customer via the vehicle's display is a convenient means to provide innovative services to vehicle users. To that end, vehicle manufacturers have developed and integrated different methods to enable service providers to communicate bi-directionally with their customers via the vehicle display which, while providing the service provider and the user with the same experience and the same abilities, may entail different requirements.

A. SUMMARY

Third-party applications running on the driver's smartphone in 'terminal mode' can be displayed in the vehicle's HMI by means of 'mirroring'.

Besides the mere mirroring functionality, third-party content can be brought to the vehicle through the Extended Vehicle via a manufacturer-specific solution (eg SDL, Apple Car Play, Android Auto, etc).

These solutions are mobile application interfaces. Applications running on a smartphone can connect via Bluetooth or USB to the vehicle. Control is managed via the vehicle's display, its hard buttons and through voice control. Data that is relevant to the interaction with the application is exchanged exclusively between the smartphone application and the vehicle. The manufacturer does not have any knowledge of, or any access to the data exchanged.

The application can receive data but cannot write. This ensures a high level of security as nothing in the car can be modified. It further ensures a high level of transparency as there is a full disclosure of data elements available.

Alternatively, there are other solutions which manufacturers can implement to allow third-party infotainment applications to display content on the HMI.

Vehicle manufacturers are already working through B2B arrangements with third-party service providers to enable them to interact with their consenting customers.

Different approaches are possible to allow third parties to communicate directly with their customer in the vehicle, depending on the technology deployed by the manufacturer, for example:

- **Message centre**: Connected drive messaging service to third party allowing for info-messages with content (text) and sender details (navigable address and phone number) to be communicated to the driver.
- **Manufacturer-specific system**: Manufacturer-specific environment (OS) and app store allowing third parties to develop and deploy their own applications in the vehicle's HMI.
- **Partner system:** Software framework (such as Android Automotive for some multimedia applications) and apps store solution (for more deeply embedded application) provided by a supplier allowing, via a software development kit (SDK). Third parties to develop, test and deploy their own applications in the vehicle with access to vehicle data and HMI.

Depending on the technology used (manufacturer-specific or sub-contractor solution), governance of this process is performed by the vehicle manufacturer or in some cases the platform manager (eg Apple for CarPlay or Google for Android).

B. CAVEATS

Access to the HMI (including its screen and controls) must comply with basic conditions, amongst which:

- Legal requirements, notably regarding driver distraction, ethical / moral requirements.
- HMI design specifications, eg font size, layout, driver centring, animations, determined by the manufacturer.
- Architecture, resources, and security specifications.

2. Write access

In principle, write access levels 1 to 6 are possible by third parties for relevant use-cases (eg remote diagnostics support) over the Extended Vehicle interface selected by the manufacturer, or where applicable via the manufacturer's marketplace, when permitted by the vehicle's design. Their usage is dependent on the existence of a B2B agreement between the manufacturer and the specific third party.

Furthermore, levels 1 to 3 may also be possible via a Neutral Server for relevant use-cases. This means that a third-party service provider can access levels 1 to 3 without disclosing its identity to the manufacturer.

Write access levels are described in Annex I.

B. POLICY RECOMMENDATIONS

1. Guidelines for the deployment of third-party application

As described above, the automobile industry supports a process for the analysis of an access request that is known and shared. This includes an access request for vehicle resources from an application developer wishing to deploy their application in a vehicle's infotainment system.

With a similar view to ensuring certainty to service providers when seeking access to in-vehicle resources from vehicle manufacturers, the upcoming regulation could provide for the publication of a set of guidelines on the deployment of third-party application in a vehicle.

These guidelines should be technology neutral; they should respect the manufacturers' choice of the technology that should be deployed in the vehicle that they produce.

By way of illustration, ACEA and its members have developed indicative guidelines that could be followed by manufacturers and third parties to develop such applications, and which define the roles and responsibilities of each actor.

ACEA's indicative guidelines to deploy third-party applications in the vehicle are described in Annex II.

2. Principle of equal right to write access

A. PRINCIPLE

To further enable the principle of fair access to the vehicle's resources, the Commission could enshrine in the upcoming regulation the right for authorised third parties to be given access to the same level of write access, at the same time and to the same extent as granted to the manufacturer acting as service providers and to its authorised repair shops active on the same relevant market. This corresponds to write access levels 1 to 6 as described in Annex I.

This right shall be subject to the caveats described below.

B. CAVEATS

In contrast to read-only access to vehicle data stored in the backend, write access allowing for an interactive connection to the vehicle, its data and resources presents additional risks to the integrity of the vehicle's systems, its operational safety, and the safety of its occupants.

Restrictions shall therefore apply with regards to for example data protection, data privacy, IP rights, cyber security or homologation.

Only specific cases of write access are feasible and can be implemented without any homologation's issues.

Nevertheless, all relevant data and functions are made available by the vehicle manufacturer via an abstraction layer so that particularly risky operations and operating modes can be avoided.

The vehicle must be safe and secure for writing access (eg to avoid sliding or trapping of persons in the window). This status must be confirmed by the vehicle as a prerequisite for any write access, in addition to the basic consent of the vehicle owner for the service offered.

Furthermore, there are cases in which the person in the vehicle (eg driver or repair shop's employee) must additionally confirm that neither persons nor the environment are harmed in any way (eg engine turned on in a closed room).

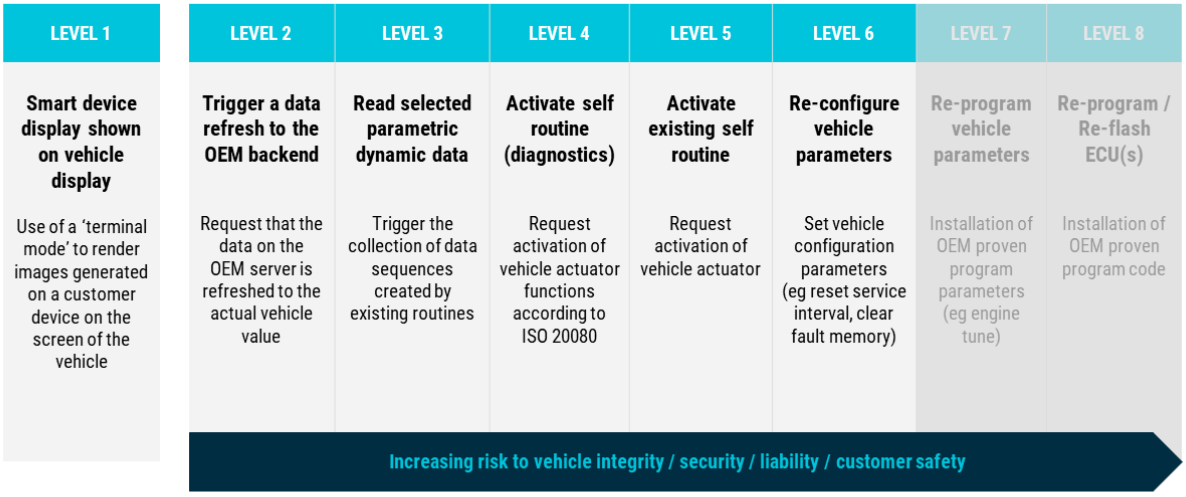
In any case, write access can only be given to one party at a time to avoid mutual interference.

Indeed, ACEA and its members believe that these recommendations will ensure that all market players seeking to provide services to connected vehicle are equipped with the same tools and have access to the same input. This will allow them to compete fairly and on equal grounds and continue to innovate in a way that will broaden consumer choice, strengthen the European data economy, and benefit society at large.

ANNEXES

ANNEX I – WRITE ACCESS LEVELS

WRITE ACCESS LEVELS



ANNEX II – ACEA INDICATIVE GUIDELINES FOR THE DEPLOYMENT OF THIRD-PARTY APPLICATIONS

1. Security, vehicle integrity, driver distraction

- The manufacturer or the platform manger provides developer guidelines for its deployed platform strictly where specific adaptions are needed for the platform.
- The manufacturer or the platform manager provides SDK for the development of apps, where available, subject to license agreement.
- For safety reasons, the control of applications may depend on whether the vehicle in motion or stationary and will be stipulated by the manufacturer or the platform manager depending on safety assessment.
- Third parties shall be requested to provides app source code for security review.
- Third parties shall ensure compliance with applicable legislation relating to driver distraction. A verification via the manufacturer is required.

2. Vehicle resources

- Memory / processor requirements is defined by the manufacturer or the platform manager based on the resources available.
- Deployment of new features by the manufacturer or the platform manager, as well as those required to comply with applicable legislation, will take priority over third-party apps. Load testing of hardware (CPU, GPU and memory) needs to be conducted by the manufacturer in order to ensure a stable system.

3. Corporate design

- The manufacturer or the platform manager provides widget set for applications.
- Standard widgets and associated settings are managed within an SDK.
- The desktop is defined by the manufacturer or the platform manager in the context of the vehicle's HMI.

4. Content relevance

- Applications are expected to fulfil predefined criteria (eg related to services around the car, mobility or driving experience, risk of driver distraction) and may not be accepted if they do not comply with these criteria.

5. Integration and test

- The manufacturer or the platform manager provides integration, test, bug fix processes.
- Integration and test schedules are agreed between the manufacturer or the platform manager and third parties.
- Incompatibilities between applications, or between an application and the platform, identified by the manufacturer or the platform manager, must be resolved by the third-party developer.
- If the manufacturer updates or patches the vehicle system, the application provider is required to ensure compatibility or remove the application.
- The application provider is expected to provide support to its customers. The manufacturer or the platform manager does not provide customer support for integrated third-party applications.

- Third parties are to provide remuneration for integration and test services provided by the manufacturer or the platform manager.
- The manufacturer shall not be held liable for any breach of data protection and privacy rules by third parties.

6. Operation and maintenance

- Throughout the vehicle's lifecycle, the manufacturers' system must be allowed to monitor the operation, as well as incoming and outgoing data streams to ensure that the application operates correctly (eg ensuring latest cyber security level).
- In case of a malfunction, the manufacturer or the platform manager is entitled to deactivate the app until the cause of the malfunction has been fixed.

7. Data transfer (including application updates)

- Remuneration for the transfer of data resulting from the on-board app is determined by the manufacturer or the platform manager.
- To guarantee certain levels of latency for new technologies such as assisted driving and highly automated driving, some limitations are required. Third-party software shall not jeopardise essential vehicle software. Should this requirement be disregarded by a third party, the manufacturer shall be free to introduce any corresponding restrictive measure it sees fit to address the issue.

8. App store

- Applications are made available via an app store, or another other user-friendly means (eg over-the-air).
- From the available apps in the vehicle, the customer decides which apps are to be installed in the vehicle.

ABOUT THE EU AUTOMOBILE INDUSTRY

- 12.6 million Europeans work in the auto industry (directly and indirectly), accounting for 6.6% of all EU jobs
- 11.6% of EU manufacturing jobs – some 3.5 million – are in the automotive sector
- Motor vehicles are responsible for €398.4 billion of tax revenue for governments across key European markets
- The automobile industry generates a trade surplus of €76.3 billion for the European Union
- The turnover generated by the auto industry represents more than 8% of the EU's GDP
- Investing €62 billion in R&D per year, automotive is Europe's largest private contributor to innovation, accounting for 33% of the EU total

REPRESENTING EUROPE'S 15 MAJOR CAR, VAN, TRUCK AND BUS MANUFACTURERS

ACEA
European Automobile
Manufacturers' Association
+32 2 732 55 50
info@acea.auto
www.acea.auto

twitter.com/ACEA_auto

linkedin.com/company/acea

youtube.com/c/ACEAauto