FEDERATION INTERNATIONALE DE L'AUTOMOBILE
REGION I - EUROPE, THE MIDDLE EAST AND AFRICA

# POLICY POSITION ON CAR CONNECTIVITY


## Executive Summary

Car connectivity allows for promising applications in the fields of travel, traffic and vehicle support, particularly in terms of repair and maintenance. Data is the key enabler of this new economy. Access to data and its usage rights will be determining factors for market players to design and offer services in the future. European motorists are willing to embrace car connectivity[1], provided that they know which data their vehicle shares and are given a real choice with whom they wish to share data.

The existing European regulatory framework on repair and maintenance addresses the situation prior to connectivity. In this document, FIA Region I takes stock of the manner in which the regulatory framework successfully allows for competition in the aftermarket in the pre-connectivity context. It further outlines the current developments, related challenges and develops a series of policy recommendations. These recommendations pursue three main objectives:

- Data protection: drivers should retain ownership of data and give informed consent on its use
- Free choice & portability: drivers should have the right to choose their preferred service providers and freely consent to data being transmitted by their vehicle
- Fair competition: a variety of service providers should have the right to develop safe products & functionalities.

[1] A **connected car** is a car equipped with Internet access, and usually also with a wireless local area network. This allows the car to share data with other devices both inside as well as outside the vehicle.

## Legislative Background

Cars are complex products; they represent a high expense on households in repair and maintenance over their lifetime. The European Union therefore enacted a framework[2] to ensure sound competition between brand dealerships and independent garages. Based on existing legislation, consumers can choose from a variety of repair and maintenance service providers today. The proposed revision of Type Approval Regulation[3] for passenger cars should regroup most of the provisions on access to repair and maintenance information, currently within Regulations (EC) No 715/2007 and 692/2008 (Euro 5 & 6). This framework however does not guarantee remote access. Increased vehicle connectivity will allow real-time access to diagnostic data which will facilitate repair and maintenance, rendering the current legislative framework partly obsolete. As technology will allow remote repairs in some cases, this should be included in the relevant legislation.

***112 eCall***
*An in-vehicle system that triggers an emergency call and sends vehicle data in the case of a crash either automatically or manually*

The mandatory implementation of the European emergency call (eCall) shed an additional light on the need to review the current framework. By 2018, passenger cars will be equipped with eCall, a system that can trigger data exchange with an emergency support centre shortly after an accident. Regulation 2015/758 foresees the coexistence of a public service, which will direct the call to emergency number 112 and a so called Third Party Service eCall, which will send the call to a private operator. As a logical consequence, the Commission will also evaluate the possibility to mandate eCall on a "*interoperable, standardised, secure and open-access platform*" by 9 June 2017.

In its report on the Digital Single Market, the European Parliament calls for "*a regulatory framework for connected vehicles to ensure interoperability with different services (…) to uphold fair competition*" and to satisfy the need for safe products, which respect data protection. Mandating a neutral technology to implement eCall would allow consumers to reap the full benefit of connectivity.

Connected vehicles will play a central role in many citizens' daily life and should be at the heart of new mobility models. The deployment of Intelligent Transport Systems (ITS) will require vast amount of data to be gathered and processed for the benefit of all. While the need to ensure access to data is paramount for ensuring a healthy economic development of this new field of opportunities, the protection of personal data is essential, as well as cybersecurity. The Commission has worked with stakeholders to define key recommendations for C-ITS deployment.

[2] Motor Vehicle Block Exemption Regulation 4651/2010
[3] Proposal for a Regulation of the European Parliament and Council on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles", COM (2016)/0014 COD

Public perception is also key: a recent survey commissioned by FIA Region I shows that a vast majority of road users consider that the vehicle driver or owner should own their data[4]. In the survey, 95% called for legislation to protect their vehicle data. Therefore, a robust data protection framework, adapted to the specifics of in-vehicle data, needs to be developed.

## FIA Region I Position

European consumers are ready to embrace connectivity, but not at the expense of data privacy or their freedom to choose service providers. Today, decision-makers are faced with the challenge of safeguarding competition in an increasingly immaterial world. Connected motorists expect to be empowered to freely choose from a variety of safe and secure product functionalities directly from their dashboard – and be able to select various options over the lifetime of their vehicles. In 2014, the average vehicle in Europe was about 10 years old[5]. A robust overhaul of existing legislation on repair and maintenance information provisions is needed to ensure a level playing field for Independent Operators.

***Independent Operator***
*A natural or legal person other than an authorised dealer or repairer, who is directly involved in the repair and maintenance of the vehicles*

Motorists need a clear framework on vehicle data, which will be at the heart of many services in the future. A specific framework on data ownership would give users the clarity they need about their data rights and would truly empower them.

## Adapt existing framework of access to vehicle data to technical progress

### 1. Legislative framework

Current European legislation creates a level playing field today by allowing non-discriminatory access to repair and maintenance information. The existing framework is composed of the Block Exemption Regulation (EU) No 461/2010 and Regulations 715/2007 and 692/2008 on type approval of motor vehicles with respect to emissions. The system foresees a fair access to vehicle data in the same scale and in the same timeframe for independent operators as brand repairers. This framework covers the basics to ensure competition and choice in a world where physical access to the vehicle is needed for monitoring, diagnostics and repair.

Increased connected features will radically change that landscape. Connected vehicles can offer real-time monitoring of the vehicle's electronic control units. This allows for predictions if and when a certain component will fail, perform remote diagnostics and sometimes even remote repair. Vehicle manufacturers offer these services to users based on contracts: remote sourcing of vehicle data allows for improved support of repair and maintenance.

[4] FIA Region I, "What Europeans think about connected cars", Brussels, January 2016
[5] http://www.acea.be/statistics/tag/category/average-vehicle-age

Connectivity should lead to a decrease of breakdowns, anticipatory maintenance for better reliability, reduce costs and increase convenience for users. So far, there is no agreed technical interface upon which third parties could remotely access data and thus be able to offer the same services.

The mandatory implementation of eCall should trigger an in-depth revision of the framework, which has delivered real benefits for users so far, to adapt it to the connected world. The revision of the framework should ensure that consumers have the right to choose from a variety of safe functionalities and products at the best price.

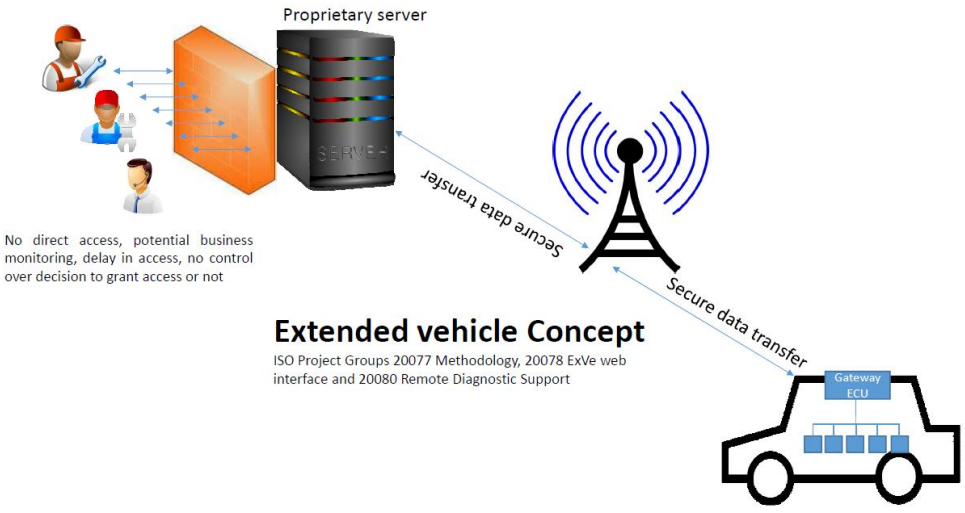
We therefore call on the Commission to:

- Issue a legislative proposal on an "standardised, secure and open access platform", on which eCall should be based as requested in Regulation 2015/758/EU
- Adapt the type approval provisions on access to repair and maintenance information to include fair and non-discriminatory remote access to real-time vehicle data
- Foresee a neutral certification scheme for in-vehicle applications based on safety, security and data integrity requirements to create a level playing field between vehicle manufacturers, authorised and independent economic operators. Special attention should be paid to the risk of driver distraction
- Ensure that the vehicle owner or driver can opt in or out of any data transmission, as personal data must be based on consent by adopting specific rules on data ownership

## 2. Possible technical architectures defined by the C-ITS platform

### o Extended vehicle

Vehicle manufacturers currently propose the **Extended Vehicle concept**, a set of international standards (ISO), which foresee the access to a limited amount of data via data servers solely under their control. Launched in 2015, the ISO standard is expected to be finalised by 2018.

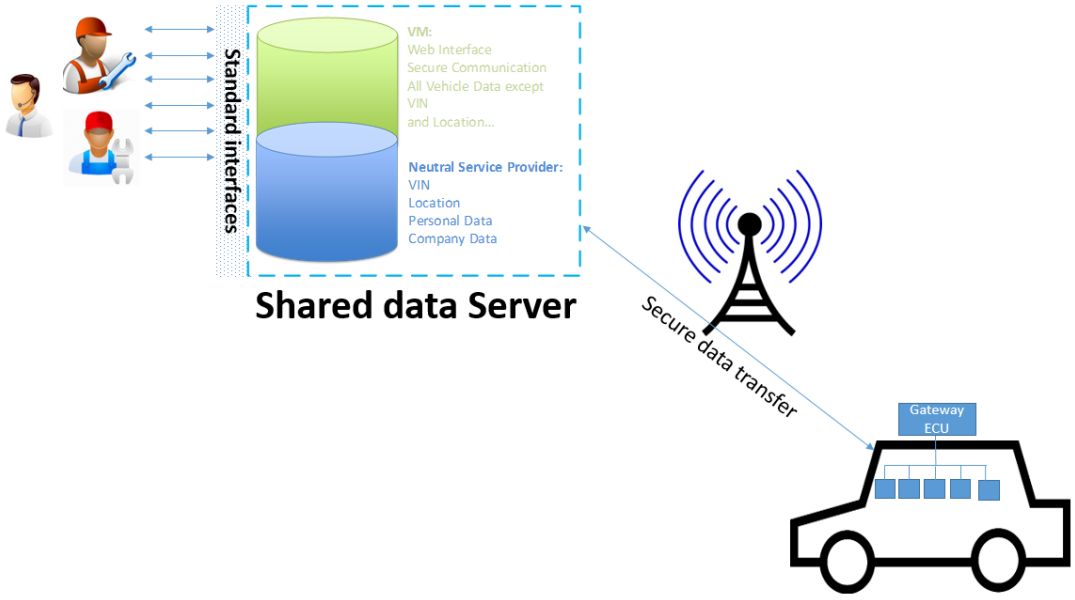


Once finalised, manufacturers will have the possibility to implement this standard on a voluntary basis. In this technical architecture, all vehicle data is sent to a proprietary server under the control of the vehicle manufacturer. Vehicle manufacturers would then grant access to a limited set of data, as described by law, to independent operators. Any additional data exchange – even with explicit motorist consent – would be subject to business-to-business contracts for any existing of future services. This would limit the consumer's choice of any future service providers to a list of manufacturer chosen suppliers.

Vehicle manufacturers get direct, full and privileged access to vehicle data. They can discretionarily decide whether or not an independent operator gets access to real-time data without justifying their choice. This will lead to a situation where innovation is held hostage: some applications may be made unduly burdensome or expensive and therefore never materialise, despite high motorist demand. In addition, all vehicle data would necessarily transit via manufacturer servers, which would give them a powerful tool to directly monitor competitor business. They would also benefit from a privileged access to the customer's dashboard and personal information. In this scenario, use cases for connectivity would be strictly limited to existing services. Innovation and competition would be significantly limited: this solution is therefore far from optimal from a user's perspective.

- Shared data server solution

Some of the shortcomings of the Extended Vehicle proposal could be addressed by entrusting the running of the server to a neutral third party. In a transitional phase, vehicle data would still transit via a server. The server would be divided to ensure a differentiated access to two users: the vehicle manufacturer and a neutral server provider. The partition would allow vehicle manufacturers to access anonymous data and secure communication. The neutral service provider running the server would give access to vehicle data to various providers, based on informed driver consent.



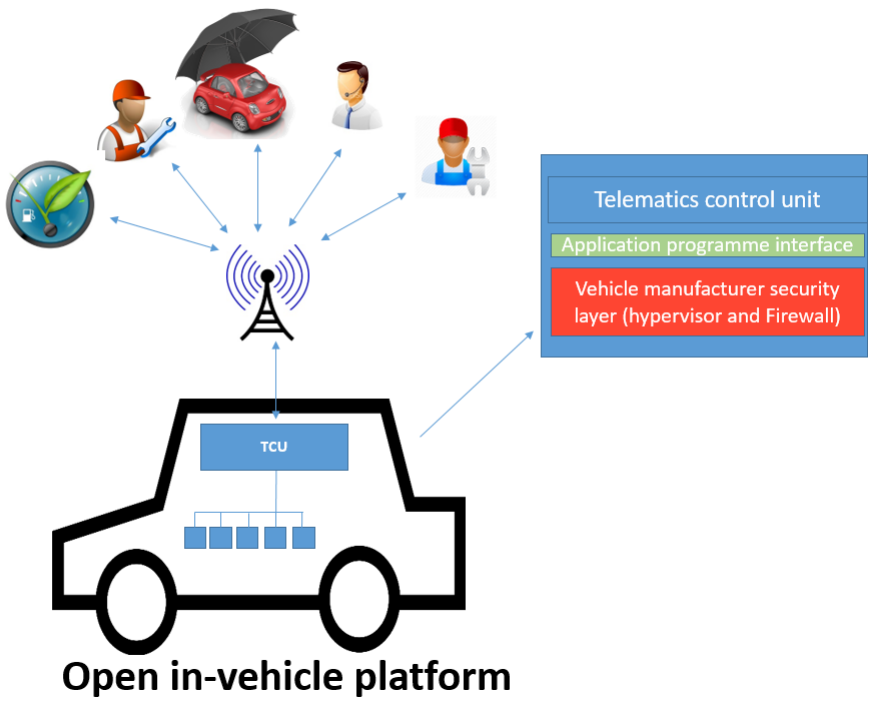
The neutral service provider would be commissioned and controlled by a consortium representing interested stakeholders. In order to allow a fair and secure access to sensitive vehicle data, independent operators and vehicle manufacturers have set up a Forum for Access to security related data, called SERMI. The SERMI association defines an accreditation process to allow access to security related data. Any decision on the scheme needs unanimity of stakeholders. This Forum could inspire a governance model for the shared server.

Therefore, the FIA calls for:

- The Commission to ensure the neutrality of a server solution by mandating a mixed consortium, representing business interests but also those of the consumer to run the server and certify applications in a transitional phase. This server should be based in the EU to ensure the necessary safeguards for the enforcement of European data protection legislation.
- Stakeholders to work out criteria to be fulfilled by applications in order to ensure driver safety and security as well as the integrity of the data being sent and processed. The neutral SERMI consortium could be used to draft the criteria and certify applications before they are made available to drivers.
    - Open in-vehicle platform solution

Ultimately, the in-vehicle architecture should be adapted to include an on-board application platform. This platform could support different functionalities directly from the dashboard.

This evolution can already be noted with the integration of various phone operating systems in-vehicle via MirrorLink, Apple Car Play or Android Auto. Today, this interface can already provide access to navigation, music and phone apps via a smartphone while driving. The apps run on the smartphone, but the driver sees them on the dashboard display and hears audio via the car's speakers.



Technically, the vehicle would comprise a security layer including a hypervisor[6] and firewall designed by the vehicle manufacturer. The hypervisor would be responsible for allowing different operating systems to run and manage priorities according to pre-set boundaries.

Applications would be granted a certain level of priority depending on how much they rely on in-vehicle resources and their level of importance for safety. An emergency functionality such as eCall would for example take precedence over applications such as infotainment or preventive maintenance.

The application programme interface would then set out the protocols for building applications. These protocols would be made available to operators wishing to design applications. Once certified by a consortium of stakeholders, applications would be made available to drivers directly on their dashboard. This solution would lead to high innovation and competition and increase consumers' choice.

**The FIA calls on the Commission to ensure neutrality by design for telematics platforms by mandating an open and secured approach allowing consumers to freely choose safe applications.**

## Data protection & Data ownership

90% of motorists say that data emitted by their vehicles either belongs to the vehicle driver or to the owner. Existing European legislative framework on data protection does not foresee a data ownership per se. The framework only sets out rules according to which personal data must be processed. It includes the right for a data subjects to access, modify or delete personal information and safeguards on data transfer and processing.

In line with previous findings from WP 29[7], the C-ITS Platform report concludes that most data derived from a vehicle should be deemed personal. All vehicle data transmitted must be processed according to the principles of data protection. FIA Region I research[8] shows that today, data gathered by connected vehicles is stored either up to its deletion in the manufacturer's workshop or over the component's life time. Data on the driver profile, mileage, liquid levels up to system faults and personal data from a Bluetooth connected phone is gathered.

Some applications may be mandated by law if they have a proven benefit for society as a whole, such as eCall. However, the vast majority of applications will need to be based on the users informed consent for the sending and processing of their data. When asked, motorists indicate that consent should be given either for a given time (58%) or per ride (25%)[9].

[6] A hypervisor also called a virtual machine manager, is a programme that allows multiple operating systems to share a single hardware host (the physical vehicle)
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf
[8] FIA Region I technical tests performed on a conventionally-fuelled and an electric vehicle: http://www.mycarmydata.eu/
[9] FIA Region I survey carried out in 12 countries, 1000 replies per country: http://www.mycarmydata.eu/wp-content/themes/shalashaska/assets/docs/FIA_survey_2016.pdf

Consumer free choice can only be ensured via equal access to in-vehicle data and a neutral certification scheme for applications. Motorists should have a free choice between a whole range of safe and secure applications throughout the lifetime of their vehicle. They should be able to conveniently deactivate any chosen application themselves via the vehicle dashboard.

**FIA Region I therefore calls on the Commission to adopt specific rules on data ownership and guidance on personal data use to complement technical measures so that citizens are given control over the data their vehicles produce.**

## Fédération Internationale de l'Automobile (FIA) Region I office

FIA Region I is a consumer body representing 107 Mobility Clubs and their 38.5 million members from across Europe, the Middle East and Africa. The FIA represents the interests of our members as motorists, riders, pedestrians and passengers. FIA Region I is working to ensure safe, affordable, clean and efficient mobility for all. Learn more at www.fiaregion1.com