1991
2016
ACEA
European
Automobile
Manufacturers
Association

ACEA Strategy Paper on

Connectivity

APRIL 2016

ACEA

European
Automobile
Manufacturers
Association

EXECUTIVE SUMMARY

Connected and automated driving will revolutionise individual mobility within the space of just a few years. It will offer new potential for safe, efficient, comfortable and environmentally-friendly transport but equally create new areas of business with new players that will impact existing automotive business models.

To optimise this development for the benefit of society, the necessary conditions must be created now. Public authorities should take a holistic view, pool all available expertise and coordinate their activities carefully. The automotive industry, vehicle manufacturers as well as suppliers, stand ready to cooperate with road operators, telecommunications operators, ICT companies, third-party service providers and with public authorities to ensure that the necessary cross-sector industrial policies are adopted as a matter of urgency. While some matters require an EU response, dialogue and cooperation with the US and Japan should be envisaged to prevent different regions from adopting fundamentally diverging policies.

Policy matters that need addressing include fair competition, data protection and privacy, cybersecurity, road safety and liability. The interest of third-party service providers and new competitors in accessing vehicle data and using them for commercial purposes is an issue that requires particular attention. The EU should establish a regulatory framework for access to vehicle data that takes account of the fact that vehicle manufacturers invest heavily in the ability of vehicles to generate data and are ultimately responsible for ensuring the vehicle's safety and integrity as well as the protection of the user's personal data and privacy.

In the absence of an adequate legal framework, a very small number of companies based outside the European Union could rapidly acquire the same dominant position in the area of in-vehicle services as they already have in the field of data processing, search engines, online services or smartphones. Should this occur, vehicle manufacturers risk being left with stranded investments, a loss of company know-how, commercial secrets and industrial property rights. The consequences for the competitiveness of the auto industry, service providers and for job and value creation in Europe would be significant.

The best technical approach to ensuring safe and secure third-party access to vehicle data is by means of the 'extended vehicle' concept, which provides access to vehicle data in accordance with clearly defined technical, data protection and competition rules through various interfaces and means of data storage, embedded and/or off-board, managed by the vehicle manufacturer. The extended vehicle is currently being standardised within ISO.

1. BENEFITS OF CONNECTIVITY

Connectivity creates social, economic and environmental benefits

The vehicle of tomorrow is connected and digital. Mobility is taking on a new dimension – through communication between vehicles, between vehicle and infrastructure, and between vehicle occupants and their environment – but also with occupants accessing their own data and media, for example, through online services. In-car internet access opens up a wide range of new applications and services.

Automatic information sharing between road users in real time offers significant potential for further improvements in road safety and resource-efficient, time-saving transportation. Vehicles, their operators and their occupants are aware of traffic-light phases and roadworks, warned by vehicles ahead of hazardous situations, such as accidents, obstacles or icy roads, and are able to respond accordingly. Traffic systems linked intelligently to various modes of transport enable customised intermodal mobility solutions. Public infrastructure can use these new technologies to connect vehicles with available spaces to make parking management more efficient and reduce traffic from vehicles looking for somewhere to park.

Comprehensive vehicle connectivity offers huge economic and ecological potential with sizeable social benefits:

- Major improvements in traffic system efficiency through optimised utilisation of road infrastructure capacity; traffic congestion avoidance using dynamic route guidance.
- Long-term energy savings on the roads, with a corresponding reduction in emissions through road/traffic-adjusted (adaptive) operating strategies (eg engine control).
- Broad-ranging e-mobility market ramp-up through close networking with infrastructure and optimisation of charging behaviour.
- Efficient networking between different modes of transport through individually customised, intermodal mobility offerings.
- Significant increase in freight transport efficiency through optimal utilisation of commercial vehicles by means of fleet management (eg by avoiding empty runs).
- More effective hazard recognition and prevention through anticipatory and adaptive driving with potential reduction in the number of road fatalities and accidents.
- Recognition of emergency vehicles with special privileges and rights of way/using emergency signals (cross traffic, emergency lane).

2. DATA IS THE BASIS FOR CONNECTIVITY

Data is the currency of the digital world

Most vehicle data is generated within the vehicle control units. This technical performance data 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 may vary according to manufacturer, vehicle type and equipment. Most of this data is volatile. However, some operating data is recorded and stored by for quality assurance purposes and the fulfilment of statutory product monitoring obligations.

Vehicle manufacturers already offer a wide variety of data-based assistance, information and other services, enabling customers to enjoy greater comfort, safety and enhanced efficiency. These services provide a broad range of information, such as real-time traffic warnings; modal or intermodal route guidance; localised weather, road conditions and addresses for hotels, restaurants, ATMs or electric charging stations. Safety-relevant functions such as eCall, braking assistance and lane departure warning are also available in individual cases. In the commercial vehicle sector in particular, the evaluation of telematics data enables customers to drive more efficiently and therefore more economically.

With respect to service, drivers are notified of upcoming service needs, electric vehicle range or the location of the nearest charging station. They can receive status information for key wear parts such as brake pads and engine oil. They can also call up entertainment features and, in many cases, make appointments, reservations and bookings online from their vehicle. New services and applications are being added all the time.

With the rising volume of in-vehicle data, third parties are increasingly interested in accessing and using vehicle data. In addition to providers such as garages and breakdown services, insurance companies (eg for pricing based on mileage or driving profile), financial and fleet service providers, road infrastructure operators (tolls), entertainment and travel service providers, social networks, and search engine operators and advertising marketers, are all interested in the unrestricted commercial exploitation of vehicle data. At the same time, our customers expect to be able to access their usual services in the vehicle.

Giving any third party unlimited and uncontrolled access to vehicle data would create serious issues of personal data protection, security, safety, liability and competition. These issues need to be addressed urgently.

3. PROTECTION OF PERSONAL DATA IS PARAMOUNT

No data sharing without contract or consent

Some of the data that are processed in vehicles or in relation to connected services are definitely relevant in terms of data protection and privacy. Many other data are primarily of a technical nature. Their relevance in terms of data protection and privacy depends on the extent to which they can be combined with other data that may permit the identification of a natural person.

Vehicle manufacturers are committed to providing our customers with a high level of personal data protection. This is why on 16 September 2015 the member companies of ACEA have adopted a statement which sets out the principles of data protection that they intend to respect in relation to the connected vehicles and services that they will put on the market in the European Union themselves or through their affiliated companies.

The foundation for the responsible handling of personal data is transparency and self-determination for the user. Vehicle manufacturers aim to design their vehicles and services so that where possible customers can choose whether to share personal data. This means that personal data will be shared with third parties who use these data for their own commercial purposes only on the basis of a contract, with the consent of the customer or to comply with legal obligations. Furthermore, customers will be able to de-activate the geolocation functionality of their connected vehicles and in the connected services that are offered except where geolocation data must be processed to comply with contractual or legal obligations (for example: emergency call).

This also applies in cases where the vehicle manufacturer transfers personal data to service providers entrusted with performing the service in question. Where data processing is outsourced, contractual safeguards are put in place to protect personal data.

Where vehicle manufacturers do not control personal data processed by unaffiliated third parties who provide applications or services through the communications platforms in the vehicle, these service providers will be encouraged to apply the same principles.

4. NO DATA ACCESS WITHOUT SECURITY, SAFETY AND LIABILITY

A vehicle is not a smartphone

Nor is it a PC that can be rebooted if a problem occurs while driving. Motor vehicles contain highly complex, technically-sensitive systems that must meet high technical and legal standards. These systems are developed and monitored by the vehicle manufacturer in strict compliance with road safety regulations, product safety and quality standards – in some cases, far beyond what is legally required. Ultimately, vehicle manufacturers are responsible for the safety and integrity of their products.

Security & safety are the top priority

To protect the vehicle's up to 100 control units from hacking, manipulation and malware, manufacturers are constantly refining software and hardware structures within the vehicle. By separating control circuits and using the latest encryption methods – from the vehicle's telematics interface all the way to the vehicle manufacturer's backend – combined with various security tests, manufacturers are able to provide state-of-the-art protection for safety-critical functions in line with the latest technological standards.

As the technological possibilities for illegal intervention also continue to evolve, vehicle manufacturers must respond promptly to emerging technical risks and immediately gather all available information from third parties. For example, vehicle manufacturers are setting up an automotive Information Sharing and Analysis Centre (ISAC) to share information about the latest security threats and possible countermeasures between vehicle manufacturers, suppliers, mobile telecommunications operators and possibly ICT companies. While this centre is located in the United States, its scope is global – as are cybersecurity threats. We believe this type of cooperation is more effective in combating cyberattacks than setting minimum requirements for hardware and/or software since such requirements will not be adequate to deal with a threat that is evolving continuously.

Vehicle manufacturers are fundamentally willing to share selected vehicle data with third parties provided this occurs in a way that meets strict requirements for road and product safety, as well as data security, and does not undermine their liability.

This implies that any risk of attack or access to the vehicle's security electronics from external systems or software programs that are not under the vehicle manufacturer's control should be avoided. Even uncontrolled third-party access to vehicle functions or data that are not directly security-relevant could lead to secondary 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.

It should be understood that direct third-party access to vehicle functions would facilitate hacker attacks since every new external data interface increases the number of potential targets and entry points. An uncontrolled flow of data or parallel data connections could also hamper data bus systems or allow central functions to be manipulated and brought to a standstill (for example, component reset or vehicle immobilisation).

Additional safety risks in terms of driver distraction could arise if external third parties are granted uncontrolled access to the vehicle's on-board systems, user interfaces and function displays, for example through apps or additional control units. Vehicle and traffic-related information displayed on a central on-board monitor during driving must meet the vehicle manufacturer's quality and safety criteria and be compatible with their systems. Applications visualised in the head-up display, for example, are safety-critical due to broad networking with other vehicle functions and must therefore be centrally developed as part of a consistent operating concept.

No automatic liability for third-party apps

Vehicle manufacturers are unable to accept automatic (incalculable) liability for applications developed by third parties. Nor can vehicle manufacturers be expected to automatically test and approve all applications available on the market (release problem). Certification by the manufacturer is feasible, at least in theory, but would involve substantial costs (testing) and risks (subsequent software modifications, such as write access or security flaws not excluded through certification).

Vehicle manufacturers are not in a position to assume responsibility for or monitor all third-party applications on mobile devices – which would have direct legal consequences for customer product liability and warranty claims, as well as for data protection and security of user data. Furthermore, the vehicle manufacturer has a legitimate interest in protecting its technical know-how, for example relating to new models or technologies developed within the company (intellectual property). The security of this information could no longer be assured if vehicle systems were open to third parties without restriction or control.

For this reason, third-party applications that interact with the vehicle should only be developed and approved in cooperation with the vehicle manufacturer to eliminate security, data protection and product liability risks.

This will also facilitate the work of regulatory and supervisory authorities, insurance companies and infrastructure managers who will continue to deal with a single, central partner – the vehicle manufacturer – on approval-related and data protection matters, instead of with a large number of different service providers, many of whom are based outside the EU.

Liability of third parties

In the world of connected and automated vehicles, it should be clear that liability for defects or incidents will not always lie with the manufacturer of the vehicle, the components or the software. Particularly in the case of V2X communication, the liability of road operators, mobile telecommunications operators, internet providers and third-party service providers can be at stake. We believe policy makers should as a matter of urgency clarify the degree to which and the conditions under which each of these parties would be liable.

5. NO DATA ACCESS WITHOUT COMPENSATION

Commercial service providers should pay usage fees

As providers of mobility services, vehicle manufacturers have invested consistently and extensively in vehicle electronics, vehicle safety, IT systems architecture, secure data processing capacities, data transfer technology and intellectual property. Without this systems infrastructure inside the vehicle, vehicle connectivity and communications with external providers and mobile devices would not be conceivable. Furthermore, manufacturers constantly invest in operation (including 'over the air' data transmission via the mobile network), infrastructure projects, technical configurations and software programs to meet the highest data protection and data security requirements. Also, they ensure that data that varies from one vehicle manufacturer to another can be translated into flawless workable formats for apps and services. Finally, they operate and maintain and the servers that enable third parties to access vehicle data (extended vehicle).

Considering that third parties who use this infrastructure and communication channels generally do so to offer commercial services to vehicle owners and drivers, a fair competitive environment implies that they should compensate vehicle manufacturers for the development, operation and maintenance costs they incur by paying usage fees.

The same should apply when vehicle manufacturers perform services for app developers. For example, to enable third parties to present their offerings under technically secure and commercially competitive conditions, a number of vehicle manufacturers have developed an app framework, which provides a platform for third parties to offer their own value-added services with a very diverse range of content. If vehicle manufacturers perform services on behalf of a third party during app development, for example functional or security testing, de-identification or encryption of personal data, certification or authentication, they should be paid for these services.

A separate discussion should take place as to the conditions under which safety-critical data (information about icy roads, traffic congestion, etc) would be forwarded to a central point so that it can be used for traffic planning and road safety purposes.

6. A MATTER OF COMPETITIVENESS

The future competitiveness of the European automobile industry depends on the ability of vehicle manufacturers to obtain a reasonable return on the investment they are making in connectivity. In today's digital world, the industry's main competitors in this field are not the non-European vehicle manufacturers or the independent after-market operators. It is a limited number of large, mostly non-European internet and ICT companies who are world-leaders in data storage and processing and who see enormous potential for internet-based services in relation to connected and automated vehicles.

There is no doubt that the growing connectivity of motor vehicles, together with their progressive automation that will give drivers more time to carry out activities other than driving when they are in a vehicle, will create a potential additional market volume for internet-based services almost equal to the current market for internet services. Today, approximately 2.4 billion people spend an average of 20 minutes online every day (800 million hours per day). That same amount of time is spent in the car (800 million cars, with an average driving time per day of one hour).

A number of new players have become involved in developing highly automated vehicles, primarily with the aim of exploiting the business potential. They are less interested in creating their own vehicle offering than in acquiring potentially 'indispensable' capabilities at the interfaces between the vehicle and its surroundings, thereby gaining direct, comprehensive access to user data. Evaluating this data enables them to continuously improve their own offering or, if the data is forwarded or sold, to allow other interested parties to use it.

The clear aim of these new competitors is to obtain direct access to in-vehicle data in return for provision of map information and usage of their internet services (and search functions, in particular) so they can use this data directly or forward it to third-party providers with a view to offering commercial services. Their argument is that customers want to use the same services in their car as on other devices in an identical form – making the integration of corresponding products in the vehicle essential to maintaining future competitiveness.

The free flow of data risks creating an oligopolistic market structure

The risk is that this will this lead to a very small number of companies based outside the European Union acquiring the same dominant position in the area of in-vehicle services as they already have in the field of data processing, search engines, online services or smartphones. Should this occur, vehicle manufacturers risk being left with stranded investments, a loss of company know-how, commercial secrets and industrial property rights. Policy makers therefore need to ask themselves whether it is in the interest of genuine competition, for example, to allow map and infrastructure information from a single or a limited number of companies to be linked in an integrated business model either to the direct offering of all other possible services provided by the same company or to the transfer of data to third-party providers.

The rapid digitalisation of the automotive sector implies that automotive companies need to develop and sustain new business models to rival those of their emerging competitors. The critical success factor for these business models is not technology or design but data.

Thus, it is crucially important that legislators take the economic value of data into account when developing and setting policies of data ownership and data use. Policy makers must ensure balanced access to commercially usable vehicle data. Proponents of the 'free flow of data' may consider that making as much data as possible to as many market participants will promote competition, stimulate innovation and lead to additional job and value creation in the EU. However, the opposite might be true.

In reality, much will depend on how third parties will be able to access data. A current legislative initiative in several US states would enable customers to provide one-time general consent for all agreed data generated with a third-party supplier to be transferred to that party – in effect, without the involvement of the manufacturer. The explicit argument here is to encourage competition for mobility services. However, the opposite effect is likely: this move would strengthen a very small number of firmly-established central system suppliers in the field of online services, who would then gain control of both the interface between vehicle user and manufacturer and between user and third-party providers. Thus, they could use the wide-ranging combination of all vehicle-related services with existing offerings to expand their dominant position and hinder effective competition.

In our view, a better and more balanced alternative would be to provide third-party data access through an agreement with the vehicle manufacturer, who would undertake to transfer data and ensure that legal requirements toward the customer are fulfilled.

7. THE EXTENDED VEHICLE PROVIDES THE BEST TECHNICAL SOLUTION

A standardised solution that is safe and secure

The ‘extended vehicle’ provides the best means to grant third parties access to vehicle data they might legitimately request in order to offer services to the vehicle owner or driver while simultaneously enabling vehicle manufacturers to ensure vehicle safety, product monitoring, IT security and data protection compliance.

An extended vehicle is understood as a physical road vehicle with external software and hardware extensions for some of its features. These extensions are developed, implemented and managed by the vehicle manufacturer. The vehicle manufacturer is fully responsible for the communication among the various parts of the extended vehicle, especially between the internal and external software and hardware components.

The extended vehicle offers open yet protected access interfaces for the provision of services by vehicle manufacturers or third parties. The interfaces need to be designed and implemented in such a way that access to the extended vehicle does not jeopardize security, safety, product integrity, data privacy or any other rights or legal obligations.

Depending on the purpose for which access is sought, the extended vehicle can be accessed through:

- The on-board diagnostics (OBD) interface for emission control and legally prescribed diagnostic services and the fleet management systems (FMS) interface for heavy-duty vehicles (based on the industry standard);
- A web interface: for example, for remote diagnostic support (RDS) and for remote fleet management systems (rFMS) for heavy-duty vehicles (based on the industry standard);
- An interface for safety-related applications in the field of cooperative intelligent transport systems (C-ITS) such as CAM and DENM messages.

A series of standardisation projects dealing with the extended vehicle and the extended-vehicle web interface have been approved and launched by ISO in 2014. Each of the projects has a specific purpose: ISO 20077 relates to the extended vehicle methodology, ISO 20078 to the web interface and ISO 20080 to the provision of remote diagnostic support.

The extended vehicle also offers a secure connection between an in-vehicle system and the manufacturer’s central server, which protects all data transfers from unauthorised disclosure and manipulation and provides third parties with read access to securely transmitted vehicle data as needed, with the same quality and scope of data available as for the vehicle manufacturer's service organisation. To use this data, quality standards must be in place, network stability must be assured and information regarding data integrity must be available.

Access should be given to specific data sets

For these reasons, it is essential to form vehicle data categories with different access rights according to the functionality required. These categories should differentiate between areas such as intellectual property of the manufacturer, safety-critical applications, telematics and infotainment applications. Each of these applications has different requirements that call for differentiated solutions and access rights.

Certain datasets from defined data categories would be made available to third parties with appropriate authorisation in accordance with ISO 20077. The scope of third-party access to vehicle data determined according to sub-sets of data or clearly defined access rights (for example, according to selection and number of apps). Data access would be granted on the basis of user consent and commercial agreements between the manufacturer and third-party providers.

Using the 'extended vehicle' concept would have the following advantages:

- The vehicle manufacturer controls and secures data transmission channels (access to the vehicle) to ensure optimal vehicle integration, data security and data protection, and secure the power network and system stability (system expertise).
- In particular, the security of the interface between vehicle and manufacturer backend, which is part of the extended vehicle, is very high in a 1:1 relationship. .
- If a new system security risk emerges, emergency intervention can be initiated more effectively and security software updates performed centrally and reliably by the manufacturer 'over the air' (versus recall of each individual vehicle).
- Vehicle manufacturers remain able to support customers in the event of a malfunction, since they are familiar with the entire vehicle system and manufacturer backend and can perform diagnostics. This would not be possible with a local data interface in the vehicle.
- Standardised provision of vehicle data to service providers identified by the customer via a defined interface minimises development effort for third parties, thereby promoting new and innovative services throughout the automotive sector
- Smaller providers, in particular, benefit from being able to call up precisely-defined standardised data packages, which they can interpret and use without any further manufacturer-specific know-how, ie with minimum development and investment (for example in secure data transfer channels) on their part. Simple usage fees for maintenance

and operation of standardised server interfaces – in place of substantial investments in model-specific reengineering, parallel application development and duplicated protection – make it easier for third parties to enter the market.

- Providers selected and authorised by the customer are granted read access to specific vehicle data. Interfaces are designed to exclude write access to safety-related and mission-critical vehicle data. The vehicle bus load cannot be modified by third parties beyond the specification limits.
- Legal data protection requirements can be implemented much more effectively and transparently for the customer or controlled by customers themselves. Customers decide which personal data should be made available to which providers for which applications and authorise the vehicle manufacturer to grant selected third parties access to selected data packages. Customers choose their own configuration and always know when which data is transmitted to which service provider.
- There is no way for unwanted services, offers or advertising to reach the vehicle or the customer. Customer consent is the basis for all data-based value-added services.

1991
2016

ACEA

European
Automobile
Manufacturers
Association

ABOUT ACEA

ACEA’s members are 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, Volvo Group. More information can be found on www.acea.be.

ABOUT THE EU AUTOMOBILE INDUSTRY

- Some 12.1 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's manufacturing employment.
- Motor vehicles account for €396 billion in tax contribution in the EU15.
- The sector is also a key driver of knowledge and innovation, representing Europe's largest private contributor to R&D, with €41.5 billion invested annually.

European Automobile Manufacturers' Association – ACEA
Avenue des Nerviens 85 | B-1040 Brussels | www.acea.be
T +32 2 732 55 50 | M +32 485 886 647 | F +32 738 73 10 | info@acea.be | @ACEA_eu