Chapter 31
Competition, Security, and Transparency: Data in Connected Vehicles

Karsten Schulze

Abstract State-of-the-art cars are increasingly becoming computers on wheels, constantly collecting, storing, and transmitting data. This goes hand in hand with better market opportunities for certain service providers with access to the data.

There is still no clear legal regulation on who the customer can share their data with—and in what way—nor how transparency and security can be guaranteed for such data in the process. Without legal regulation of data access, there will be no way to ensure a level playing field among providers and freedom of choice for consumers in the future.

Three basic principles apply to the access to vehicle data:

- Third-party service providers should be able to develop new services without depending on car manufacturers.
- Independent service providers, such as independent workshops, insurers, and automobile clubs, should be able to reach customers through the same channels as the vehicle manufacturers.
- Vehicle manufacturers should not be allowed to monitor vehicle users or the service providers selected by vehicle owners.

31.1 Data in Connected Vehicles

Digital transformation is having a far-reaching impact on the automotive sector. Technological development in connected driving and new online business models will thoroughly reshape mobility. Sensors, digital data processing, and data communication enable new functionalities which make driving safer, more comfortable, and more efficient (see Fig. 31.1).

This generates ever-increasing data volumes, which are gaining more and more economic importance. After all, the evaluation of the data will allow service

K. Schulze (✉)
Allgemeiner Deutscher Automobil-Club e.V. (ADAC), Munich, Germany
e-mail: Karsten.schulze@adac.de

© The Author(s) 2022

B. Otto et al. (eds.), *Designing Data Spaces*,
https://doi.org/10.1007/978-3-030-93975-5_31

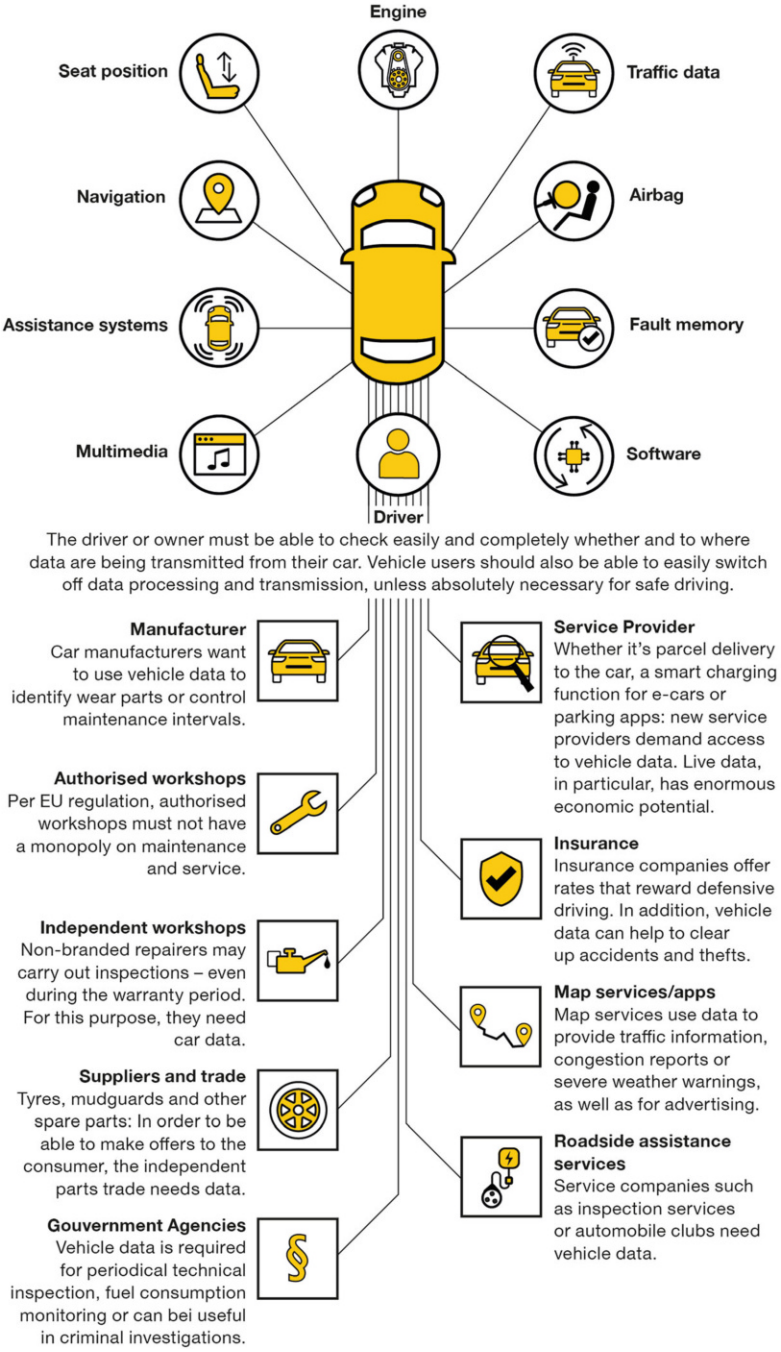

Fig. 31.1 Vehicle-generated datasets and potential uses

providers to optimize their car-related offers in the future. This goes hand in hand with better market opportunities for certain service providers with access to the data.

Data from connected vehicles are specially protected by law as personal data [1]. It is neither relevant whether the data comprise technical information nor whether the data are vehicle-generated or provided by the customer—in all of these cases, the data contain information relating to an identified or identifiable person as specified in the General Data Protection Regulation. However, there is still no clear legal regulation on who the customer can share their data with—and in what way—nor how transparency and security can be guaranteed for such data. Without such regulation, those who have initial access to the data will prevail in the market. In our case, the vehicle manufacturers have that privilege. As a result, they have a gatekeeper position in the market and can control the competition. In the medium to long term, this will have a negative impact on the market as far as the diversity of offers and suppliers and consequently also prices and freedom of choice for consumers are concerned. I take the view that the proposals of the automotive industry for regulating data access are not suitable to eliminate this gatekeeper position.

31.2 Plans of the Automotive Industry Thwart Competition

According to a Europe-wide survey conducted by the FIA (Fédération Internationale de l'Automobile), 78 percent of vehicle users want to choose their own service providers, e.g., workshop, insurance company, or roadside assistance provider [2]. To ensure this, vehicle manufacturers suggest that access to vehicle data be granted via the Extended Vehicle (ExVe)/Neutral Server ("NEVADA Share & Secure"). According to this concept, the vehicle data are made available via the manufacturers' own servers, and access by third parties is monitored and subject to a fee. In this way, the manufacturer takes on the function of both a rights administrator (who gets access?) and a resource provider (which data and functions are made available on what terms?). Currently, the vehicle manufacturer decides on data access solely on the basis of business relations between the companies concerned, which gives the manufacturer a considerable competitive and negotiating edge. For example, consumers who want to share their data with a third party via Nevada will hardly be able to do so if the third party does not conclude B2B contracts with the manufacturer. This concept enables manufacturers to find out which third-party providers access vehicle data, as well as when and how often. As a result, the manufacturers find out a lot about the business activities of other market players. In addition, direct access to the customer in the vehicle via the on-board system is reserved for manufacturers; the ExVe/Nevada concept does not provide such integration for independent market participants. In this concept, therefore, the consumers' right to transmit their data to service providers freely selected by them without prior filtering of offers is hardly enforceable.

Against this background, a broad spectrum of third parties involved in the market, including, e.g., car repairers, technical service providers, as well as ADAC, reject the

concept, because access to data must not depend on the goodwill of a manufacturer toward its competitors.

Therefore, I advocate a swift adaptation of the European legal framework to take account of the digital transformation in the passenger car sector: without legal regulation of data access, there will be no way to ensure a level playing field among providers and freedom of choice for consumers in the future.

31.3 Quick Regulation of Data Access Needed

In 2016, according to industry figures, sales of parts in the automotive aftermarket amounted to €20 billion in Germany alone. Labor costs were another almost €11 billion [3]. Access to vehicle data and users is thus a key factor for the competitiveness of many companies operating in this market. As connectivity increases, data access bears more and more economic relevance, and a swift political decision on the regulatory framework is therefore urgently needed. A FIA-commissioned economic study shows without pro-competitive regulation, independent service providers across Europe might face a loss in revenue of €15 billion by 2025. By 2030, this sum could rise to €33 billion due to further increasing degrees of connectivity [4]. In order to benefit from the full potential of connected vehicles and digital transformation in general, access to vehicle-generated data is essential. This is the only way for third parties to offer car-related services, thus ensuring the consumers' freedom of choice and competition in the long term. Political decision-makers must therefore promptly create a level playing field allowing all stakeholders to act on an equal footing. In fact, the following disadvantages are conceivable, to the detriment of competitors and consumers:

Unnecessary costs	Restrictions	Delays	Surveillance
Vehicle manufacturers charge independent third-party providers for access to vehicle data In doing so, the manufacturers make money from data which the consumer has generated and whose added value should therefore also benefit the consumer—e.g., in the form of attractive and inexpensive offers	Independent service providers could be denied access to relevant data This would hamper or altogether preclude the development of innovative services	Data would be available to third-party providers only with some delay This would make the services they offer less attractive compared to those offered directly by the manufacturers or by companies preferred by them	The server-based data access concepts proposed by the manufacturers allow them to obtain a comprehensive market overview They provide manufacturers, who are also market participants, with a comprehensive overview of their competitors' business models and relationships. This is detrimental to competition

Without regulating access to vehicle data to give all market players equal opportunities and consumers authority over their data, there is a risk of market imbalances in very specific cases. Below are some examples.

Maintenance and repair: Many consumers today exercise their option to have inspections and repairs carried out by independent workshops which are more affordable than service providers authorized by the manufacturers. In the future, manufacturers could make offers to the user directly in the vehicle – more price-sensitive customers would receive a discount, and appointments would be synchronized directly with their smartphone diary. Granted: that sounds convenient. Who would then still bother inquiring about other offers? However, if not every supplier has the same opportunities to approach the customer, competition will be eliminated in the long term. This will lead to rising prices.

Insurance: More and more consumers are opting for telematics tariffs to obtain discounts on their car insurance. For this purpose, the insurer assesses the driver's style on the basis of various parameters and calculates the insurance premium accordingly. However, the decision on who receives the data for such insurance offers should not be up to the manufacturer, but only to the users who should have control over their data.

Roadside assistance: While many drivers nowadays opt to use the services of a roadside assistance organization in the event of a breakdown, in the future, manufacturers could directly employ their own network when a breakdown occurs—alerted via the on-board system—and take the car to one of the manufacturer's authorized workshops. This would give car manufacturers a significant competitive advantage in the entire aftermarket, which would indirectly lead to rising prices for the consumer. In this case too, I insist that car drivers must retain full freedom of choice of their service providers.

E-mobility: The vehicle-to-grid function allows electricity from cars to be fed into the grid, thus helping stabilize the power networks. In ADAC's view, the question of how to handle car data is a decisive factor for successful implementation—ultimately, suitable indicative data could help distribution network operators take the potential energy demand into account in their operational planning [5]. Access to vehicle data is relevant for planning when which car can charge and when excess energy needs to be fed into the grid. In this case, too, a regulation for fair and secure data access is essential.

31.4 Ensuring Competition: Clear Rules for Access to Data

I believe that access to vehicle data must comply with the following basic principles:

- Third-party service providers should be able to develop new services without depending on car manufacturers.

- Independent service providers, e.g., independent workshops, insurers, and automobile clubs, should be able to reach customers through the same channels as the vehicle manufacturers.
- Manufacturers should not be able to monitor the vehicle owner/driver or the service providers selected by the vehicle owner.

In the medium term, ADAC considers the open telematics platform (OTP) to be the best solution for fair competition in motor vehicle maintenance and repair services. Only open, standardized, non-discriminatory, and secure access to the data in the vehicle will enable other players to compete with a manufacturer's products and services and to develop new services. The European eCall Type Approval Regulation (EU) 2015/758 already stipulates that in-vehicle eCall systems should be based on an interoperable, standardized, secure, and open-access platform. ADAC supports such a platform granting open access to all market participants, car manufacturers, independent repairers, insurers, automobile clubs, and other authorized third parties, thus guaranteeing customers' freedom of choice and fair competitive conditions. One major challenge concerning the OTP is to ensure IT security for the access over the vehicle's entire lifetime. ADAC is in favor of a central automotive gateway in the vehicle, which controls communication from/to the vehicle and only allows access to third parties authorized by the vehicle owner. The concept was developed by TÜV-IT and represents a viable IT security concept that enables secure and non-discriminatory access to the OTP [6].

In order to avoid competitive disadvantages on the part of independent market participants in the short term, ADAC is advocating the temporary use of a so-called shared server. This concept is technologically comparable to the Extended Vehicle, but the shared server is operated and controlled by a neutral administrator as an independent third party ("data trustee"). It must be ensured, however, that customer and business data from independent third-party providers are neither accessible to nor usable by a market participant. This is the only way to prevent car manufacturers from acquiring a dominant market position, as would be the case under the Extended Vehicle (ExVe)/Neutral Server concept.

In order to create the conditions for technical regulation in the form of an OTP or, on an interim basis, a shared server, data access needs to be codified rapidly at the European level within the type-approval context.

31.5 Ensuring Data Security Even with Competitive Data Access

System deficiencies making vehicles susceptible to, e.g., keyless go thefts or odometer tampering have shown the need for car manufacturers to enhance IT security. A connected vehicle requires a reliable security architecture for optimal protection against safety-relevant interventions by criminal hackers. From my point of view,

data processing in the car must be protected against manipulation and illegal access over the entire life of the vehicle; this should be checked during type-approval.

However, data security is not a viable argument for allowing vehicle manufacturers first access to vehicle data on manufacturer-owned servers. In my view, the question of the security of vehicle data should not be tied to their storage location, but rather to a security architecture that takes into account the risks of connected cars and provides the best possible protection for consumers. Such protection should be based on standards long since common practice in other industries such as the IT sector. This protection standard should be confirmed by an impartial body, e.g., the Federal Office for Information Security (BSI), on the basis of internationally certified processes such as Common Criteria (ISO/IEC 15408).

Against this background, data access must be ensured via an open and standardized platform, since no one has insight into the manufacturers' systems. Communication with the IT systems in the vehicle must also be encrypted via a secure communication interface. Throughout the vehicle's life, car manufacturers must provide safety-relevant software updates and, where required from a technological point of view, implement required hardware adjustments. Owners must be able to rely on safely using their vehicles in the long term.

31.6 Data Transparency and Data Ownership Create Confidence in New Technology

There is also a need for action on the issue of data transparency. Currently, only vehicle manufacturers know in detail what data are generated, processed, stored, and transmitted in cars. I therefore urge that consumers be informed in detail and transparently about the data exchange between their cars and the manufacturers. The vehicle user should be informed and asked for consent when transmitting/receiving data—as is also common practice in the IT sector, e.g., for software updates or fault code transmissions—unless it is a matter of safety-relevant updates. The data privacy agreements which car manufacturers regularly use to obtain new car buyers' consent to unlimited data access will not be sufficient.

ADAC recommends making it mandatory to publish a list specifying all vehicle data collected, processed, and transmitted for each model ("car data list"). An impartial body should be authorized to check this list to ensure that data protection rules are respected. If the manufacturers refuse a voluntary commitment, the legislator should create a legal basis. Except for certain data whose use is required by law (e.g., eCall), the vehicle user should have the option to easily deactivate the processing and transmission of data that is not absolutely necessary for safe vehicle operation.

31.7 Need for Political Action

- Swift creation of a legal framework for access to vehicle-generated data at EU level
- Definition of clear technical specifications for an open telematics platform to safeguard competition in the automotive aftermarket
- Binding regulations obliging manufacturers to guarantee IT security over the entire lifetime of the vehicle
- Creation of a consumer-friendly regulatory environment for data in terms of transparency (car data lists) and the ability to easily switch off data processing and transmission

References

1. Osborne Clark. (2017). *What EU legislation says about car data. Legal Memorandum on Connected Vehicles and Data*.
2. *FIA Region I: What Europeans think about connected cars* (2016).
3. Gesamtverband Autoteile-Handel e.V. (German Association of Car Part Distributors). *Martkvolumina*. Accessed from https://www.gva.de/branche/marktvolumina.php (German only).
4. Schöneberger advisory services: The automotive digital transformation and the economic impacts of existing data access models (2019).
5. Bundesverband der Energie- und Wasserwirtschaft e.V. (2018). *(German Association of Energy and Water Industries): Digitalisierung, Normung und Standardisierung in der Elektromobilität. Erfolgsfaktoren für die Energiebranche* (German only).
6. Verband der TÜV e.V. (2019). *(German Association of Technical Inspection Agencies): Verkehrssicherheit und Umweltschutz durch Fernzugriff auf Fahrzeugdaten* (German only).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.