Peter Geffers, Ford

‘Highlighting the positive aspects of connectivity’

Car manufacturers are often accused of being careless and non-transparent with their customers' data. Peter Geffers from Ford defends against this prejudice and outlines what politicians and the industry intend to do with data from connected cars.

Mr. Geffers, car manufacturers are sometimes labeled as opaque data giants that hold or even mishandle customer data. Where does this perception come from?

This perception is based on many different reasons, which are not exclusively on the part of the car manufacturers. The cliché persists that the automotive industry is sitting on terabytes of vehicle data and that vehicles today are like smartphones on wheels. Five to six years ago, OEMs started to network vehicles on a larger scale via modems. This happened more or less ‘silently’, i.e. new vehicles were delivered with modems, although customers did not yet have access to a wide range of connectivity features via the manufacturer-specific apps. It was therefore not visible to all customers what benefits they would gain from the connectivity of their vehicles. At that time, the General Data Protection Regulation was the main basis for the extraction and use of vehicle data. In concrete terms, this means that even back then, as a manufacturer, we needed a legal basis, such as the consent of our customers, to use personal vehicle data. In addition, data was processed in anonymized form, i.e. without traceability to the specific customer, to carry out product improvements or error analyses, for example. The fact that there was always a legal framework to which the manufacturers had to adhere was perhaps not communicated transparently enough to the general public.

This obviously leads to misunderstandings not only among end customers.

These circumstances create room for speculation among both customers and other market participants who would like to have access to vehicle-generated data to offer data-based services that compete with the manufacturer's own new data-based offerings. In addition, the data supply, ie. the data that a vehicle extracts, is unfortunately often overestimated by market participants. There is an assumption that a vehicle transmits everything that is generated in the vehicle during driving. However, this is not the case, as most of the data is so-called ‘transient data’, i.e. data that only exists in the vehicle for a brief moment and is exchanged between the control units. An example of this would be the engine transmission control.

To what extent does the networking of vehicles with each other and with the environment offer an opportunity to regain customer trust?

We must succeed in highlighting the positive aspects of connectivity and the resulting benefits for the mobility of tomorrow. This also includes transparent and good communication about the use of data and the resulting benefits for all mobility participants. Thanks to this transparency, our customers trust us to do the right thing with the vehicle-generated data. I would like to cite electromobility as an example here. If we as a society want to achieve the transport transition, we need to share data on charging statuses and planned charging times of our vehicle battery storage systems with the grid operators, just as we want to use charging stations on our vehicle routes in order to be able to provide energy in the most environmentally friendly way possible from the customer's perspective with very short or no waiting times. It is irrelevant who drives to a charging station. Rather, the decisive factor is when and where how much energy are required by how many vehicles.

In addition to car manufacturers such as BMW and Mercedes, Ford has also been a member of the EU Data for Road Safety (DFRS) initiative since mid-2019. What is behind it?

Data For Road Safety is a partnership between private and public institutions to increase road safety on European roads with the aim of halving the number of road fatalities by 2030. The basis for this partnership is Delegated Act 886/2013, i.e. a regulation of the European Commission, which requires all road users to provide the following road safety-relevant data, if technically available. This includes a total of eight events such as slippery road surfaces, people, animals or obstacles on the road, accidents, short-term roadworks, restricted visibility, wrong-way driver warnings, road closures and exceptional weather conditions. This data is shared anonymously with all members of the DFRS for the sole purpose of warning road users. The more road users share this data, the more precise the traffic information becomes and can therefore, for example, issue targeted warnings in sections of traffic about black ice or the end of a traffic jam. These warnings are then displayed specifically via the current geo-position of the vehicle or a navigation application on a mobile device and, unlike radio traffic announcements, are transmitted with pinpoint accuracy.

Which players are involved in DFRS?

Since the start of the initiative in 2019, we have been able to gain many new private members such as Volvo or Audi, as well as telematics service providers such as Inrix and Geotab and ASFINAG, in addition to other founding members such as Here and TomTom or various road authorities. Over the past few years, we have continuously built up the ecosystem in compliance with data protection laws and have now moved on to the operational phase via a proof of concept. With each new DFRS partner, we are getting closer to our goal of eliminating the number of traffic accidents as far as possible.

How important are common industry standards for the cross-manufacturer exchange of vehicle and traffic data?

International norms and standards are decisive factors in the digital and sustainable transformation. They ensure that technical and digital solutions are as interoperable as possible worldwide. However, they must not become an obstacle to innovation and a rapid market launch. Standards usually emerge over time where many market participants do the same thing without being able to claim a special advantage for themselves, or where communication between systems or vehicles is essential, as is the case with autonomous driving.

What does that mean in concrete terms?

In practice, this means that we have the advantage when exchanging vehicle data that we can adapt the format of the data in the cloud so that users can process the data better. Standards therefore always follow market developments to a certain extent. Where many people do similar things without having an advantage and communicate with each other, there is a common need to standardize these interfaces in the medium term, as this reduces the workload for everyone involved. However, legislation that prescribes standardization would be completely counterproductive and overshoot the mark. It would mean that manufacturers would have no incentive to innovate and market these innovations. Standardization processes often take several years and then have future introduction dates.

We therefore very much welcome the fact that Germany is involved in the field of standardization with its German Strategy Forum and is one of the leading nations in the management of technical standardization committees at international level. Furthermore, together with many suppliers, vehicle manufacturers and other market players, we are part of the Connected Vehicle Systems Alliance (COVESA) initiative. This initiative is already pursuing the goal of establishing a signal specification for vehicle data (VSS) without the need for a legal requirement. In the medium term, this will have the desired effect of establishing data standards without the need for sector-specific regulation.

‘International standards are decisive factors for transformation, but must not become a stumbling block for innovation’, warns Peter Geffers (Photo: Ford Werke GmbH)

The more traffic data is circulated via the cloud, the greater the potential for cyberattacks. What potential dangers are piling up right now?

The potential danger of cyberattacks on vehicles is increasing enormously since vehicles are connected to the Internet of Things (IoT) - theoretically 24 hours a day, seven days a week. The amount of data initially plays a subordinate role. Cyberattacks generally aim to cause harm to people or companies, which is then averted by paying a ‘ransom’. This approach has increased rapidly in recent years. As almost every new vehicle is now connected, a market is emerging for criminals to expand their activities to connected vehicles.

In a non-networked vehicle, it would take far too much effort to insert an OBD dongle into a vehicle in order to carry out a cyberattack on it. To limit or even better eliminate this potential danger, we advocate that access to vehicle data, functions and resources should only be granted via us as the vehicle manufacturer. If we had to make this access available to unknown third parties without restriction, we as the manufacturer would, in the worst-case scenario, no longer be able to distinguish authorized access from a cyberattack and the transfer of liability might even have to pass to the users who grant third parties this access.

The EU Data Act, which comes into force in 2025, is intended to simplify access to data from connected vehicles and boost competition in the market. The VDA sees this as more of a stumbling block for the car industry's ability to innovate. Do you take a similarly critical view of the new regulations?

In principle, we at Ford and our associations welcome the EU Data Act, as the legislator has struck a good balance. On the one hand, the Data Act strengthens the rights of users to gain access to the data they themselves generate when operating a vehicle or to make this data available to third parties at their request.

In principle, there is nothing wrong with this, as it can help to advance the mobility of tomorrow and the networking of vehicles with the IoT. On the other hand, the Data Act also enables us to protect our innovations and investments. We make high investments in our vehicle developments, which we also have to amortize over the life cycle of a product. This also includes data-based services that are based, for example, on innovations that represent intellectual property worthy of protection.

If we were forced to share all the services developed by processing raw data ourselves for the market launch of a product, there would no longer be any economic incentive to invest in these services and in networking. Third parties, on the other hand, would even have the advantage of marketing these services without investment, which would represent a competitive disadvantage for us as a manufacturer.

In addition to the Data Act, a sector-specific regulation for access to vehicle data is also currently being discussed. Why does the automotive industry need its own data rules?

We are of the opinion that there is currently no need for sector-specific regulation. The Data Act is a comprehensive, sector-independent set of rules for access to data in the IoT, which also includes vehicle data.

Supplementing this with sector-specific regulation before it comes into force does not seem to make much sense to us. The EU Commission should wait until the Data Act comes into force and analyze its impact on the market for vehicle data. Article 41 of the Data Act even provides for such an analysis by the Commission. However, we are of course aware that there are certainly interest groups that are calling very loudly for sector-specific regulation. Here, however, we should take a more differentiated view of the issue - also in this discussion.

Because not all data is the same. Very different types of data, functions and resources can potentially be made available in the vehicle. The questions must be how and who can access it because vehicle safety must continue to be guaranteed, just as the protection of trade secrets must be safeguarded. Manufacturers are obliged to do this by other parties. Third-party access to data, functions, and resources in safety-relevant areas of the vehicle bypassing the vehicle manufacturer cannot be in the interests of consumers. In this discussion, which is very complex and technical, we appeal to you to scrutinize the interests of third parties. We therefore largely reject the proposals for this sector-specific regulation that we are aware of, as they do not take sufficient account of the risks associated with the issues of innovation capability, standardization or cybersecurity that have already been discussed and should not be adopted hastily.

Read the original interview here: https://www.automotiveit.eu/technology/muessen-die-positiven-aspekte-der-vernetzung-herausstellen-860.html