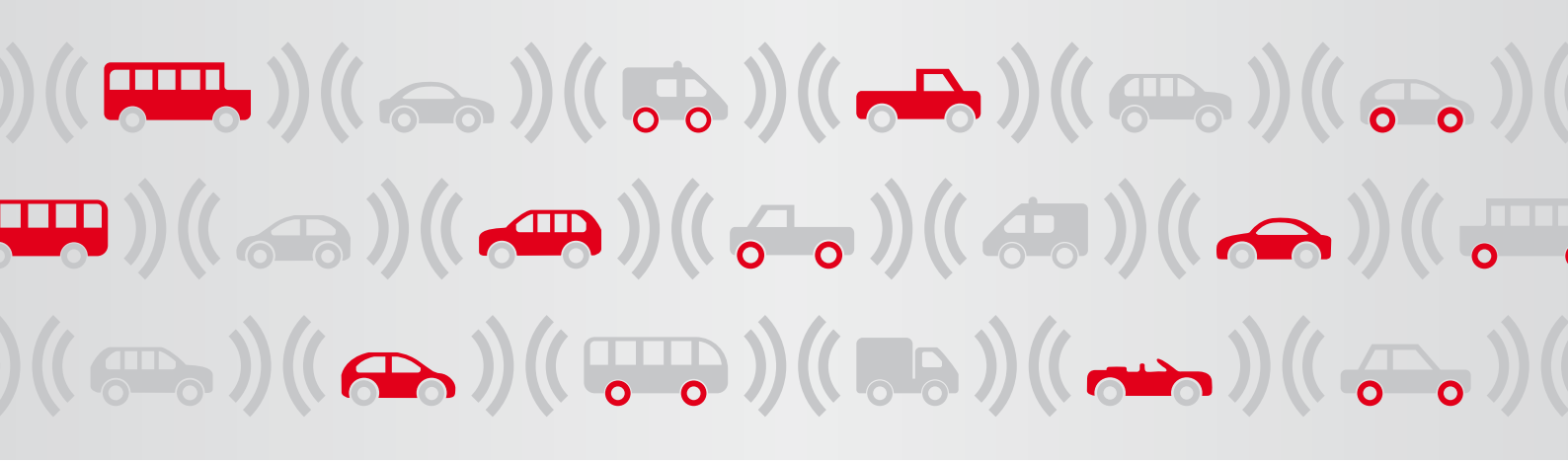


Connected and Autonomous Mobility

Challenges in the fields of cyber security, data protection, and warranty and liability law

Authors

Klaus Brisch LL.M., Dr. Jens Eckhardt, Prof. Dr. Marcus Gelderie,

Daniel Groß, Thorsten Jansen LL.M., Tobias Knoben,

Marco Müller-ter Jung LL.M., Prof. Dr.-Ing. Dr. h.c. Dieter Schramm,

Nils Steffen, Thorsten Stuke, Thomas Weber

eco

ASSOCIATION OF THE INTERNET INDUSTRY

WE ARE SHAPING THE INTERNET.

YESTERDAY. TODAY. BEYOND TOMORROW.

Content

Oliver J. Süme
Chair of the Board, eco – Association of the Internet Industry

1. Foreword

Dear Readers,

The mobility sector is facing enormous changes with digitalization. German carmakers have announced major investments. Over the next five years, Volkswagen plans to spend 44 billion Euro on the development and introduction of new technologies such as self-driving cars and electric mobility. This sounds impressive, but there is actually no alternative if the sector is not to fall behind in the fast-paced development in the international market.

It is not only the car itself that is undergoing major change; our understanding of mobility is also changing. We increasingly perceive the ability to get from one place to another as a service that is available on request – whether our own car is parked in the garage or not. Car-sharing or mobility apps help us to get to our destination. Our means of transportation are no longer isolated objects, but increasingly components of a mobility ecosystem that spans the globe.

This is giving rise to new data on a large scale: position data, speed data, environmental data, data on driving behavior, entertainment, and maintenance data. Thanks to the Internet industry and its digital infrastructures, we can make the most of this data. We need 5G technology, data centers, and edge computing to make mobility more convenient, faster, and safer.

The last point is crucial: safety is a central aspect for the acceptance of self-driving cars. Our most urgent task is therefore to protect vehicles from attacks by cyber criminals. The necessary standards and certificates for a sophisticated, reliable, and trustworthy infrastructure can only be created hand in hand by those involved in the industry. Here it is necessary to work together constructively.

For this to work, another prerequisite for success is data protection. Here, Germany and Europe have the opportunity to set international standards with the help of the European Union's General Data Protection Regulation (GDPR). At the same time, there is the challenge that data protection requirements also make digital business models more complicated – if not altogether impossible. The stringent data protection requirements should be harmonized with these new business models; whether these involve ride sharing or car sharing, travel portals, or insurance companies.

Fully autonomous driving will conquer the roads in the near future. With this paper, we want to contribute to getting the self-driving car "on the road", replete with cyber security, data protection, and well-defined areas of responsibility and liability. As the Association of the Internet Industry, we have compiled analyses and recommendations for action for decision-makers at OEMs and suppliers, in research, politics, and administration. Let us shape the mobility of the future together.

Your,

Oliver Süme
Chair of the Board, eco – Association of the Internet Industry

2. Ecosystem of the Mobility Industry

The ways in which we get from point A to point B will change dramatically in the coming years. The transport means will no longer be in the foreground; mobility will become a service. The number of autonomous and connected vehicles will increase. In order to establish and extend the necessary digital infrastructure, a strong Internet industry is required, whose companies will assume a more important role in the mobility ecosystem.

2.1 Mobility 2030 – A look into the future

Imagine you are in the year 2030, you live in Berlin or Paris, and you want to travel to Beijing. You inform your smart assistant, which supports you in organizing your day, of the travel destination and departure time. The system has access to a mobility portal and can look up information on means of transport and infrastructures such as streets, railway networks, and flight paths. It books the optimal connection from your home to Beijing: fast and easily, cheaply, and in line with your preferences.

At the desired time, you head off on your journey: You are collected from your home by an autonomous robotaxi, which takes you to the airport. Perhaps you don't even own a private car. Along the way, the vehicle picks up another two passengers from your suburb who are also heading to the airport, and when you get there, you hop on the plane to Beijing. From Beijing's Mega-Airport, you travel to the city center in a high-speed train. A software-controlled air taxi then takes you from the station to your customer or your hotel.

In all probability, this is what the mobility of the future will look like[1]. We may not even perceive it as such, because we will be able to move from point A to point B without even lifting a finger. At no point in the journey described above are we required to tend to our own comfort, a means of transport, or paying for a ticket, something which is taken care of automatically via payment systems and regardless of currency. There might even be travel flat rates, through which passengers can book a monthly kilometer volume. Waiting around for the next leg of the journey will be a thing of the past. Travel will become stress-free, especially given that we will not need to even touch a steering wheel throughout our journey – thanks to the seamless interconnection and autonomous behavior of our various means of transport.

This new type of interconnection of the means of transport will make it possible for people to make a completely new demands on their mobility. City dwellers, in particular, will no longer own their own car, but will make use of services like car sharing and car pooling. People will expect Mobility as a Service – and that the service is permanently available for the consumer.

Automated or autonomous driving is only allowed in limited contexts today. In particular use cases, such as parking, autonomous systems are permitted to take over longitudinal and lateral control. Several important steps still need to be taken in the areas of technical safety and regulations to reach a higher level of automation, through to complete software-control of the vehicle – and these steps need to be taken fast, because the development is unstoppable, and fully-automated driving is almost upon us.

2.2 The platform economy

A basis of this "new" mobility is the platform economy. Mobility platforms make it possible for customers to calculate the optimal route from point A to point B taking all means of transport into account. These services, then, will be at the center of future mobility, rather than the actual means of transport.[2] The car will become just part of a larger system and will therefore rely on being interconnected with other system components.

Several sectors have already experienced the shift to a platform economy. This includes retail (Amazon, e-commerce), tourism (Airbnb), and music (Spotify). In the mobility sector, Uber is a very prominent example of the fact that this sector has also been in the process of transformation for some time now. Several traditional automobile manufacturers have already developed new business areas which are based on the foundational principles of the platform economy (for example, Car2Go, DriveNow, and Moia).

The greatest asset of this economy is the vast quantity of data that is generated through the interconnection of digital services.[3] In the case of mobility, the data concerned includes information on

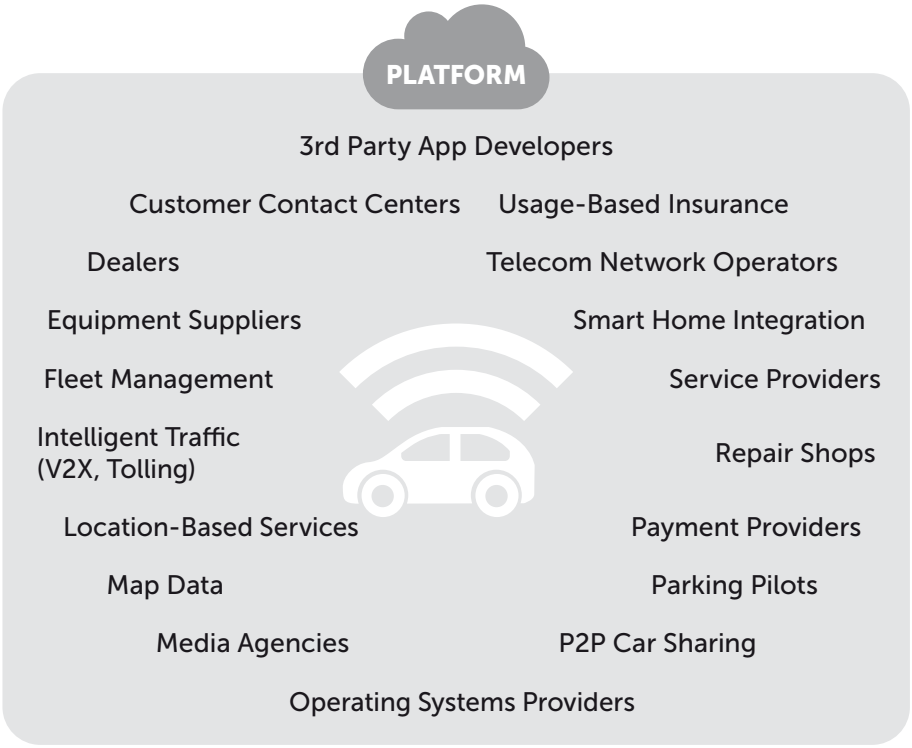
1 See, inter alia, Heller (2018): Wie wir demnächst von A nach B kommen; Zukunftsinstitut (2017): Die Evolution der Mobilität

2 Ibid.

3 545 Petabytes per annum are forecast for 2020 – an increase of 186 percent compared to 2013. See Seibert (2015): Wie verändern digitale Plattformen die Automobilwirtschaft?

Fig. 1

The platform economy of connected and autonomous vehicles



individual consumer comfort, traffic situations, weather, position, entertainment profiles, and data from satellite systems. Autonomous vehicles also depend on the analysis data from the surrounding environment and the behavior of other vehicles on the road.[4]

This large amount of data forms the basis for new business models, which offer the user the best possible individually-tailored mobility services. Additional stakeholders could benefit from mobility services such as parking apps, travel portals, and traffic management systems. Car insurers, for example, could use the data generated by a car in order to adapt the policy premium to the driving style ("pay as you drive"). For the maintenance of traffic infrastructure, data collected by sensors could be used to analyze the condition of roads and information on traffic flows and provide information regarding the need to resurface roads or remove obstacles. [5]

The car will become an open unit in the new ecosystem and will share data with many partners.[6] This being the case, ensuring the security and integrity of systems against unauthorized access to functions and data is absolutely crucial. The General Data Protection Regulation (GDPR) offers a legal framework for digital business models and operations. In addition to the GDPR, Chapter 5 analyzes futher data protection regulations with regard to their applicability for future mobility business models.

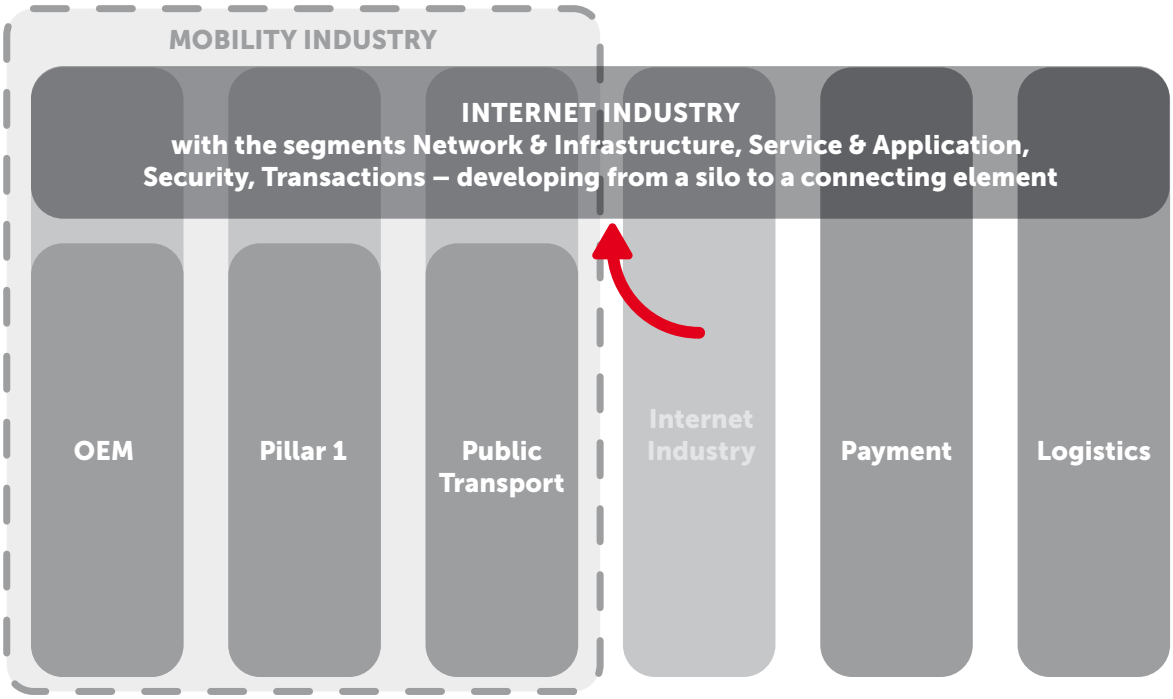
2.3 Changes in the ecosystem

For such a critical component of society as mobility, it is of enormous importance that this complete digitalized system operates continuously. This implies that the players involved work together in a highly interconnected way, and that there is a kind of "system operator" for the digital infrastructure. This is the case both for the components that make an optimal journey from point A to point B possible for the customer, and also for those that guarantee the safe movements of vehicles that are being controlled without human intervention. Because ultimately, "modern cars are in themselves a type of data center – they carry a processing power of more than 100 CPU and need to validate data within milliseconds before they can send the results, not only to their internal driving systems, but also for communication purposes to other vehicles on the road."[7]

While the car has until now existed as an isolated capsule, it will in future become increasingly a component of an extensive ecosystem. The data exchange in this complex construct, comprised of sensors, electronic components, and on-board entertainment systems in the car, mobile units along the street and in smart cities, and workshop measurement tools, as well as gateways, mobility platform servers, and the satellite network, will grow enormously.[8] Cyber criminals must not be given the chance to hack into this sensitive system, in their quest to cause willful damage or to steal data.

4 This topic will be expanded upon in Chapter 3.1
5 Figure 1 shows some of the beneficiaries of the platform economy in the field of mobility.
6 See Veronesi/Eibisch (2018): The Car as Connected Platform
7 Zachmann (2018): The Car as a Driver for Data Growth Needing New Infrastructure Solutions
8 See Comastri (2018): New Frontiers for Car Security: API Management

Fig. 2



This requires a seamlessly functioning digitally interconnected infrastructure, which is needed to make mobility platforms and connected and autonomous vehicles a reality:

- Fast and permanently available networks
- Data centers for the processing of mountains of data
- Platforms that control services
- Maximum protection of the data and the infrastructure
- Service providers and integrators that keep the systems operating

The performance of this infrastructure is already enormously important for driving and for planning routes. The use of carsharing services by consumers[9] is constantly growing. Map-supported services simplify navigation and finding somewhere to park. Several on-board systems, such as Concierge, as well as entertainment services, are standard in new models. The on-board software is to a certain extent automatically kept up-to-date through over-the-air updates. Workshop and manufacturer systems for reading diagnostic data[10] have become indispensable.

We are getting closer and closer to the end of the silo economy, and the automotive industry is in the process of transformation.[11] Until now, there has been a clearly-structured supply chain, in which OEMs[12], suppliers, software producers, and others led a silo-based existence and executed the wishes of their contracting partners in isolation. Cooperation with IT and Internet players will soon be unavoidable[13], in order to realize not only the seamless, secure, and low-latency interconnection of the vehicle and its components, but also the continuously increasing level of autonomy. Christoph Weigler, Head of UBER Germany, is convinced that it will not come down to an either-or situation, but a cooperation. "The environment is becoming ever more complex, partnerships are already indispensable today. Classic automobile manufacturers and technology companies will cooperate much more closely in the future than they already do today."[14] The pivot point of this ecosystem will be the Internet industry, especially when it comes to security and digital infrastructure.[15]

Did you know? In Germany, the Internet industry will overtake the automotive industry in 2028 and, as a result, will dominate business models! This makes working across industries very worthwhile.[16]

9 See Bundesverband CarSharing e.V.: Aktuelle Zahlen und Daten zum CarSharing in Deutschland
10 See Chapter 3.3
11 See Seiberth (2015)
12 Original Equipment Manufacturers

13 See Figure 2: Changes in the mobility ecosystem
14 Christoph Weigler was cited in the Spiegel news magazine article Sommerfeld (2018): Wie sich die Autoindustrie neu erfindet - und unser Leben damit verändert
15 See Seiberth: Branchengrenzen
16 See eco – Association of the Internet Industry/Arthur D. Little (2016): The German Internet Industry 2016-2019

Interview

Mobility service provider – "A service provider that brings together the many and various mobility options and bundles them intelligently"

Gerrit Pohl,
Chief Digital Officer, ADAC SE

Interview with Gerrit Pohl, Chief Digital Officer, ADAC SE

Mr Pohl, how would you define a "mobility service provider"?
That is a broad field, of course, but I see it as being a service provider that brings together the many and various mobility options on one interface and bundles them intelligently. The customer can purchase these really easily and avail of an additional range of mobility-based services. So, perfectly organized on the digital level, but still predominantly analog services.

In your opinion, what is the biggest challenge for creating the highest level of autonomous driving on European roads?
There will be copious mathematical challenges when the fully automated meets the partially automated or the completely manual, especially in an urban environment. Predicting the unpredictable is of course a major challenge, but the fully autonomous vehicle must be able to react in a maximally safe way to all of these things. That means that if someone can solve this in India, for example, it will be solved everywhere. But beyond this, there are highly complex approval, liability, and insurance questions pending.

What role will the ADAC [the General German Automobile Club] play in future in the world of autonomous and connected mobility?
Our position as a consumer protection association and as a neutral consultant will gain in importance in a mobility world which is changing increasingly quickly. Apart from that, we will continually consider how we can make the various forms of mobility accessible to our members and at the same time protect them as comprehensibly as possible against the risks. But one thing is clear: Our services need to increasingly demonstrate a high degree of relevance in everyday life, and for this reason we are already looking at relevant topics in addition to mobility.

Top 5

Short summary of Chapter 2

- *Mobility will become a permanently accessible service.*
- *It is characterized by interconnection, autonomous vehicles, the sharing economy, and – though not addressed in detail here – post-fossil fuels.*
- *Platforms will become the core of this "new mobility".*
- *New disruptive business models will be developed.*
- *The Internet industry will become the pivot point of the players in the newly-developing mobility ecosystem.*

3. Data Exchange from Connected and Automated Vehicles

Through interconnection and automation, the car will increasingly become a part of the Internet of Things. The vehicles exchange enormous amounts of data, be it with each other or in the interplay with traffic infrastructure components, for example via sensors on traffic lights or in the asphalt.

3.1 Collection of data

The collection of data occurs on the one hand by or through the car itself, and on the other hand through the infrastructure. Collection through the car is well established and has been occurring for many years, whereas (as of 2018) collection via infrastructure has so far only occurred in the context of managed systems, e.g. toll systems or general surveillance measures. This will change as vehicles become more autonomous and cities become "smarter".

The German Association of the Automotive Industry (VDA) differentiates between the following categories of data in the connected vehicle:[17]

- The purpose is regulated by law, e.g. OBD II[18] and e-Call (EU)
- Modern data services, e.g. anonymized and pseudonymized Car-to-X services and predictive diagnosis
- Customer-owned / external data, e.g. infotainment and comfort settings, navigation destinations, address book
- Operating values generated in the vehicle and displayed to the driver, e.g. fuel level and consumption
- Aggregated vehicle data generated in the vehicle, e.g. error memory, number of faulty functions, average consumption, average speed
- Technical data generated in the vehicle, e.g. sensor data, actuator data, motor injection pattern, behavior of automatic transmission

17 See Verband der Automobilindustrie e.V. (2014): Datenschutz-Prinzipien für vernetzte Fahrzeuge
18 On-Board Diagnosis II

3.1.1 Collection of data in the vehicle

Initially, differentiation needs to be made between the collection of the movements and other status variables of the vehicle and, in future, also of the driver through proprioceptive[19] sensors, and the recording of the environment through exteroceptive[20] sensors.

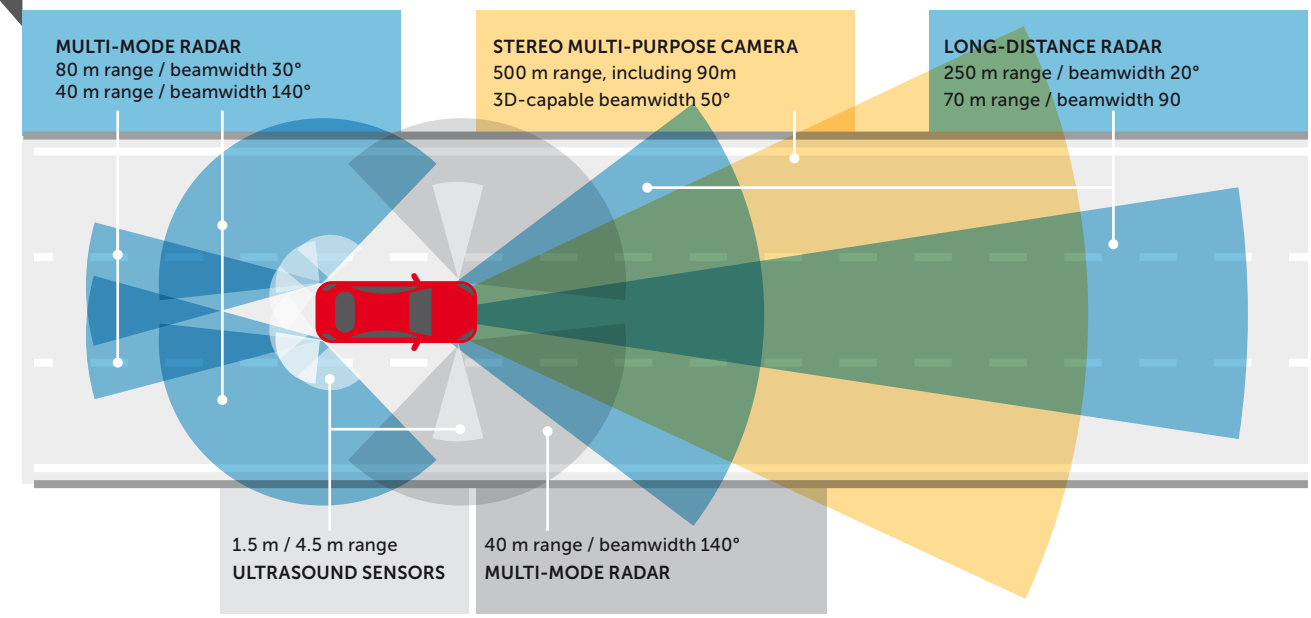
Proprioceptive sensors collect the vehicle's own movements, the internal functions, and the condition of the vehicle through a multitude of sensors, which enable the collection of, for example, the vehicle movement data, temperature, and transmission settings, but also control elements like pedals and the steering wheel. Such sensors have been used widely ever since the emergence of braking systems and vehicle dynamics controls[21]. Added to this are sensors that collect diagnostic data, in order to, if necessary, forward this on to the mechanic, the manufacturer (via an additional OBD dongle and GSM or smartphones), or other service providers. Such systems are also capable of forwarding location data and movement data. Examples for this are, in the OEM area, Mercedes Me[22] and, in the third-party provider area, RYD[23]. Further collection and transmission of movement data takes place through connected navigation systems, where required augmented through the use of smartphone data, also through OEMs and third-party providers. This means that proprioceptive vehicle data does not necessarily require special sensors, but simply carrying a smartphone can enable the collection of the "driver/vehicle unit".

Exteroceptive sensors record the environment of the vehicle, meaning other road users, the infrastructure, weather data, etc. Here also, since the introduction of ACC (Adaptive Cruise Control), which requires a radar sensor for the measurement of differences in speed and distance to other vehicles, a multitude of sensors have been used, such as radar and lidar sensors, cameras, and ultrasound and infrared sensors. Figure 3 illustrates the features of a newest generation vehicle with exteroceptive sensors.

19 Perceptions from within one's own body (here "the vehicle") from the Latin proprius "own" und recipere "receive"
20 External perceptions (here from outside the vehicle); from the Latin extra "outside" and recipere "receive"
21 This includes systems such as ABS, ASR, ESP, etc.
22 See https://www.mercedes-benz.com/en/mercedes-me/
23 See https://ryd.one/

Fig. 3

Features of a vehicle with extraprioceptive sensors



3.1.2 Infrastructure-supported collection of data

Car-to-Infrastructure Communication (C2I) is a concept for the communication of vehicles with infrastructural equipment. The infrastructure components can be intelligent traffic signs, light signal systems, traffic management systems, radio beacons, intersections equipped with radio masts or Intelligent Roadside Stations (IRS), via which a connection can be established, e.g. to Internet-based services, emergency services, the vehicle owner, or the vehicle manufacturer. In many cities, these installations form a part of a smart city concept. Systems that transmit diagnostic or emergency data directly to the vehicle manufacturer or mechanic are already in use today. The communication can also take place via so-called roadside units (RSU), which are positioned on transport routes and are connected with each other by access routers (AR).

The "physical layer" for such concepts is, as a rule, wireless, and includes in particular mobile telecommunication systems such as GSM, UMTS, HSPA, Long Term Evolution (LTE), WLAN, and WiMAX[24]. Other equipment can of course also be integrated, such as broadcasting systems with traffic information, DAB+, etc. In addition, the standard Cellular V2X, as part of 5G, has been made available for the automotive sector.

As of today, the transitions between networks do not yet function flawlessly and can certainly lead to difficulties in the legal analysis of accidents. It is possible that an interface analysis will be required in order to investigate whether or not the cause of an accident may have resulted from such a gap causing a temporary network outage in the car and leading to an erroneous reaction.

3.2 The car as part of the Internet of Things

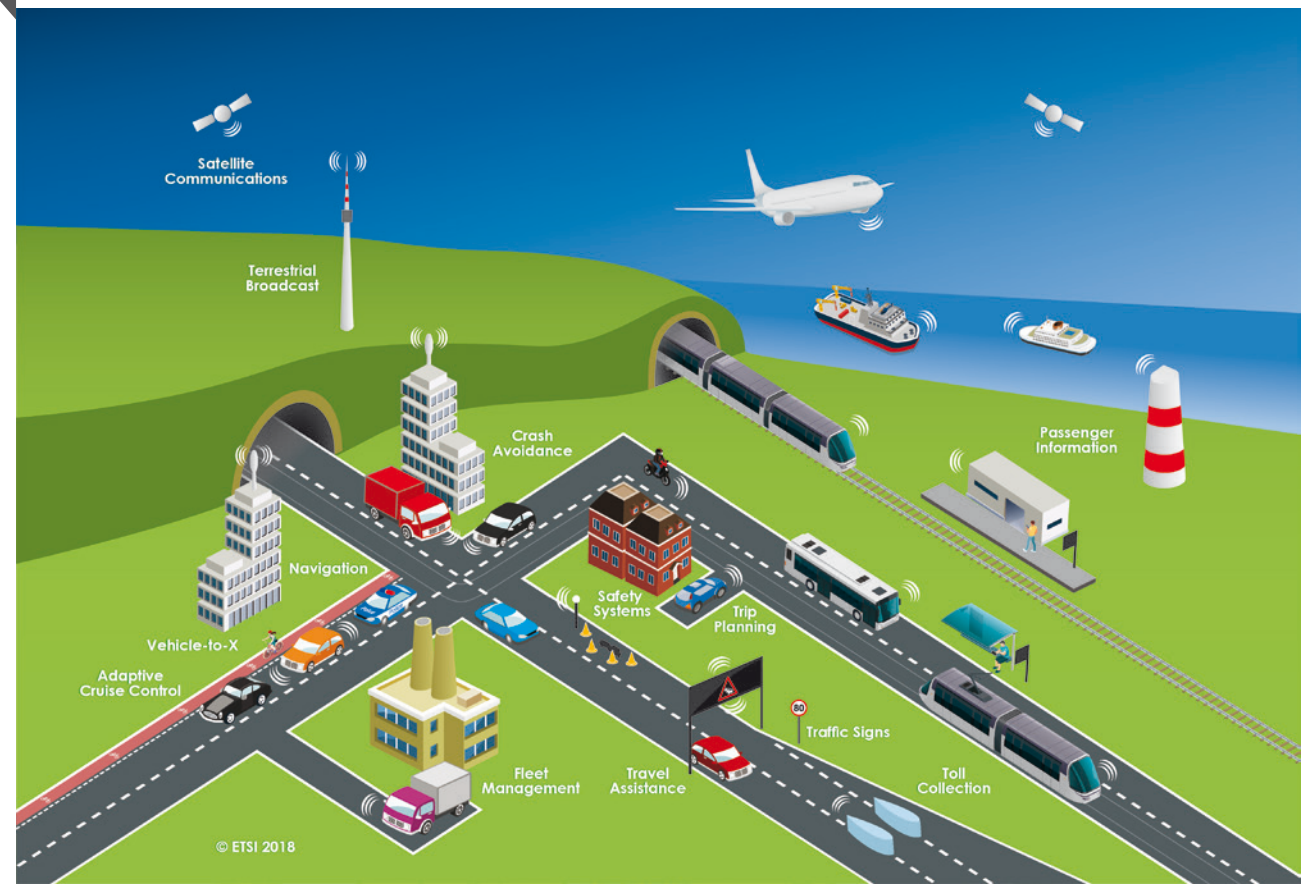
The term Car2X Communication refers both to the wireless networking of vehicles with one another (Car-to-Car, Car2C) and also to the integration of the infrastructure (Car-to-Infrastructure, Car2I) and further road users. It forms a part of the Intelligent Transport Systems (ITS), as shown in Figure 4. This is the term as it is understood by the European Telecommunications Standards Institute (ETSI) which, alongside the European Committee for Standardization (CEN), plays a leading role in Europe and in efforts towards international harmonization.

24 WiMAX (Worldwide Interoperability for Microwave Access) is a wireless access technology to broadband Internet and is frequently used as a synonym for wireless systems according to the IEEE-Standard 802.16, similar to WLAN, which is based on the IEEE-Standard 802.11.

Communications Concepts for Connected Cars

Car to X Concept	Description	Examples of data transmitted
Car to Car	Communication between two vehicles	Movement data, status data
Car to Infrastructure	Communication between vehicle and infrastructure systems	Light signal systems, traffic signs
Car to Mobile	Communication between vehicle and telephone network	Infotainment, Smart Services

Fig. 4 **Complete Concept of an Intelligent Transport System (ITS) according to ETSI**



The goal of these attempts at standardization is, in particular, the unification of the network architecture and the access paths, security protocols, and data formats. This should ensure that the communication between the different road users from diverse interest groups can be guaranteed. This includes the many automobile manufacturers, but also the telecommunications providers, suppliers, infrastructure providers, mobility service providers, public transport companies etc. The term Car2X therefore includes concrete technical approaches to solutions and standards for the interconnection of traffic systems. Through the many and diverse interfaces for data exchange, the car is becoming more and more a component of the Internet of Things.

3.3 Diagnosis and updates of control units "over the air"

3.3.1 Conventional vehicle diagnosis

In the standard diagnostic functions which have been used to date, data is collected via an already large number of sensors that are either separately placed or built into control units. Monitoring takes place either when the motor is started or continuously during the operation of the vehicle. As a rule, the only information stored is any irregularities registered during the monitoring. These are then, as a rule, read out via the OBD-II interface with special testers during the next visit to the mechanic, and, if necessary, linked to an integrated "expert system" and interpreted, in order to find the cause of the problem. For this, standardized description formats are used both in the vehicle and on the part of the workshop inspector. An online diagnosis is not possible for such a procedure, but is also not necessary for conventional vehicles. Responsibility for the data collected remains with the respective mechanic, perhaps also with the manufacturer. As these are snapshots taken in the moment of the test, as a rule a history cannot be created.

3.3.2 Future diagnostic systems

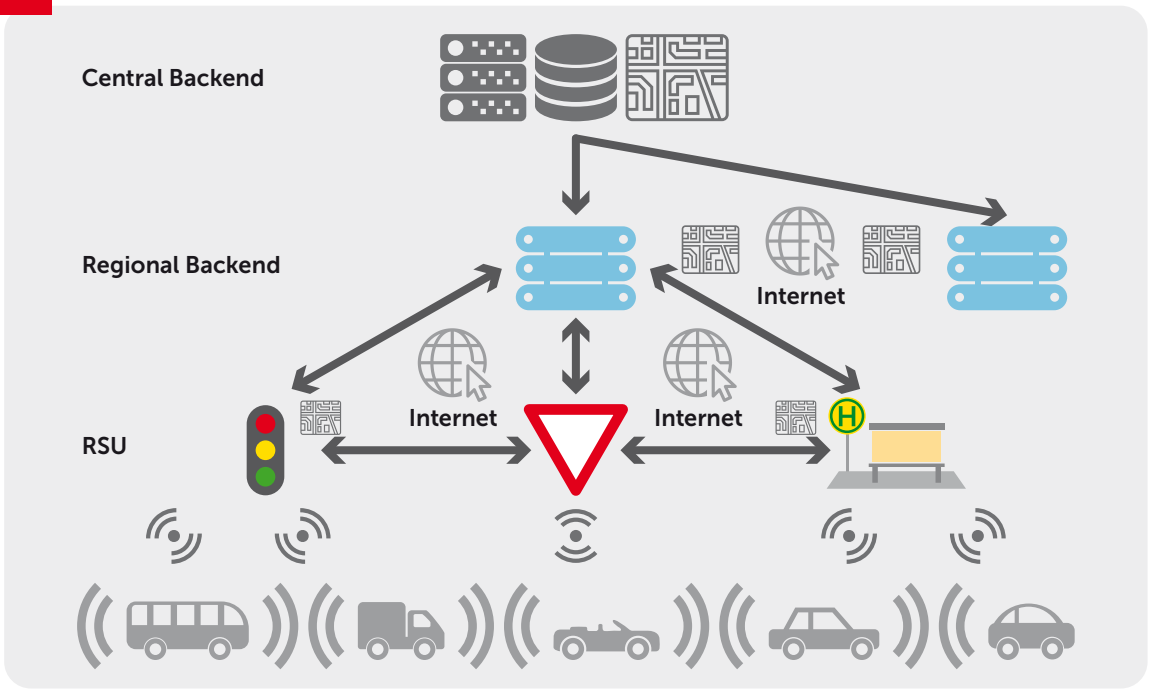
In future use cases like autonomous vehicles, the conventional procedure will no longer be sufficient. In this case, the data must be collected online, which also makes it possible to store this data in a "cloud". This type of data collection could be used for "predictive maintenance", e.g. to predict the failure of components as a result of metal fatigue[25]. Car manufacturers' systems will in future be capable of deducing the use of and wear and tear on vehicles through the recording of collective load. Such systems are also suitable for proving use which is contrary to the designated purpose. The data can also be used as loading information – for the design of future vehicles or for the prediction of quality costs – by recording the customer use behavior in real-world traffic conditions.

A further application is the installation of new software versions (SOTA: Software-over-the-Air). This process offers the potential

25 See Kong et al. (2017): Mission profiling of road data measurement for coil spring fatigue life

Fig. 5

Communication levels of connected traffic systems



to constantly and rapidly fix vulnerabilities with patches, eliminate errors, and install and activate new functions. An on-board control unit accepts the software packet and distributes it to the target devices in the car, over the Ethernet systems or CAN-Bus. Tesla, for example, activates functions upon payment of a surcharge, without a trip to the mechanic. Another example is the installation of updates, also without the need to visit a car repair shop; something that is already state of the art today for navigation and entertainment functions.

This type of maintenance and diagnosis enables, on the one hand, the prompt elimination of errors without needing to visit a mechanic, prevents sweeping product recalls, and plays an important role in the development of new business models (see Tesla). On the other hand, however, it harbors the risk of abuse by third parties or by the car manufacturer itself. For example, it would be possible to collect data on customer user behavior, in order to prove use which is contrary to the designated purpose. For the update process itself, it is necessary to ensure a maximum level of protection of the "air interface", to prevent the installation of manipulated software. A hacked autonomous vehicle with a remote control unit would be an absolute catastrophe with unforeseeable consequences for all road users.

3.4 Cooperative driving and exchange of sensor data

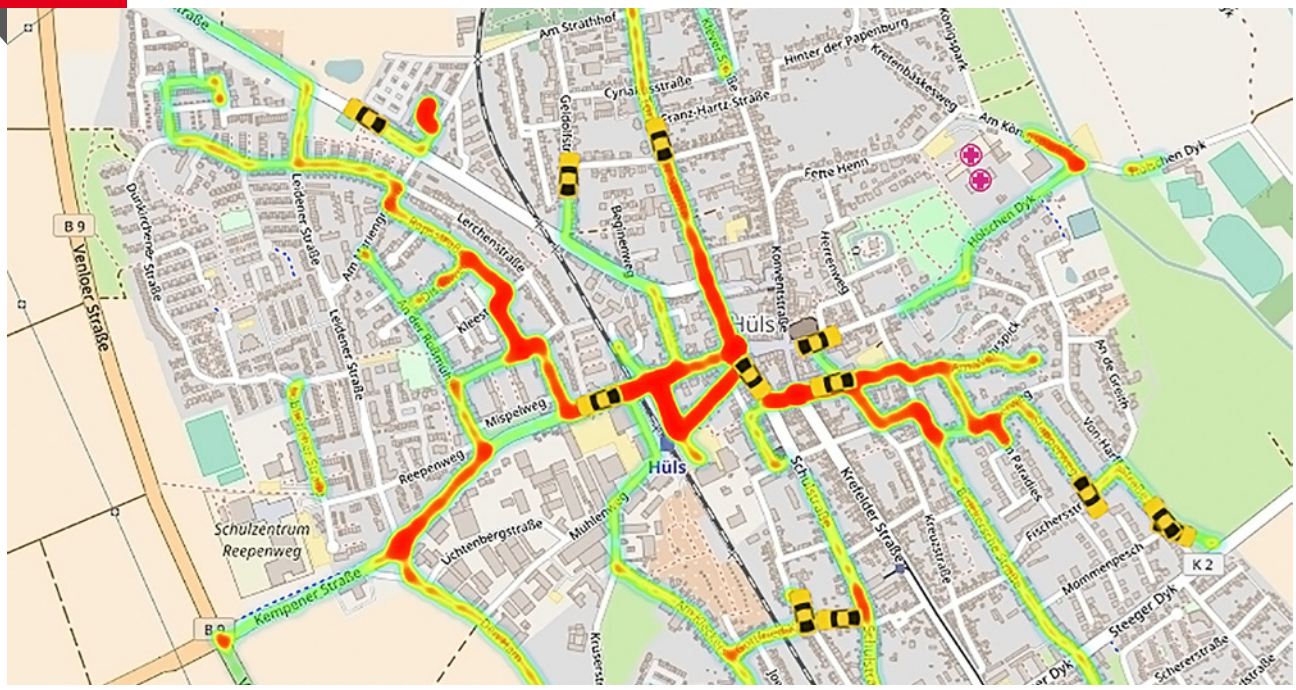
Currently, the sensor data collected in the vehicle is exclusively used for functions in that respective vehicle. Initial research results, such as those of the KO-FAS project[26], have demonstrated that the transmission of relevant data enables critical traffic situations to be detected early and thus conflict situations can be avoided and accidents prevented. This can be achieved, on the one hand, by warning the driver about dangers earlier, as well as through the direct intervention of the assistance and emergency systems designated for this purpose. Especially against the backdrop of future applications in the area of highly automated and autonomous vehicles, this is of particular interest.

In the project SEEROAD[27], a vehicle-based sensor system is to be developed for the collection of data on the road surface condition, in order to enable highly automated future systems to adapt the vehicle dynamics – meaning the speeds and trajectories – to the environmental conditions. A further objective is to also make the collected information available to other road users, for example in the form of a dynamic road surface conditions map. Figure 5 illustrates the possible levels and paths which can apply to the distribution of vehicle-specific data.

26 The Ko-FAS research initiative http://www.kofas.de/
27 See https://seeroad.uni-bremen.de/

Fig. 6

Representation of transferred sensor data on a backend



This is, in principle, already technically feasible. Figure 6 shows a possible way of presenting information from sensor data as an overlay on a standard map. However, there are still a diverse range of challenges that need to be addressed in the area of distributed sensor information. These include, among others:

- Data security: What impact do defective data, erroneous data, and potentially manipulated data have on vehicle systems?
- Data sovereignty: Who is responsible for the data collected – before, during, and after transmission?

The question of data security is critical, because the data must potentially be routed along different channels through multiple networks (e.g. the mobile telecommunication networks and the Internet) during transmission from one road user to another, and these transitions always represent a security risk.

Top 5

Short summary of Chapter 3

- *The core of the new mobility is data. The collection of data occurs on both the vehicle side and on the infrastructure side.*
- *The infrastructure-based collection of data will increase significantly through smart cities and autonomous vehicles.*
- *Data transmissions are segmented into the concepts Car-to-X, Car-to-Car, Car-to-Infrastructure, and Car-to-Mobile.*
- *Prominent examples for the exchange of data from connected vehicles are Over-the-Air updates and diagnosis, and cooperative driving for the transmission of critical traffic situations to other vehicles.*
- *Through the many interfaces and wireless transmissions, more and more cars are becoming part of the Internet of Things*

4. Cyber Security of Connected and Autonomous Automobile Systems

The interconnection of the automobile harbors enormous potential for new technical features. It is creating new business models, such as in the areas of ride and car sharing. Other business models are expanding: For example, functionalities for already purchased cars can be activated over the Internet for a fee.

At the same time, it presents the automobile ecosystem with a range of threats which it has not been exposed to previously. Vehicles are suddenly becoming vulnerable to attacks from the Internet. The technical challenges for IT and cyber security in relation to autonomous and Connected Cars frequently do not differ greatly from those found in other IT landscapes, like smartphones and desktop PCs. A software update can represent a potential gateway for attackers, and must be secured, for example with digital signatures. Regular updates are absolutely essential in order to react to new threats and to continually guarantee the security of the system. However, IT security in the automotive sector also faces several challenges that do not arise in other market segments.

4.1 Challenges for IT security and cyber security

A modern vehicle contains a multitude of electronic control units (ECUs). The individual control units differ from one another strongly with regard to software and hardware. The ECUs are interconnected via diverse network technologies and communicate over diverse protocols, often automobile-specific.

The diagnostics described in the previous chapter provide a good example. Control units in the vehicle offer diagnostic interfaces, which service personnel or the customer can, potentially without physical access to the vehicle, gain access to. ECUs can also receive and analyze the diagnostic data from other ECUs; in order to display a warning sign in the driver's field of view, give an acoustic warning, or trigger an action of the control unit of an autonomous vehicle, for example. In the case of remote access, the diagnostic data is routed over a control unit with Internet connectivity, in order to be able to actually leave the vehicle.

Typically, the vehicle architecture for the control unit is intended for a fixed and defined number of tasks – for example, engine control or receiving signals from a transponder key. Many control units fulfill multiple tasks simultaneously, such as the Infotainment system, which often also displays information about tire pressure and other diagnostic data. In this way, an overall vehicle architecture is created, in which functionality is coupled with specific ECUs. As a result, different models and different series of one model have a similar number and a similar type of ECUs at their disposal.

From the perspective of IT security, however, it is a mistake to believe that the ECUs are the same, or at any rate similar, across the various series and models and that they could, as a consequence, be installed also in subsequent models in order to transfer a vehicle function to the new product, like a building block. ECUs in various projects are often produced and programmed by different suppliers. Not least as a result of this, the capabilities and the functions of the ECUs change with regard to the hardware and software, even when the functionality visible to the customer remains the same. In addition, new functions are usually introduced to the market in new vehicles. These functions are enabled by new ECUs or through the further development of existing ECUs.

A security concept for the vehicle which makes assumptions about the ECUs to be built into it can therefore quickly become invalid and is no longer transferable to new series. The developers of an ECU could, for example, assume that the data processed by the ECU is not critical from a data protection perspective, and therefore forego the encryption of this data, or even store the data upfront in error reports. Now, if a GPS stamp is added to this sensor data in a new model, this assumption is no longer valid. Thus, existing solutions can suddenly become insecure, even though they previously had had an acceptable security level. This can result in the unsecured storage of personal data, without anyone noticing. Consequently, it is also not possible to get customer consent. The strongly heterogeneous organizational structure of the automotive industry reduces communication between the developers and thus hides such problems. In contrast to functional errors found while testing the vehicle, such an error can remain without apparent consequence – at least until an attacker exploits the problems or they become publicized.

4.2 Threat models and redundant security as preventative measures

This kind of problem can be countered with a combination of measures. Firstly, the threat model should be kept up-to-date. This is the list of threats and their countermeasures. If these countermeasures are based on assumptions about the network topology or the hardware of an ECU, then the assumptions no longer apply. Threat models are an indispensable tool in the development and maintenance of secure systems. In the automotive industry, as a result of the heterogeneous project structures, they are particularly suited to detecting errors systematically and early. If it is explicitly stated in a threat model that the threat of unauthorized reading of data has not been taken into account because the data is seen to be non-critical, this can be detected when the requirements change.

As essential as threat models are, they require active examination of the system and of changing specifications. It is, in turn, becoming more difficult to manage this weighty task due to the sheer number of ECUs and developers, particularly when every small change means that the specifications of the entire threat model need to be reworked. To remedy this, it is helpful to make as few assumptions as possible and instead to keep the design conservative. In other words: The more threats that an ECU can confront independently, the fewer limitations its use will place on the overall system. In the case described above, one can forego the assumption that the data is non-critical. Then, all data is handled as potentially in need of protection, leading to the need to make use of encryption and strong authentication. In this case, the stored data remains secure even if it is suddenly transmitted via the Internet. Analogous to functional safety, a conservative design with redundant security measures offers the best way of securing a system against changing architecture and technology.

In conjunction with autonomous and Connected Cars, the landscape described above is even more heterogeneous. Cooperative driving, as described above (see Section 3.4), demands the exchange of data, in particular sensor data, from the vehicle to the outside. Data is now not only generated by the on-board network and it is not only processed in the on-board network of the vehicle that collects it. This form of interconnecting the vehicle, at the latest, therefore means that the threat model of the vehicle must on principle assume unsecured transmission channels. The origin of data must be checked and the prospective recipient of the data must be authenticated. From a cryptographic perspective, there should no longer be a differentiation between own data and data from external sources. All data should be authenticated, validated and, if necessary, protected with the same levels of caution and care.

4.3 Lifecycle and software updates

Alongside the strongly heterogeneous nature of the automotive industry, there is also a second difference to the classic IT industry. While modern consumer electronics devices, such as smartphones, smartwatches, tablets and laptops have a normal lifetime of just a few years, the lifetime of a car is considerably longer. A vehicle may often be in use for over 20 years. Manufacturers guarantee the availability of spare parts for a period of approximately 10 years. In the main, cars are not further developed substantially within this time period, which is also as a result of the business model which limits the manufacturer's costs to the development and production phases. Until now, this has also included software. The long lifetime and the ending of development at the beginning of production have a profound effect on IT security.

Firstly, no modern software product is left long-term in the state in which it was initially brought to market. Many business models are based on services which adapt to new challenges, contexts, and functions. Updates are thus a familiar part of the use of almost every digital product. New functionality can be made available, sometimes for a fee. More often, though, updates rectify problems and errors in the software. Many of these errors are IT security errors. Some are purely functional problems.

The enormous importance that software updates have for IT security cannot be emphasized enough. Software contains security-critical errors and these errors must be remedied. Security-critical errors arise, in contrast to functional errors, not only through carelessness or a lack of testing. They also arise through the always evolving development of attack methods. A recent example for this kind of error are the vulnerabilities Meltdown and Spectre in modern processors, which emerged at the beginning of 2018. Before these vulnerabilities became known, no defense strategy against them could be developed, because these kind of threats were themselves unknown. Quick updates are the only way to counter such threats.

4.4 Keeping encryption and protocols up-to-date

A closely related problem is that of aging cryptography. In many areas of IT security, cryptographic methods are used. Network traffic, for example, is encrypted, and communication partners are authenticated by means of cryptographic protocols. In the already discussed example of software updates, cryptography is an irreplaceable component. In the form of signatures, it serves as protection against manipulation, and verifies that the update comes from the producer. If this signature is circumvented by an attacker, for example because the signature process is no longer secure, the attacker can, in some circumstances, install any software onto the control unit – which can have grave consequences for life and limb.

Cryptography and protocols that are built on cryptography are continually reworked and adapted on the basis of new incidents. For example, the widely-distributed TLS protocol, with which a connection between the browser and the bank website, but also between vehicle and backend is secured, is now available in Version 1.3. Older versions, like 1.0, are seen as obsolete and insecure today. There are 19 years between these two versions – there are cars that are older than this on our roads. These jumps between versions also need to be taken by manufacturers for old vehicles, in order to guarantee the security of the system for a period of 10 years or more.

In conclusion, it can be said that the automotive industry, through its network of suppliers and their sub-contracted firms, is enormously complex. This complexity is increased through the multitude of models and series produced by the manufacturers. This is an enormous challenge for IT security, which can only be countered through systematic threat models on the part of the OEMs and through consistently conservative security architecture. Given that errors inevitably occur and attack methods are also continually developing, software updates for all ECUs are an indispensable component of a sound security concept.

Finally, it should be mentioned that we have not looked here at the specific technical challenges of the Connected Car. These include, among others, the securing of data traffic between the vehicle and the backend, and the protection of software in the vehicle – or during transmission to the vehicle, for example, during an update – against manipulation. These problems hardly differ on a technical level from their counterparts in related disciplines, like cloud services, which are dependent on constant and secure connections, e.g. in telemedicine and connected production management. The securing of devices and updates has already been solved for smartphones, and these solutions are transferrable. Equally, the Internet industry is aware of the methods of securing network communication. They are nevertheless central responsibilities of the automotive industry. The special challenge will be to transfer the existing solutions to the automotive ecosystem, which – as described above – is not always compatible with the IT industry.

Interview

"Cyber criminals are no less restrained with cars, on grounds of conscience, than they are in other areas."

Interview with Prof. Norbert Pohlmann, Board Member for IT Security, eco – Association of the Internet Industry

Cars are communicating more and more with each other and with their environment. As a result, they also attract the attention of cyber criminals. Prof. Norbert Pohlmann, Board Member for IT Security in the eco Association, calls on the industry to cooperate more, in order to jointly accomplish the greatest possible level of security.

Prof. Pohlmann, what are the IT security challenges in the Connected Car?

In the past, the IT in cars was isolated from the outside world. As a result, unwanted access from outside was not possible. In the meantime, more and more systems in cars are connected, for example, for navigation or the automatic emergency call system eCall. Added to this are systems for infotainment, or the automatic payment of parking fees and tolls, or Car-to-Car communication. In the future, cars will drive themselves. Then they will be dependent on even more information from the outside world – from the traffic control systems through to the traffic lights.

What are the specific dangers?

Through extensive interconnection, complex IT ecosystems develop in which hackers can search for attack possibilities. As soon as they discover a vulnerability, they will exploit it. For example, they could attempt to place a blackmail Trojan and demand a ransom with the threat of immobilizing the car. The list of possible attack vectors is long, and we cannot expect cyber criminals to be more restrained with cars, on grounds of conscience, than they are in other areas.

Given the dangers, should we just forego connecting cars in the first place?

Autonomous driving offers the opportunity to strongly reduce the number of traffic fatalities. Choosing not to take advantage of this opportunity due to a fear of failure is surely going in the wrong direction. Connected Cars will be safe if we make this our goal today. There are high expectations of the German automotive industry, when it comes to the reliability and security of the Connected Car. Manufacturers need to start working now towards fulfilling these expectations.

Prof. Norbert Pohlmann,
Board Member for IT Security, eco – Association of the Internet Industry

What do you expect specifically of the automotive industry?

The automotive industry needs a collective strategy for the infrastructure of the Connected Car. Only in this way can secure and trustworthy data exchange be guaranteed for everyone. The core of this strategy must be cross-company standards – be it for the assistance systems, for recharging batteries, or for authentication to open and start the car. Currently, every carmaker is working on its own infrastructure. This just increases both the complexity and the risk of vulnerabilities. Only by means of general standards and certificates that demonstrate a well thought-out, reliable, trustworthy, and secure infrastructure, can the security of Connected Cars be ensured in the long run – a basic prerequisite for people to accept self-driving cars.

Top 5

Short summary of Chapter 4

- *Through the extensive interconnection of cars, IT ecosystems develop in which hackers can find attack possibilities. The complexity is increased by the variety of models and series of components.*
- *A big challenge in the area of cyber security is changes in the individual electronic components through further development or changing suppliers. This can be countered by threat models and an innovative and global IT security architecture.*
- *Differentiation between data collected by the vehicle itself and data from external sources results in a limitation on IT security. Data protection is becoming a comprehensive task.*
- *Long-term availability of software updates is urgently required, because the lifecycle of a car is often several decades long.*
- *Encryption technologies and protocols must be kept highly up-to-date*

5. Data Protection

Due to the growing degree of automation and interconnection of vehicles, the exchange of data between cars and infrastructure is increasing. This is necessary to keep information-based systems up and running. However, since the European General Data Protection Regulation (GDPR) came into force, the exchange of data and the right to process data are subject to clear rules which have international applicability. Nevertheless, the GDPR is not the only data protection regulation and it does not apply under all conditions.

5.1 Data protection legal framework conditions

Data protection law serves to protect natural persons with regard to the processing of personal data (Art. 1(1) GDPR). It has a primary goal: Data subjects should be able to decide who processes which data, for what purpose, and why. This also applies to mobility.

Since 25 May 2018, the General Data Protection Regulation (GDPR) has been directly applicable law in all EU Member States as an EU regulation to regulate the protection of personal data. In principle, it takes precedence over national regulations that have the same scope of application. The German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG), which came into force at the same time on 25 May 2018, is limited to regulating issues which the GDPR calls for or exceptionally allows for national regulation.

In addition, special data protection regulations in the German Telecommunications Act (TKG) (Sections 91 et seq.) and in the German Telemedia Act (TMG) (Sections 11 et seq.) are also relevant for the present context. At present, the prevailing view is that Sections 11 et seq. of the Telemedia Act will be completely superseded by the GDPR. Certain provisions of Sections 91 et seq. of the Telecommunications Act will continue to apply under Art. 95 GDPR. This unclear legal situation is due to the fact that German legislators have not yet provided the necessary legal clarity by repealing the provisions of telemedia and telecommunications law or adapting them to the requirements of the GDPR.

Furthermore, the ePrivacy Regulation[28] currently under discussion may be applicable to Connected Cars in the future, in particular, to the extent that data is transmitted electronically. The ePrivacy Regulation's primary aim is the protection of personal data during communication in public communication networks.

5.2 Scope of data protection law

The GDPR applies to the fully or partially automated processing of personal data and to the non-automated processing of personal data stored or intended to be stored in a file system (Art. 2(1) GDPR).

In the present context, it can be assumed that data processing is typically automated. It is therefore decisive whether personal data are processed. Art. 4(1) GDPR defines "personal data" as all information relating to an identified or identifiable natural person. This person is referred to as the "data subject" in the GDPR. An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art. 4(1) GDPR). Recital 26 of the General Data Protection Regulation provides further indications as to how the personal reference is to be understood:

> *"...To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. ..."*

There has been ongoing controversy for years in Germany concerning the question of when someone is identifiable. According to a decision of the European Court of Justice in the Breyer vs. Germany case, a data subject is identifiable for a data processor when the

28 The Electronic Communications Code is an EU directive which deals with the legal and technical framework for the provision of electronic communications services and electronic communications networks and is intended to create uniform standards within the EU. The legal aspects of data protection are to be regulated primarily by the ePrivacy Regulation, as it stands at the time of going to press.

processor can connect the data – also using further information from third parties – to a natural person (the so-called subjective approach). Contrary to the so-called objective approach, however, the processor is not considered to have access to all and any arbitrary findings, but only to those which can actually be accessed under consideration of the aforementioned criteria. The whole question remains legally controversial.

Conversely, however, it also becomes clear that high standards apply to the anonymization or anonymity of data which is not subject to data protection law. Recital 26 GDPR contains the following statement (which follows the above quotation):

> *"... The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."*

It is important to differentiate between anonymization – which does not allow any conclusions to be drawn about a natural person – and pseudonymization. Article 4(5) GDPR defines pseudonymization as:

> *"... the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".*

Pseudonymous data is a subset of personal data and is therefore subject to the protection of the GDPR. However, this special form of personal data can give rise to legally-relevant special constellations: If, for example, the operator of a vehicle fleet stores the movement data of their vehicles in order to forward running performance data for monitoring and controlling wear to a maintenance company, the data for the fleet operator and the maintenance company can sometimes have completely different data protection qualities. The fleet operator knows which vehicles are assigned to which persons and therefore the mileage data is always personal data. The maintenance company, on the other hand, only receives the pure mileage data of all vehicle types in the fleet. However, it does not know which persons the vehicles are assigned to. Therefore, it can sometimes be possible that a set of data constitutes personal data for one recipient, while another recipient cannot attribute the same set of data to any natural persons. This circumstance must be taken into account when creating the data processing systems.

It is thus clear that the scope of data protection law is broad and that the requirements for its application are not high.

Whether the data subject is a consumer or an entrepreneur is not decisive for the application of the GDPR.[29] Data protection law is not a consumer protection law. On the other hand, data relating exclusively to legal persons are excluded from the scope of protection of the GDPR. This includes, for example, data about limited liability companies, stock corporations, or registered associations.[30] A special feature, however, is that the data protection provisions of the German Telecommunications Act (TKG) (see below for more details) and in all likelihood the EU's planned ePrivacy Regulation also apply to legal entities.

The protection of the GDPR therefore also does not apply to pure machine data. However, if such data can be related to a natural person and contain a statement relating to this natural person, they are also considered personal data:

- For example, data on the "wear and tear" of the vehicle during fully autonomous driving is at first glance purely factual information for the maintenance interval and therefore not personal. As soon as this data can be attributed to a person (e.g. contractual partner, lessee, insurance policy-holder), it can (also) be personal data, and data protection law must be observed. It is important, however, that such identification can result not only from such a direct reference, but also indirectly, if the connection can be established on the basis of other, further information from the data processor. This could, for example, be the case if the data processor does not originally know to whom the car was assigned for use (e.g. if the lessee is a legal entity), but can determine who is actually using the car on the basis of a payment, personal contact in customer service, or a registration.

29 A registered merchant (in German: eingetragene Kaufmann (e.K.)) is a natural person and therefore protected by the GDPR.

30 It is disputed whether and in which cases the GDPR applies to partnerships like the German non-trading partnerships (Gesellschaften Bürgerlichen Rechts – GbR), general partnerships (offene Handelsgesellschaften – OHG), and private limited partnerships (Kommanditgesellschaften – KG).

The extent to which such driving history data can be related to individuals has already become clear. In 2016, a driver of a car from a rental fleet was identified on the basis of their registration data and the blame for a traffic accident was proven on the basis of an analysis of the driving history recorded and stored by the vehicle.

- This is not just relevant for the processing of machine data, there is also the question of whether data relating to humans are processed along with data on legal entities. This can be the case, for example, if a legal entity (e.g. limited liability company) is the formal contractual partner, but the provider nevertheless knows the actual user (e.g. the managing director). Even if this is not the case for the provider, data protection law can still apply in the internal relationship, for example between the company leasing the car and the employee who uses the car.

Whether machine data constitutes personal data or data related to the people "behind" legal entities is something that must be evaluated individually in concrete cases. It is clear, though, that no sweeping "exclusions" of data protection law can be made.

5.3 Which data protection act is applicable?

The GDPR is not the only law in Germany that contains data protection provisions. In the opinion of the vast majority, the data protection provisions of the Telemedia Act (TMG) – as already mentioned above – are superseded by the GDPR. However, the data protection provisions of the Telecommunications Act (TKG) and the planned ePrivacy Regulation remain applicable.

The data protection provisions of the TKG and the planned ePrivacy Regulation contain special provisions for the processing of data arising in the course of and as a result of transmission via communications networks (in particular for location data). With regard to the admissibility of processing, these data protection provisions are "stricter" than the GDPR, as they do not provide for admissibility on the basis of a weighing of interests, but only in the cases explicitly regulated by the data protection provisions. However, these admissibility provisions are not tailored to the contexts of Connected Cars or IoT. As a result, there is a (too) narrow legal framework for Connected Cars or IoT in practice.

Art. 95 GDPR does not impose any additional obligations on the GDPR "in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC." In the prevailing view, the provisions in the data protection provisions of the TKG for providers of publicly accessible communications services continue to apply, insofar as the provisions in Sections 91 et seq. TKG are based on Directive 2002/58/EC.

In order to determine whether the data protection provisions of the TKG apply instead of the GDPR, the following aspects must be examined – a simplified summary of the process.

- Data must be collected as part of a publicly accessible communications service within a public communications network. The TKG is less likely to be applicable to vehicle diagnostic systems. This may be the case for vehicle manufacturers who provide the user with a telecommunications connection in order to use it to communicate or for use applications over the Internet. The evaluation of SOTA and the exchange of sensor data will depend on the type of update and the contract with the customer. The decisive factor will therefore be whether the car is only connected for the provider's own purposes or whether it (also) serves to communicate with the user.
- The data protection provisions of the TKG then apply with regard to the inventory, traffic, and location data associated with the publicly accessible communications service.

Otherwise, the provisions of the GDPR apply. Ever since the GDPR became applicable, the details of this delimitation have been controversial. The legislator has still not yet adapted the scope of the data protection provisions of the TKG to the context of public networks at the time of going to press.

It is currently unclear whether, when, and with what scope the ePrivacy Regulation will enter into force. It is intended to replace the ePrivacy Directive 2002/58/EC, which was implemented in Germany in the data protection provisions of the TKG. The data protection provisions of the TKG would then be superseded by these and would have to be repealed by the German legislator. The discussion on which law is applicable therefore continues to play a role.

5.4 Who is responsible for data protection?

The GDPR designates the person responsible for data protection as the controller. The controller is defined in Art. 4 No. 7 as follows:

"the natural or legal person, public authority, agency or

other body which, alone or jointly with others, determines the purposes and means of the processing of personal data [...]".

The decisive factor is therefore who actually decides on the purposes and means of the processing. Even if two controllers jointly determine the purposes and means, each remains responsible for compliance with the obligations of the GDPR. In its decision on Facebook fan pages, the European Court of Justice used the predecessor regulation in the Data Protection Directive 95/46/EC to specify criteria on the basis of which joint responsibility must be assumed.

The European Court of Justice has also clarified that joint control does not require uniform co-determination of the purposes and means of data processing. In this context, it may be sufficient for one controller to "initiate" the processing by the other controller. The requirements for such an initiation have not yet been conclusively clarified in individual cases. A further criterion is that one person benefits from the data processing of the other. The significance and application of these criteria is currently the subject of controversial debate, as it is apparent that it is not easy to use these criteria to draw the line between separate, sole responsibility and joint responsibility.

A crucial change – from the German point of view – brought about by the GDPR is that further data protection regulations apply if two or more controllers jointly determine the purposes and means of data processing. In this respect, they are jointly responsible.

This modification is likely to be of great significance in the area of Connected Cars, but especially in the area of autonomous vehicles. As explained in Chapter 3, a large amount of sensor data and other usage data is generated in the vehicles, which does not necessarily have to be collected and processed exclusively by the vehicle manufacturer. Rather, it is conceivable that other companies, such as maintenance and repair companies, insurance companies, or providers of on-board entertainment programs, may also process the data generated in or by the car for their own purposes. In this respect, it is obvious that these bodies will act as joint controllers with regard to the data to be processed.

Joint controllership has far-reaching consequences for those involved:

- Pursuant to Art. 26 GDPR, the joint controllers must regulate among themselves who fulfils the rights of data subjects (information, rectification, erasure, data transferability, right to be forgotten, etc.) and in what way, and must make the essential elements of this agreement known to the data subject.
- They may be jointly and severally liable for damages in the external relationship under Art. 82 GDPR.

However, joint controllership should not be understood to imply any facilitation with regard to the joint processing of personal data. Each of the persons responsible is treated as an independent controller under data protection law and must be entitled to process data themselves within the meaning of Art. 6 GDPR. Joint controllership is not a legal basis for data processing.

The GDPR defines the processor as a further data processor. According to Art. 4(8) GDPR, this is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Art. 28 GDPR specifies that a processor may not decide on the purpose and means of processing. They may only act in accordance with instructions.

In summary: The GDPR differentiates between processors with different requirements and different relationships to each other. When deciding on how to manage data processing and how to offer services to data subjects, it must be specifically examined who, within the meaning of the GDPR, decides on the purposes and means of processing alone (controller), together with (an) other so-called joint controller, or vis-à-vis a processor acting in accordance with instructions (order processing).

In the context of the development and implementation of Connected Car applications, a concrete assessment must therefore be made at an early stage as to whether joint controllership applies as a result of the initiation of data processing or for other reasons. This results in further requirements for data processing. For example, manufacturers, insurers, and car-sharing providers can be joint controllers if they jointly determine the means and purposes of processing personal data.

For the sake of completeness, it should be pointed out that, in certain constellations, the special provisions of employee data protection according to Section 26 of the German Federal Data Protection Act (BDSG) in conjunction with Art. 88 GDPR can be applied. This applies, in particular, if the contractual partner is not directly the user him or herself, but the car is provided by the employer and the employer (also) processes personal data from the Connected

Car applications. This means that while the general data protection regulations of the GDPR apply between the provider and the employer, the employee data protection regulations apply between the employer and the employee. The employer is then considered to be the controller in relation to the employee.

The yardstick for the legality of data processing in these constellations is basically the necessity of data processing for the performance of the employment relationship. In this respect, it must be carefully examined whether and if so to what extent the analysis of the vehicle data can be assigned to the employment relationship and the data are processed for the purposes of the employment relationship. The prerequisites for the protection of employee data are interpreted narrowly and the necessary criteria for an employment relationship as specified in Section 26 BDSG will not exist in every constellation. Whether and to what extent the admissibility provisions of the GDPR (in particular the balancing of interests pursuant to Art. 6(1)(f) GDPR) can also be applied is controversial and must be assessed on a case-by-case basis. The consent of the employee will typically not suffice as effective consent must be voluntary; at least, legal practice often disputes the ability to freely make a decision and thus whether consent is indeed voluntary due to the inherent dependency in the employment relationship.

5.5 Data protection law: Requirements for admissibility and documentation

With the commencement of application of the GDPR, in addition to the admissibility assessment (see section 0), strictly defined regulations on the documentation and organization of compliance with data protection have come into force (see sections 0 and 0). This is the actual paradigm shift in data protection law as a result of the GDPR.

These requirements are not Connected Car-specific but apply generally to all processing of personal data. The documentation requirements will not in themselves lead to the inadmissibility of data processing. But their non-observance is nevertheless subject to a fine.

A concluding presentation of these new requirements due to the GDPR is also not possible in this guideline and would shift the focus of content. In order to clarify the scope, individual aspects will nevertheless be dealt with in the following.

5.5.1 Admissibility of processing

Data protection law is characterized by the principle that any processing of personal data is inadmissible unless the data subject has consented, or a law permits or orders the processing in accordance with the GDPR (so-called prohibition with reservation of consent; Article 5(1)(a), Article 6(1) GDPR). In addition, there is the principle of purpose limitation, according to which the admissibility for the respective processing purpose must be examined (e.g. contract execution and advertising are two different purposes) (Article 5(1)(b), Article 6(4) GDPR).

In the context of Connected Car applications, the following factors must be considered:

- The fulfilment of a contract with the person whose data are processed (Article 6(1)(b) GDPR),
- The balancing of interests (Art. 6 (1)(f) GDPR), and
- Consent, whereby the voluntary nature thereof must be carefully examined (Article 6(1)(a) GDPR).

In the example of the over-the-air update mentioned above, the processing of personal data is probably also necessary in order to assign the update to the correct vehicle. This is particularly the case if updates or additional functions are offered at a surcharge. Since the update is either installed on the basis of a (chargeable) additional agreement or is necessary for the operation of the vehicle (and thus is at least part of the manufacturer's warranty, perhaps even of the purchase contract), processing will usually take place here to fulfil a contract.

5.2.2 Transparency of processing

The transparency of data processing is an essential element of the data subject's right to self-determination, which is why compliance with the relevant requirements has always enjoyed the particular attention of data protection supervisory authorities. Articles 13 and 14 of the GDPR outline comprehensive obligations of controllers to inform data subjects, which are proactively structured. These are comprehensive in terms of content (among other things: processors, purpose of processing, legal basis, deletion regulations, transfer to third countries, recipients or sources of the data) and can be triggered by various processes:

- data collection,
- processing for a specific purpose,
- the intention to transfer the data to a third party, and
- when the data are not collected directly from the data subject (e.g. from other data processors or from the Internet).

Especially in complex data processing, this obligation to inform and the provision of information at the right time becomes a challenge.

In connection with Connected Cars, personal data is collected from participants (e.g. drivers), but also from third parties who have no relationship to the controller. However, both groups of persons must be informed in accordance with Articles 13 and 14 GDPR. One possible solution could be, for example, that the persons are informed by the provider – similar to detailed call records in the telecommunications sector – and that no further information is therefore required from the other parties involved.

The challenge is not only how to inform data subjects, but also who should do so. The GDPR specifies that the controller (see above) has the obligation to inform. There are always several parties involved in the operation of an autonomously driving car who may be obliged to provide information. Practical experience shows that the controllers must coordinate in order to find a practicable and yet data protection-compliant way of fulfilling transparency obligations.

Those responsible will often act as joint controllers (see section 5.4). In this case, they are even obliged to determine how to fulfill the obligations towards the data subject.

These legal questions and their practical implementation must be taken into account as early as the design phase for a Connected Car.

A further question also arises in the context of the use case "Cooperative Driving" (see Chapter 3.4). If, during the exchange of sensor data, further data are transmitted which at least indirectly allow conclusions to be drawn about a natural person, and if personal data are therefore transmitted, the data subject must in principle be informed in accordance with Articles 13 and 14 GDPR. Whether the method of transmission is such that the provision of the mandatory information would require a disproportionate effort pursuant to Art. 14(5)(b) GDPR can only be conclusively assessed once the use case has been finally determined and the data exchange can be fully analyzed.

5.5.3 Principles and documentation requirements

The principles governing the processing of personal data are governed by Art. 5(1) GDPR. This must be observed with regard to any processing of personal data. These principles are particularly important because they are subject to the controller's "accountability" as defined in Art. 5(2) GDPR: The controller must ensure compliance with the data protection requirements and must be able to prove compliance with them. This duty to provide evidence addresses the central regulation of documentation (in addition to the list of processing activities (Art. 30 GDPR) and the transparency regulations (Art. 13, Art. 14 GDPR).

The regulations require a fundamental, case-by-case data protection assessment of every processing operation involving personal data and the documentation of this. A central connecting factor here is the designation of the controller, because every controller is obliged to do this for themselves. Even in the case of joint controllership, the duty of documentation must be fulfilled by each controller.

5.6 Who is protected if the contractual partner and the user are not the same?

The GDPR protects the "data subject", i.e. every natural person in accordance with Art. 4(1) GDPR, in relation to whom data is processed (see above). In this respect, the scope of protection of the GDPR is broad. In the area of Connected Car applications, all data subjects are protected, regardless of whether they are the keeper of the car, the driver, or third parties affected by the processing.

A comparison with the data protection provisions of the German Telecommunications Act (TKG) opens up a new line of thought: Connected Car applications show a distribution of roles that are similar to the distribution foreseen in the data protection provisions of the TKG. The TKG distinguishes between "subscriber" and "user". The subscriber is the contractual partner of the data processor (cf. Section 3(20) TKG). The user is the party which uses an application but is not the contractual partner (cf. Section 3(14) TKG). This distinction is interesting, on the one hand, because the terminology enables a differentiation of roles and, on the other hand, because the TKG also differentiates between these roles in the admissibility and transparency regulations. This constellation is particularly suited to Connected Car applications: the contractual partner with regard to the vehicle or the Connected Car application on the one hand, and the other users on the other.

A similar differentiation in roles should also be implemented in Connected Car applications. The introduction of differentiation is not an option in the GDPR. However, this differentiation makes the differences between these roles clear for the admissibility assessment and the implementation of the transparency requirements. This is because the involvement of a contractual partner is different

to that of a mere user, who is often unknown to the provider. In addition, the GDPR also allows for the design of graduated information structures on the basis of the identification of the differences between the various roles, for example by obliging the contractual partner to inform each user to whom they entrust the vehicle.

In any case, the TKG data protection provisions show that a conceptual differentiation of roles leads to clarity in evaluation and design.

5.7 Privacy by Design and by Default

The GDPR regulates requirements for the processing of personal data under the heading "Data protection by design and by default" in Art. 25 GDPR. The regulation addresses all controllers, including the manufacturers of vehicles and sensor technology.

"Data protection by design" outlined in Article 25(1) of the GDPR requires that appropriate technical and organizational measures be taken – like for example pseudonymization – which effectively implement data protection principles such as data minimization, and that the necessary safeguards to comply with the requirements of this regulation and to protect the rights of data subjects be included in the processing. This should be done both at the time when the resources for the processing are determined and at the time of the actual processing, taking into account the state of the art of technology, the implementation costs, and the type, scope, circumstances, and purposes of the processing, as well as the various probabilities of occurrence and the severity of the risks associated with the processing for the rights and freedoms of natural persons.

The Connected Car application must therefore be designed from the outset in such a way that as little data as possible is processed for the intended purpose. For systems in Connected Cars which are intended to avoid collisions with cyclists or pedestrians, for example, this means the following: in accordance with the aforementioned principles, the systems must be technically designed in such a way that they reliably recognize pedestrians and cyclists as other road users, but cannot personally identify them. This can be achieved, for example, by using only low-resolution imaging systems that in themselves exclude the identifiability of an individual. Alternatively, the systems in question could be technically designed in such a way that the data collected for collision avoidance is already anonymized at the time of collection.

Furthermore, data protection by default pursuant to Art. 25(2) GDPR requires that the controller takes suitable technical and organizational measures for the respective data processing, which ensure that – by default – only personal data which is required for the respective specific processing purpose is actually processed. This obligation applies to the amount, the scope of processing, the retention period, and the accessibility of personal data collected.

The second approach is based on the application itself. Data processing per se is not prohibited, but rather the applications provided must be set in such a way that – upon delivery – unnecessary processing is deactivated and must be activated by the data subject.

5.8 Security of processing and data protection impact assessment

The "security of processing" is part of the protection of personal data. Despite the conceptual proximity to IT security, the protection objective is not the same as that of IT security, which aims at the basic protection of IT systems.

5.8.1 Security of processing

The GDPR has fundamentally and significantly extended the security requirements for processing compared to previous data protection law (cf. Section 9 of the older version of the German Data Protection Act (BDSG)). The principle is laid down as follows in Art. 32(1) GDPR and is elaborated upon in the further paragraphs of Art. 32 GDPR:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".*

On this basis, Article 32 of the GDPR states that measures are to be determined and documented and how this is to be done. Contrary to previous data protection law, for example under the old version of the German BDSG, violations of the security of the processing are also subject to fines. This also highlights the new significance that has been accorded to this.

5.8.2 Data protection impact assessment

The data protection impact assessment introduced by the GDPR in Article 35 follows on from the requirements regarding the security of processing. If a form of processing, in particular the use of new technologies, is likely to result in a high risk to the rights and freedoms of natural persons due to the nature, scope, circumstances, or purposes of the processing, the controller is firstly to carry out an assessment of the consequences of the planned processing operations for the protection of personal data. The detailed structure is set out in the further paragraphs of Article 35.

This means that each processing operation must first be examined to determine whether such a high risk is likely to exist and, if so, a comprehensive risk assessment must be carried out. This risk may still be low for over-the-air updates, but a high risk must be assumed if extensive processing of personal data regarding the location of natural persons is undertaken on the basis of location data. In the area of autonomous driving, it will therefore be essential to carry out data protection impact assessments.

The GDPR thus demands that the risks for the data protection of the data subjects be determined before processing begins. Even if Article 35 GDPR does not result in the direct (in)admissibility of a processing operation as a result, the result must nevertheless be taken into account in the lawfulness check pursuant to Article 6 GDPR (in particular in the case of a balancing of interests). In addition, the result may require the controller to consult with the supervisory authority prior to processing the data (referred to as "prior consultation") under Article 36 GDPR.

Failure to comply with these obligations is also subject to a fine, a means by which the legislator underlines the importance of this obligation within the framework of the GDPR.

Top 5

Short summary of Chapter 5

- *The General Data Protection Regulation (GDPR) applies in the field of autonomous vehicles when personal data is being processed. This must be considered when creating data processing systems. In future, the ePrivacy Directive – which is currently under discussion – and the Electronic Communications Code Directive could apply to Connected Cars if data is transferred electronically.*
- *In the scope of application of the GDPR, not only the requirements for a legal basis for the processing of personal data must be considered, but also the strictly defined regulations on the documentation and organization of compliance with data protection.*
- *A Connected Car application must be designed from inception to process as little personal data as possible for the intended purpose.*
- *The data protection-friendly default setting must ensure that only personal data are processed whose processing is necessary for the particular purpose for which they are to be processed. This applies to the amount of personal data collected, the scope of processing, the storage period, and accessibility.*
- *All data processing in the area of autonomous vehicles must be checked to see whether there is likely to be a high risk. If this is the case, then a comprehensive assessment of the risks must be carried out, for example when extensive processing of personal data regarding the location of natural persons is undertaken on the basis of location data.*

6. Warrantee and Liability Regime for Autonomous Vehicles

Autonomous vehicles raise new challenges for warranty and liability law. Their participation in road transport and the resulting potential danger to life and limb of their passengers and other road users means there are stringent requirements for safety and functionality. In particular, the risk of errors in autonomous vehicles must be addressed before they can manifest themselves, to ensure the safety of road traffic. Therefore, there is much to be said for a preventative approach to servicing and maintaining autonomous vehicles. However, the question arises as to whether this can be derived from prevailing law, or whether the existing legal framework will need to be adapted and expanded. This chapter looks at the current legal situation in Germany.

6.1 Status quo of warrantee or guarantee claims in the purchase of a car

According to prevailing law in Germany, an automobile should not be treated differently to any other moveable object. This means that there is a legally required two-year warrantee on new cars, during which a trader is liable for defects on the car (Section 438(1)(3) of the German Civil Code (Bürgerliches Gesetzbuch - BGB)), which were already in existence at the time of hand-over ("transfer of risk"). Through the special consumer protection law ruling in Section 476 BGB, the burden of proof favors the consumer with regard to defects that become apparent during the first six months from the purchase of the vehicle. For consumers' benefit, within this time period it is assumed that the motor vehicle was already defective at the time of purchase, in so far as the type of defect for which recompense is being sought is compatible with this assumption. The right to warrantee is therefore especially suited to defects that have already manifested themselves in damage. In contrast, such defects that have only led to damage in other cases, but not (yet) in the case of the purchased object in question, can result in a higher burden of proof for the purchaser.

Warranty law applies to both the mechanical components of a vehicle and its software. Software errors can also be considered material defects. However, when it comes to software, the issue of the uncertainty of damage caused by a defect arises, as does the question of whether a defect actually exists. Particularly in the field of IT security architecture, not all errors necessarily lead to an attack, even if the respective attack vector is already known in principle. In addition, new attack possibilities become known over time (see the points on Spectre and Meltdown, as well as on encryption techniques in Sections 4.3 and 4.4), ones which were not foreseeable given the state of technology at the time of handover or the "transfer of risk". In these aforementioned cases, it is very questionable whether a defect, the legally required responsibility for having caused this defect, and, ultimately, a warranty claim exist at all.

Warranty rights do not have a preventive effect by obliging the seller to take preventive action on their own initiative against a defect that may become apparent after the sale. Rather, the statutory warranty rights only provide the purchaser of a motor vehicle with claims for the rectification of an already manifested defect and the damage caused.

Warranty rights also require that they are proactively recognized and then asserted by their owner, usually the vehicle purchaser. Indeed, there is no legal obligation for the seller to proactively offer retrofit components or software updates to remedy production faults. Warranty rights do not create any obligation to further improve the functionality or performance of a sold and functional product by offering updates or upgrades.

As a result, the warranty right is structurally designed to protect the trade relationship at the time of purchase ("The buyer is to receive what they have bought and paid for"). Further (IT) security policy considerations or the prevention of damages, however, play no role in warranty law.

The consumer-protection provisions of the German Product Liability Act (Produkthaftungsgesetz) do not lead to any other results. The Product Liability Act establishes obligations on the part of the manufacturer of a defective product to pay damages. A liability for damages, however, requires, on the one hand, the occurrence of damage and, on the other hand, is aimed at compensating for this damage. This means that the law does not create any obligation

for the manufacturer of a product to offer subsequent preventive improvements for the product, despite the obligation to pay damages.

Even the possibility of granting warranty claims, whether by the seller or by the manufacturer of a motor vehicle, does not alter this situation. Warranty claims are also aimed at the subsequent elimination of defects in mechanical components and software and any resulting damage. The only difference to the warranty for defects is that the guarantor is responsible for ensuring their product is free of defects regardless of fault, which makes it easier for the claimant to assert their claims.

Under current legislation, the statutory warranty rights, product liability law, and contractually-granted guarantees mean that manufacturers or sellers of motor vehicles are generally under no obligation to provide preventive software updates for vehicles. The decision as to whether and in what form software updates are rolled out preventively is an economic decision, which lies solely with the manufacturer or seller.

6.2 Status quo of warranty and guarantee claims in rental and leasing constellations

The legal situation for vehicle rentals is different, at least in terms of the time period. Under Section 535(1)(2) BGB, the lessor of an object is obliged to keep the rental object in a condition suitable for contractual use for the duration of the rental period as a matter of principle. This means that, in the case of long-term rental contracts, the lessor of a motor vehicle must ensure that the functionality of the vehicle is maintained for more than two years.

Nonetheless, it should be noted that numerous deviating regulations have been established in individual contracts with respect to this fundamental principle, particularly in the area of vehicle leasing, which impose on the lessee the obligation to maintain the usability of the vehicle. It is also questionable to what extent the maintenance obligation under the rental agreement also includes the elimination of security vulnerabilities in software components or the provision of software updates to maintain the necessary IT security.

For this reason, there is no fundamental and preventive obligation for lessors or vehicle manufacturers to offer software updates for vehicles under rental and leasing contract law.

6.3 Warranty claims for the transmission of data by autonomous vehicles

The scenario described above only depicts the situation in which relevant software is used within the vehicle. As explained in Chapter 3, many applications for autonomous vehicles will require data to be exchanged between vehicles and even collected and processed online, for example via cloud applications. In this case, the software interfaces of the required communication infrastructure add another security-relevant aspect. The communication interfaces must be protected against external attacks so that autonomous vehicles cannot be taken over by attackers. Moreover, if the cloud-based data processing is not carried out by the respective vehicle manufacturer itself, a further party against whom claims may be asserted may be added. With regard to any warranty claims for defects, in view of the foregoing, much depends on how the use relationship of the online infrastructure is structured in concrete terms.

Here, too, the general warranty law does not provide a fundamental right to software updates. Rather, in the case of publicly accessible cloud services for the infrastructure of these services, there is an update obligation (which, however, does not give the user a right to the updates) under the German Telemedia Act (Section 13(7)), which, in implementation of the European NIS Directive, stipulates a public law obligation to secure such services. Violations, however, are essentially prosecuted by the competent supervisory authorities and do not give users the right to sue, provided that they have not suffered any damage. Furthermore, it has not yet been conclusively clarified whether this obligation to install security-relevant updates can include the vehicles themselves in addition to the actual cloud service. For this reason, this update obligation under Section 13(7) of the German Telemedia Act can only be invoked against the vehicle manufacturer by the keepers or owners of the vehicles in individual cases.

Moreover, in constellations based on data transmission for the operation of autonomous vehicles, it should be noted that in the current legal situation the scope of applicability of telecommunications law has not been clarified. Although data transmission between vehicles and/or data transmission from the vehicle to the cloud application will regularly require data transmission via the Internet or a comparable open telecommunications infrastructure, access to this telecommunications infrastructure is likely to be regularly made possible via the software available in the car. In these cases, it is still unclear whether the application qualifies as a so-called telecommunications service and is therefore subject to the regu-

latory regime of the Telemedia Act[31]. Only in this case would the special regulations under telecommunications law, which contain regulations for continuous compliance with technical standards to protect the service against attacks, become applicable.

6.4 Status quo of compliance with regulations by the keeper of the vehicle

Under road traffic law, the owner of a motor vehicle is in principle obliged to maintain it and to comply with its prescribed operability. Compliance with the prescribed operational capability is checked at regular intervals by officially recognized bodies; Section 29 of the German Road Traffic Licensing Regulations (StVZO). The inspection to be carried out also includes in particular the functionality of the engine management system, the brake system, and the steering system (Annex VIIIa of Section 29 StVZO).

This is a relevant point with regard to autonomously driving vehicles. The control software of an automobile might indeed belong to the components of the engine management, or brake and steering systems. The consequence of this would be that the owner of a vehicle, in principle, would be obliged to rectify errors in the corresponding software components or to have them rectified. However, the current mandatory test catalogue is usually limited to the functionality and compliance with defined specifications. Only in exceptional cases are certain risks which could lead to later damage considered in addition to the general condition of the vehicle, in particular leaky lines or non-sealing cabling. In order to test the IT security of the software used in the vehicle, however, the test and requirements catalogues would have to be supplemented accordingly and corresponding test processes established at the test centers.

Should such an extended inspection detect safety defects in the software before the warranty period has expired or as long as the vehicle manufacturer still provides software updates for the vehicle, the vehicle owner will be able to fulfil their legal obligations. The situation becomes much more complicated when the vehicle manufacturer decides to discontinue software support. In this case, the vehicle owner is confronted with the problem that they may not be able to obtain services on the open market that are required for troubleshooting the defective control software.

Based on today's standards, it can be assumed that software used in vehicles in the future will continue to be manufacturer-specific and proprietary, i.e. not open source. Therefore, the necessary access to the software source code will probably not be available to third parties. The right of the vehicle owner to the decompilation of the steering software under Section 69d(1) of German Copyright Law will not be much help due to the little use of and great effort involved in doing anything with the uncommented source code. The vehicle owner would therefore be practically prevented from ensuring their vehicle is in a legally-prescribed condition. This would be an unacceptable situation, given that a critical malfunction in IT systems in the important components of the motor vehicle can lead to it no longer being able to be operated safely. This poses danger to the lives and physical condition not just of its occupants, but also of other road users.

6.5 Lifecycle of an automobile

As discussed in Chapter 4.3, IT security for an autonomous vehicle should not be a task limited to the time of delivery. Rather, road safety requires that the relevant IT security be regarded as an ongoing task extending over the life cycle of a vehicle. Indeed, it is questionable whether it should be left to car manufacturers to be able to discontinue IT support for safety-relevant features for autonomously driving vehicles – there is currently no such legal obligation. Without updates to maintain safe operation, the vehicles would be rendered practically unusable for their owners.

The background to these considerations is the question of planned obsolescence, i.e. the design of certain parts or all parts for a predefined service life that is less than the normal service life, something which has already been discussed in another context. In the case of autonomous vehicles, the normal service life could be based on either the long life cycles of the automotive sector or the extremely short life cycles of the high-tech sector. In the first case, manufacturers would be forced to operate a large number of legacy IT systems that would be hopelessly overwhelmed by the rapidly evolving IT security requirements during the life cycle of the vehicle. In the second case, the usability of the entire vehicle would be called into question as soon as the first security-relevant IT component can no longer meet the requirements – regardless of whether this is as a result of ineffective hardware, outdated software, or increased demands on the software that the hardware cannot fulfill.

31 This has been submitted to the European Court of Justice for decision, see the 26.02.2018 Decision of the Higher Administrative Court of North Rhine Westphalia (OVG NRW), 13 A 17/16.

The current liability and warranty regime – as already described – is designed to protect the trading relationship at the time of transfer ("transfer of risk"), but does not explicitly deal with the durability of a product (whether hardware or software). Therefore, commercial interests, rather than legal concerns, influence the planning of the life cycle and durability. Products flawed by (too) low durability can damage the reputation of a company, with a lasting impact for years to come. In addition, support over a long life cycle has long been a recognized business model, both in terms of hardware (e.g. the spare parts business) and software (e.g. "Software as a Service"), so that the automotive industry is also likely to have a certain interest in longer life cycles.

The consumer protection and resource consumption aspects of the premature replacement of entire fleets of vehicles must, however, also be taken into account. From the point of view of consumer protection law, transparency with regard to durability, usability, and follow-up costs is likely to be of primary importance. Since consumers are likely to understandably assume that a motor vehicle has a customary long life cycle, any restrictions and follow-up costs should be specified openly and transparently in the contract at the time of purchase (insofar as purchase remains the dominant contractual model).

From an ecological point of view and in order to reduce resource consumption, it should be possible for third-party suppliers to also maintain operational safety, at least in the event that the manufacturer discontinues support. However, this would require disclosure of the interfaces, and possibly even the source code of the software used, which is currently not provided for by law (see Chapter 6.4).

With regard to the transparency of restrictions on usability and follow-up costs, there are already some obligations to provide information under consumer protection regulations, but, at least for the time being, there is still a desire to create legal certainty quickly through short deadlines (compared to the life cycle of a vehicle). Moreover, uncertainties with regard to price calculations over several years would be virtually unavoidable. Current liability law does not provide for action against manufacturers on the grounds of false statements or a product and support policy that was changed much later.

Only antitrust law currently allows for the forced opening of the market to third-party vendors to provide long-term support. There are, however, significant barriers to accessing legally protected product components (e.g. copyrighted software) by third parties, in particular competitors. As long as the discontinuation of the respective support package is justified by reasonable economic considerations, an obligation to disclose information to competitors – at least as things stand at present – is likely to have very little chance of success.

6.6 Challenges for warranty and guarantee law

The foregoing considerations and findings show that

- firstly, the keeper of the car is usually neither actually nor legally (after expiry of the short warranty or liability periods) in a position to maintain IT security and thus operational reliability,
- secondly, manufacturers are not obliged to provide support over the entire actual service life of a vehicle, and
- thirdly, third party providers are regularly not given access to protected hardware or software components.

This suggests the conclusion that current warranty and liability law covering purchase agreements cannot satisfactorily implement the IT security requirements for the protection of all road users.

Therefore, there needs to be a discussion of the enforcement of the manufacturers' obligations to remedy or supply an appropriate security update, as opposed to the alternative of the operator being obliged to take the vehicle off the road. A decommissioning order of the relevant supervisory authority, which would have to be issued if the vehicle is not safe to operate and other road users are endangered, could lead to the owner not being able to use the vehicle without any compensation claims against the manufacturer or seller once the last limitation periods have expired after just a few years.

The testing obligations currently anchored in Section 29 StVZO pose further legal challenges. On the one hand, it must be taken into account that an autonomously driving vehicle cannot be operated safely without continuous safety updates and secure, continuously available maintenance of the control software. It would therefore be conceivable to extend the catalogue of obligations under road traffic law for vehicle owners to include an obligation to operate the vehicle using the latest software version. Violations of this could be sanctioned with compulsory deregistration of the vehicle. This would ensure a uniformly high level of safety for all vehicles involved in road traffic. It would also fulfill the government's duty of care and protection, in that unsafe vehicles can, as previously,

be taken off the road in the event of IT security risks.

On the other hand, the keeper of an autonomous vehicle cannot be left alone to ensure that its IT security is maintained – as could be done to date to ensure and maintain a roadworthy condition as required under traffic law – by simply taking it to any garage of choice. If the buyers of the vehicles are to be prevented from losing part or all usability of the vehicle without any compensation after just a few years, several options are available for adapting the legal framework. At the level of contract law, it would be conceivable to statute a certain period of use or durability as part of the so-called "target condition", i.e. the entirety of the requirements which the vehicle must fulfil in order to comply with the contract. Combined with an adjustment of the limitation periods, this would at least give the buyer financial compensation, or even a claim for rectification, in the event of a later loss of usability, which would, however, still have to be enforced individually or within the framework of a model declaratory judgement – in each case with all of the litigation risks and usual duration of civil law proceedings.

Further considerations should, however, take into account that, in the event of security vulnerabilities, not only individual vehicles but entire model series are likely to be affected in most cases. It could therefore be useful to centralize the enforcement of continued usability. In addition to purely governmental monitoring by the responsible (traffic) supervisory authorities, a right to class action could be created with regard to a claim (also to be created) for the implementation of measures to maintain the (safe) usability of all affected model series. Another possibility would be to impose an obligation on manufacturers to file all software source code and blueprints in order to make it possible for another market participant to substitute the necessary measures (e.g. the creation of updates) in the event of an unlawful refusal or the insolvency of the manufacturer. Since, however, this also involves an encroachment on the manufacturer's property rights (in particular copyright and industrial property rights), it would require careful consideration of the respective constitutionally-protected positions when drafting an obligation to file such documentation.

Finally, in view of the technical possibilities of autonomous vehicles, especially in connection with sensors and IoT or blockchain applications, perhaps the regular safety inspection of motor vehicles previously provided for in Section 29 StVZO will someday become completely obsolete. Due to increasingly sophisticated and increasingly widespread sensor technology, it cannot be ruled out from a technical point of view that an autonomous vehicle will test itself so comprehensively and, if necessary, check its road traffic conformity so continuously, transparently and in a tamper-proof manner, that it can itself ensure its legal conformity. This means that regular checks, which originate from a time when a constant data connection in and between vehicles and communication between machines was still a long way off, may one day become superfluous.

6.7 Challenges for liability regimes

With connected and fully automated vehicles, the possible causes of damage are increasingly shifting from human error to the failure of IT systems with their software and hardware components. This also means that the clarification of responsibility and liability is becoming increasingly more (technically) complex, for example when, as described in Chapter 3.4, the sensor data recorded in the vehicle is transmitted to other road users for the early detection of critical traffic situations and to avoid conflict situations. When transferring data from one road user to another, the data may need to be routed through several networks on different channels. These transfers are not only a security risk. In practice, all of these facets and the constantly increasing technical complexity result in legal prosecution quickly reaching the limits of justiciability and cost-effectiveness.

This means that the existing system of liability and compulsory insurance, the established mechanisms of law of evidence in traffic accidents, and the introduction of the relevant data records into the civil process for the purpose of investigating accidents involving autonomous vehicles must be put to the legal test. In the Internet of Things, in which countless objects communicate and operate with each other in fractions of a second, the complexity of such processes will increase considerably.

However, a full analysis of all the data collected from the vehicles involved in an accident prior to the incident would be the best way of clarifying liability. The question therefore arises as to whether an obligation to disclose (only) the data relevant to the analysis of the circumstances of the accident and the causes of damage can be enforced in civil proceedings, taking into account, for example, data protection law and the specific regulations on the protection of know-how and trade secrets, and if so, who would be obliged to do so?

The provision of Section 142 of the German Code of Civil Procedure (ZPO) is in many cases unlikely to help make the data stored in the connected automobile usable. This is because the data stored in the self-driving car are probably neither certificates as defined in Section 415 ZPO nor documents as defined in Section 142 ZPO[32]. In addition, Section 142 ZPO only authorizes the competent court to issue an order for the submission of certificates or other documents to the parties or third parties, but the parties themselves have no claim to such an order. If the investigation of an accident involving self-driving cars can only be carried out by consulting the data from the other party's car, the provisions of Sections 371 and 144 ZPO may also be applicable. It should be noted, however, that the millions of data generated in the self-driving car would have to be stored partly temporarily, partly permanently in a data or cloud memory storage unit and at the same time be electronically signed in a qualified manner and protected against alteration. If this is not the case, Sections 371 (1) (2), 144 (1) (2), and 371 (a) (1) ZPO are also ruled out as regulations for access to the data of the self-driving cars involved in an accident. This data can only be used in the context of prima facie evidence. In order for the evidential value of an electronic document to be equal to that of a private certificate, however, the electronic document must also be signed with a qualified electronic signature as defined in the Digital Signature Act, Section 371 (a)(1) ZPO.

A possible procedure for including the data stored in the automobile in civil proceedings could also be to introduce the investigation results or investigation files of the investigating authorities related to the traffic accident in question into civil proceedings. If the public prosecutor's office investigates the traffic accident, it is likely that it will seize or confiscate the stored data as non-physical objects in accordance with Section 94 of the German Code of Criminal Procedure (StPO), since these data could with a high probability contribute to the clarification of the accident and thus constitute potential evidence. The data seized and evaluated by the investigating authorities could then be introduced into later civil proceedings by means of documentary evidence. However, the decision to secure the data stored in the automobile is at the discretion of the investigating authorities in each case, and individuals do not have any claim to this data. Even more recent case law on the civil procedural exploitation of dashcam recordings, whose admissibility as evidence is only permitted by case law in individual cases after careful consideration of the interests involved, does not show any new approaches.

32 Eichele (2017), Vorb zu § 415 Rz. 1, 2; Von Selle (2018), § 142, Rz. 7, § 131 Rz. 4.

The above remarks show that access to data stored in the self-driving cars involved in an accident would, at best, only be possible to a limited extent in procedural terms. There are also data protection hurdles (see above).

However, given the immense volume of data collected, the chances of gaining useful insights from the data are higher than from human observers. It can be objectively ascertained what the IoT devices perceived immediately before the accident occurred. With humans, on the other hand, perception is subjective. For this reason, use should be made of these greater opportunities to gain knowledge, on the one hand in order to effectively assert claims, and on the other – similar to aviation – to carry out comprehensive causal research to prevent future accident scenarios. If Connected Cars cause damage, there is a public interest in unreserved clarification, especially when it comes to accidents and incidents of particular importance for road safety. The premise must be to avoid repetitions in the future, especially given the complexity of possible incidents.

A glance at the law governing aircraft accident investigations shows that, in accordance with Section 3(1) of the Law on the Investigation of Accidents and Incidents in the Operation of Civil Aviation (FiUUG), accidents and incidents are subject to an investigation with the sole purpose of clarifying the causes as far as possible with the aim of preventing future accidents and incidents.

It is stated expressly in Section 3(2) FiUUG that the investigations do not serve to establish fault, liability, or claims. However, Section 21(1) FiUUG provides, with a number of exceptions (Section 21(2) FiUUG), that the German Federal Agency for Aircraft Accident Investigation may provide the persons affected by the event or their legal advisers with information from the files of the investigation procedure or grant access to the files (Section 21(3) FiUUG) if this is necessary to establish, enforce, or defend legal claims in connection with the accident or incident. The idea that a third party who has the necessary technical analyses to substantiate a claim can be petitioned for information does already exist in civil law. For example, Section 101 (9) of the German Copyright Act provides that a person infringed in the copyright sense may request information from a telecommunications company on the use of traffic data (Section 3 No. 30, German Telecommunications Act) upon prior judicial order.

Interview

"Assistance systems have no influence at all on many causes of damages."

Interview with Dr. Tibor Pataki Head of Vehicle Insurance, Vehicle Technology and Statistics at the General Association of the German Insurance Industry (GDV)

Dr. Tibor Pataki
Head of Vehicle Insurance, Vehicle Technology and Statistics at the General Association of the German Insurance Industry (GDV)

Mr. Pataki, what is the significance of data from connected vehicles for the insurance industry?

The data from connected vehicles has the potential to provide consumers with more and better services, such as faster roadside assistance, the route to the cheapest petrol station, or direct feedback on driving styles – a new market with innovative, data-based business models is emerging. In this market, not only car manufacturers, but also automobile clubs, garages, and insurers want to make new offers to their customers in the car. At present, however, only car manufacturers have access to this data. We believe that this data belongs in the hands of consumers. Only consumers should decide whether, when, and to whom they want to transfer which data. Otherwise car manufacturers can close off the emerging market, exclude other suppliers, and reap monopoly profits – to the detriment of drivers who would get a more limited offer at a higher price.

As things stand today, insurance companies in road traffic assume liability for the driver of a vehicle. What does this look like with an autonomous vehicle?

Motor vehicle insurance is technologically neutral. Motor vehicle insurance therefore also compensates the victim in the event of accidents caused by automated driving systems. It is irrelevant to the road accident victim whether the driver is at fault or whether the accident is caused by a defective tire, for example – the road accident victim has a direct and solvent contact in motor third party liability insurance. We cannot expect an accident victim to have to prove a possible product defect to the car manufacturer before they receive compensation. Product liability law is not designed for this case. In the event of a failure of the automated driving system, the insurers will find practicable solutions with the automobile manufacturers for any recourse claims.

What revenue models do insurers have in mind in this context? The number of accidents are likely to be reduced, as human error can be ruled out.

Assistance systems have no influence at all on many causes of damages. A motorway pilot does not stop car thieves any more than a parking aid protects against cars being scratched or damaged by hail, or cables being chewed on by small animals. Even the best emergency brake assistant does not change the physical laws governing the braking distance of a car. In addition, we will now see a very slow spread of automated or autonomous systems and rising repair prices in the event of damage. According to our forecast, the claims expenditure of motor insurers will fall by between 7 and a maximum of 15 percent by 2035, compared with 2015, as a result of the new systems. Technological progress will therefore only have a minor impact on claims in the foreseeable future.

Top 5

A short summary of Chapter 6

- *In German law, there is currently no legal obligation on the manufacturer/seller to provide preventive software updates or upgrades to prevent possible damage scenarios. Manufacturers are not even obliged to install security-relevant updates under the TMG and TKG, unlike for cloud service providers.*

- *The obligation according to Art. 29 StVZO to carry out regular security checks on motor vehicles cannot easily be transferred to autonomous vehicles in terms of IT security, which is to be understood as a continuous task.*

- *The maintenance of IT security for autonomous vehicles should not be a task limited to the time of delivery for the manufacturer, as otherwise the owner is prevented from putting their vehicle in a prescribed condition and would have to shut it down if the manufacturer discontinues support for the software.*

- *It is therefore necessary to discuss the enforcement of the manufacturer's obligations to repair or supply safety updates as opposed to the alternative of a decommissioning obligation on the part of the owner, taking into account the expected or specified life cycle of an automobile.*

- *The existing system of liability and compulsory insurance as well as the established mechanisms of the law of evidence in traffic accidents and the introduction of relevant data records into civil proceedings for the clarification of accidents must be put to the legal test in the case of autonomous vehicles. This is because the technical complexity can stand in the way of the clarification of accidents from an economic point of view, although a complete clarification of the cause and responsibility for an accident caused by autonomous vehicles can be required for the common good, taking full advantage of all available sources of knowledge (in particular all data from the context of the accident).*

7. Outlook

Cars, buses, and trucks are already part of digital networks via various interfaces. If we think a little further than a decade into the future, many vehicles will not only be connected, but also fully autonomous. This means a change for society as a whole, as mobility depends less and less on car ownership and a specific means of transport, but can be booked and used as a service at any time.

The automotive industry is also facing enormous changes, as its core product to date is no longer at the center of mobility itself, but has become a transport service for the customer to get from point A to point B.

The Internet industry provides the necessary digital infrastructure with data centers, cloud services, and network connections. Its technologies will be of such great importance for the automotive industry that close cooperation with the companies in its sector is absolutely essential. The automotive industry is dependent on the infrastructure and competence of the Internet industry, which is becoming the pivot point for OEMs, suppliers, railways, and public transport.

And the Internet industry is technically equipped: Data centers already offer sufficient capacity to process the enormous amounts of data from connected and autonomous vehicles. The introduction of 5G will also mark a milestone in network speed and stability.

In a few years, autonomous and increasingly strongly-Connected Cars will be seen on the roads. It is imperative to start implementing the functionality and safety of the entire autonomous driving system and the legal framework conditions for it now. One goal is maximum cyber security so that vehicles and networks are safe from attacks. Here, too, the automotive sector will not manage without the expertise of the Internet industry to protect complex IT ecosystems from hackers: Protocols must be kept up-to-date, and cars must receive updates almost in real time – throughout the entire lifecycle. The individual electronic components require standardized security threat models. Otherwise, the essential digital infrastructure could collapse.

Data protection will become a central task in order to provide the driver and the car owner with sufficient protection of their privacy and to protect them from the unjustified interests of third parties. How the data is to be protected must already be considered during software development (privacy by design / security by design).

Although the GDPR defines comprehensive regulations, in some cases it is not clear whether other data protection provisions, for example from the German TKG, are applicable. And there are several solutions for the question of which instance is ultimately responsible for data protection. One possibility would be a Joint Controllership consisting of various stakeholders from the ecosystem. Whoever ends up being responsible will be required to implement various principles ranging from documentation obligations and processing transparency to the security of data processing. Due to the complexity of the emerging ecosystem and the large number of players involved, this will be a formidable task and should not to be underestimated.

In this ecosystem, warranty regimes also face new challenges. Some regulations concerning the obligation to provide software updates are still unclear here. However, these are essential for the safety of autonomous vehicles, since they patch detected security vulnerabilities promptly and enable the vehicle owner to comply with the regulations. Particularly serious is the uncertainty of the situation following a possible discontinuation of software updates by the manufacturer, for example for a specific type of car. These vehicles could then no longer be operated safely and the owner would not be able to do anything about it. The associated considerations and findings suggest the conclusion that German (sales law-related) warranty and liability law in its current form cannot satisfactorily implement the IT security requirements for the protection of all road users.

8. Bibliography

Bundesverband CarSharing e. V. (o.J.):
Aktuelle Zahlen und Daten zum CarSharing in Deutschland, in: https://carsharing.de/alles-ueber-carsharing/carsharing-zahlen, last visited on 11.12.2018.

Comastri, Marco (2018):
New frontiers for car security: API management, in: dotmagazine, 06/2018. Available online under: https://www.dotmagazine.online/issues/mobility-and-connected-car/connected-car-security/car-security-api-management, last visited on 04.02.2019.

eco – Verband der Internetwirtschaft e. V./Arthur D. Little (2015):
Die deutsche Internetwirtschaft 2015–2019, Köln. Available online under: https://www.eco.de/wp-content/blogs.dir/studie_internetwirtschaft_2015-2019.pdf, last visited on 13.03.2019.

Eichele Hans (2017):
Vorb. zu § 415 Rz. 1, 2, in: Saenger, Ingo (Hrsg.): Zivilprozessordnung, 7th edition., Baden-Baden.

Gasser, Tom M. et al. (2012):
Rechtsfolgen zunehmender Fahrzeugautomatisierung. Gemeinsamer Schlussbericht der Projektgruppe, in: Berichte der Bundesanstalt für Straßenwesen, H. F 83.

Grünweg, Tom (2017):
Audi ist ein Level weiter, 27.09.2017, in: http://www.spiegel.de/auto/aktuell/audi-a8-audi-ist-beim-autonomen-fahren-ein-level-weiter-a-1169062.html, last visited on 03.02.2019.

Heller, Piotr (2018):
Wie wir demnächst von A nach B kommen, 16.09.2018, in: https://www.deutschlandfunk.de/zukunft-der-mobilitaet-wie-wir-demnaechst-von-a-nach-b.740.de.html?dram:article_id=427850, last visited on 14.03.2019.

Kong, Yat Sheng et al. (2017):
Mission profiling of road data measurement for coil spring fatigue life, in: Measurement. Journal of the International Measurement Confederation, Jg. 107, S. 99–110.

SAE International On-Road Automated Vehicle Standards Committee (2014):
Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE J3016. Available online under: https://www.sae.org/standards/content/j3016_201401/, last visited on 14.03.2019.

Seiberth, Gabriel (2015):
Wie verändern digitale Plattformen die Automobilwirtschaft?, in: Baums, Ansgar et al. (Hrsg.): Kompendium Industrie 4.0. Wie digitale Plattformen die Wirtschaft verändern – und wie die Politik gestalten kann, Berlin. Available online under http://plattform-maerkte.de/wp-content/uploads/2015/11/Kompendium-High.pdf, last visited on 11.12.2018.

Sommerfeld, Felix (2018):
Wie sich die Autoindustrie neu erfindet – und unser Leben damit verändert, 15.10.2018, in: http://www.spiegel.de/wirtschaft/unternehmen/autoindustrie-wie-sich-vw-bmw-und-daimler-neu-erfinden-a-1229415.html, last visited on 11.12.2018.

Verband der Automobilindustrie e. V. (2015):
Von Fahrerassistenzsystemen zum automatisierten Fahren, Berlin. Available online under: https://www.vda.de/dam/vda/publications/2015/automatisierung.pdf, last visited on 14.03.2019.

Verband der Automobilindustrie e. V. (2014):
Datenschutz-Prinzipien für vernetzte Fahrzeuge, Berlin. Available online under: https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html, last visited on 14.03.2018.

Veronesi, Lorenzo/Eibisch, James (2018):
The Car as Connected Platform – Interconnection Needs in the Automotive Industry, IDC Mini Market Spotlight, in: https://www.de-cix.net/de/about-de-cix/academy/white-papers/The-Car-as-Connected-Platform-Interconnection-Needs-in-the-Automotive-Industry, last visited on 03.02.2019.

Von Selle, Dirk (2018):
§ 142, Rz. 7, § 131 Rz. 4, in: Vorwerk, Volker/Wolf, Christian (Hrsg.): **Beck'scher Online-Kommentar ZPO**, as of 15.09.2018.

Zachmann, Frank (2018):
The car as a driver for data growth needing new infrastructure solutions, in: dotmagazine, 06/2018. Available online under: **https://www.dotmagazine.online/issues/mobility-and-connected-car/connected-car-market/car-as-driver-for-data-growth**, last visited on 03.02.2019.

Zukunftsinstitut (2017):
Die Evolution der Mobilität, hg. von ADAC e. V., München. Available online under: **https://www.zukunftsinstitut.de/fileadmin/user_upload/Publikationen/Auftragsstudien/ADAC_Mobilitaet2040_Zukunftsinstitut.pdf**, last visited on 01.02.2019.

9. Authors

Klaus Brisch LL.M.
Specialist lawyer for information technology law as well as Partner and Global Head of Technology,
DWF Germany

Klaus Brisch, Partner and Global Head of Technology at the DWF Germany law firm, is one of the leading specialist lawyers for IT law. He studied in Cologne, Bonn, and Lausanne and received his Master's degree from the University of San Diego. He is also a member of the Data Protection Law Committee of the German Federal Bar Association, of the Advisory Board of the German American Business Association (GABA) and of the Advisory Board "Additive Manufacturing" of the German Institute for Standardization (DIN).

Klaus Brisch advises on complex national and international IT projects, including issues relating to the outsourcing and migration of technologies, technology-based transactions, compliance issues, cyber security and smart grid technologies. He supports clients from various industries in structuring their IT infrastructure and thus ensures secure production and sales processes. In addition, Klaus Brisch advises clients in connection with eCommerce opportunities and all questions relating to Internet law. His practice focuses on the identification and handling of legal issues in connection with disruptive technologies such as Industry 4.0, autonomous driving and artificial intelligence.

Dr. Jens Eckhardt
Specialist lawyer for Information Technology Law and Data Protection Auditor (TÜV) as well as Compliance Officer (TÜV) and ECSA Legal Auditor, Derra, Meyer & Partner Rechtsanwälte PartGmbB

Dr. Jens Eckhardt is a specialist lawyer for information technology law as well as a ECSA Legal Auditor, Data Protection Auditor (TÜV) and Compliance Officer (TÜV). He works for the law firm Derra, Meyer & Partner Rechtsanwälte PartGmbB and has been advising national and international companies on data protection, information technology, telecommunications and marketing since 2001. The advice includes representation in court, representation vis-à-vis supervisory authorities, in particular with regard to data protection, strategic advice on the introduction of new systems, evaluation of existing systems, outsourcing, and contract drafting.

Dr. Jens Eckhardt regularly gives presentations, writes publications, and lectures at the udis Ulmer Academy for Data Protection and IT Security, the DeutscheAnwaltAkademie (German Lawyers' Academy) and the SRH Riedlingen Mobile University. At EuroCloud Deutschland_eco, he is responsible for the Legal & Compliance department on the board and acts as Head of the Legal Advisory Board, EuroCloud Star Audit.

Prof. Dr. Marcus Gelderie

Professor, Aalen University of Applied Sciences

After his doctorate in theoretical computer science and formal logic, Marcus Gelderie worked for BMW Car IT. There he focused on the IT security of on-board systems in series development. Since 2018, he has been a professor at Aalen University of Applied Sciences in the "Internet of Things" program, where he researches and teaches about the security of IoT devices.

Daniel Groß

Associate, DWF Germany

Daniel Groß is an associate at the DWF Germany law firm and is based in the Cologne office. He has extensive experience in the field of IT law and is particularly experienced in the field of project consulting regarding software and technology development. Daniel Groß completed his law studies in Münster and Bochum. Before joining DWF and being admitted to the bar in 2016, he was an in-house lawyer at FinTech Group AG and advised, in particular, in the area of IT law with a focus on financial technologies.

Daniel Groß advises software and technology companies, IT systems integrators, and telecommunications providers on the drafting of contracts with a focus on software development projects, licensing agreements, data protection, and open source software. He also advises on projects related to blockchain technology and is part of the in-house blockchain competence team.

Due to his experience in software development, he is able to communicate with software developers at eye level, to find legal solutions for technical questions, and to mediate between the technical departments and other project participants.

Thorsten Jansen LL.M.

Senior Associate, DWF Germany

Thorsten Jansen is Senior Associate at the Cologne office of DWF. He has deep knowledge of IT law, data protection and IT security compliance. He studied law in Freiburg and Sydney (LL.M.) and was admitted to the bar in 2011.

Thorsten Jansen advises clients in the technology sector on numerous IT law issues. He has extensive experience in drafting IT contracts and contract negotiations, in data protection and IT security compliance, as well as in copyright law and related areas of law.

Furthermore, Thorsten Jansen has a deep understanding of technology, in particular of IT systems used in client projects. Based on his experience gained during his work in the data center of a financial institution, Thorsten Jansen is familiar with the processes of a complex corporate network in an IT environment with the highest security requirements. Prior to this position, Thorsten Jansen managed the client IT system of a chair at the Law Faculty of the University of Freiburg.

Tobias Knoben

Project Manager, eco – Association of the Internet Industry

Tobias Knoben has been working as a Project Manager at eco – Association of the Internet Industry since 2017. There he is responsible for activities in the context of Internet of Things, Mobility, Smart City, and Smart Home, and is the eco contact person for the Competence Group IoT.

In 2009 he completed his M.A. in Communications Research and Modern History at the Rheinische Friedrich Wilhelms University in Bonn. Before joining eco, he worked as Senior Conference Manager and Project Manager at Euroforum Deutschland SE (today: Handelsblatt). There he was responsible for congresses and conferences on the topics of digitization, IT, and mobility. In this context he acquired comprehensive know-how in new technologies, economic change, and digitalization of the automotive sector.

Marco Müller-ter Jung LL.M.

Partner and specialist lawyer for information technology law, DWF Germany

Marco Müller-ter Jung, partner and specialist lawyer for IT law, works in Cologne. His main areas of expertise are IT law, intellectual property law, and data protection.

After studying law in Düsseldorf, Marco Müller-ter Jung obtained his Master of Laws (LL.M., Information Law) at the Düsseldorf Law School in 2008 and was admitted to the bar in 2009. Before joining the DWF Germany law firm, he was a lawyer at the law firm Wülfing Zeuner Rechel.

Marco Müller-ter Jung advises national and international companies on Internet, eCommerce, and data protection law as well as on IT contracts and complex IT projects, such as the procurement and integration of new technologies, migration, and outsourcing. His focus lies in advising on the legal requirements of disruptive technologies, such as the Industrial Internet, autonomous driving, and voice assistance systems. In addition, Marco Müller-ter Jung is Vice Chairman of the technical committee 105.5 "Legal Aspects of Additive Manufacturing" at the VDI.

Prof. Dr.-Ing. Dr. h.c. Dieter Schramm

Dieter Schramm completed his mathematics studies at the University of Stuttgart in 1981, worked there from 1981-1986 as a researcher, and received his doctorate in engineering in 1986. From 1986-1998, he worked at Robert Bosch GmbH as a group leader, department head of pre-development and series development for vehicle systems. He joined Tyco Electronics Ltd. in 1999 and served as Director Global Automotive Engineering until 2004 and later as CEO of Tyco Electronics Pretema GmbH. In 2004, he was appointed full professor and Head of the Department of Mechatronics at the University of Duisburg-Essen and, since 2006 Dean of the Faculty of Engineering and Head of the Department of Mechanical Engineering. His current research interests include electrified and alternative fuel-powered automobiles, driver assistance systems, vehicle dynamics, and wired manipulators. In 2015 he was awarded a Dr. h.c. by the University of Miskolc, Hungary. In addition to his research activities, he is director and partner of several companies in the field of research and further education in Germany and Malaysia.

Nils Steffen

Attorney at Law, Data Protection Officer (TÜV), and ESCA Legal Auditor, Derra, Meyer & Partner Attorneys at Law PartGmbB

Nils Steffen has been advising national and international companies throughout Europe in the fields of data protection, marketing, and competition law since 2016. His work includes out-of-court and court representation, also vis-à-vis supervisory authorities, in particular with regard to data protection, as well as contract drafting. He is a speaker at various data protection events, author of specialist articles on data protection law, co-author of the journal "Datenschutz digital", and legal auditor for EuroCloud StarAudit.

Thorsten Stuke

Expert Mobility, eco – Association of the Internet Industry, Founder and Managing Director, m2m-Tailors

Thorsten Stuke is the Managing Director and Founder of m2m Tailors. After completing his apprenticeship in the fields of aviation and business, he worked as a key account manager in the field of mobile data collection for monitoring stationary road traffic. He then served as Manager Apple Business Unit of Computer 2000 (now TechData), before becoming Head of M2M Sales and Solutions at Telefónica Germany until 2013.

Thorsten Stuke was the project manager responsible for the introduction of mobile phone parking in Cologne, Dusseldorf, and Bremen. He holds various patents in the field of M2M (protection of minors with mobile phones and secure transmission paths) and is the developer of the M2M platform with the strongest transactions in the vending market (approx. 1.5 million transactions daily).

With his extensive experience in the automotive sector, he is the leading expert on mobility topics in the eco Association.

Thomas Weber

Thomas Weber studied aerospace engineering at the University of the German Federal Armed Forces in Neubiberg. After graduation, he was employed by the German Air Force as an air traffic controller until the end of his twelve-year military service. After the end of his service period, he completed the "Automotive Engineering and Management" Masters at the University of Duisburg-Essen, where he has been working as a research assistant and doctoral student at the Chair of Mechatronics ever since.

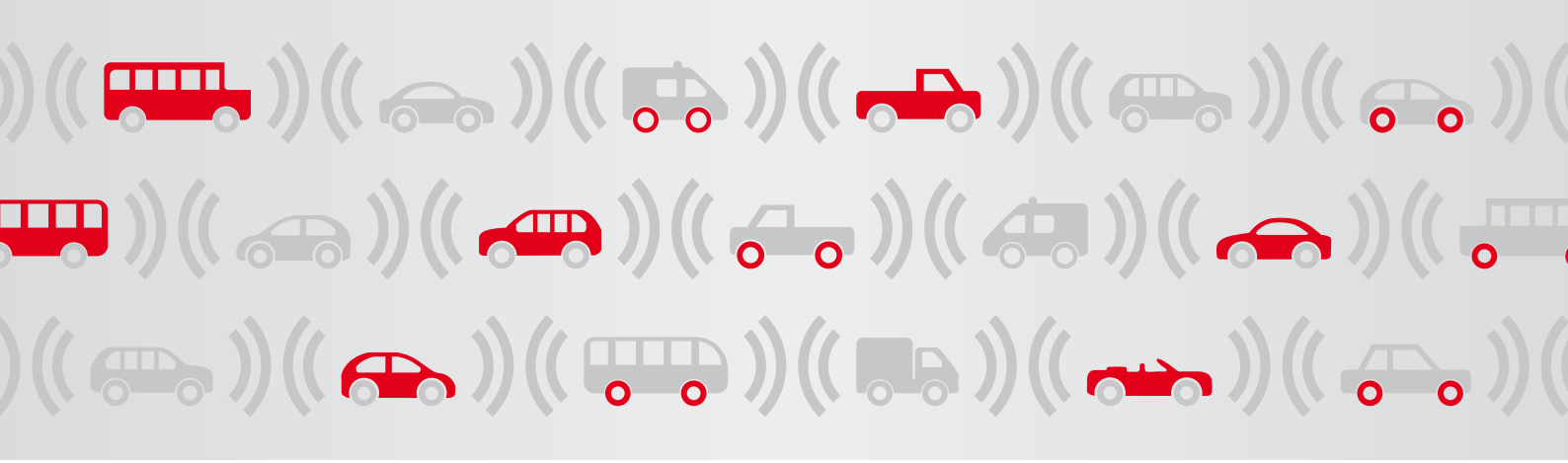
Imprint

Editor:
eco – Association of the Internet Industry
Lichtstrasse 43h
50825 Cologne, Germany

Translation:
Cáit Kinsella
Judith Ellis

Layout:
May 2019

Contact:
eco – Association of the Internet Industry
Tel.: +49 221 - 70 00 48-0
Email: iot@eco.de



eco - Association of the Internet Industry
Lichtstr. 43h, 50825 Cologne, Germany
Phone +49(0)221/700048-0
Fax +49(0)221/700048-111
info@eco.de, international.eco.de
@eco_de, @ecoverband

ASSOCIATION OF THE INTERNET INDUSTRY
WE ARE SHAPING THE INTERNET.
YESTERDAY. TODAY. BEYOND TOMORROW.