HAL
open science

Smart Cars Cruising on the Road Paved with Good Intentions? – Workshop on Big Data Applications and Individual Rights Under the New European General Data Protection Regulation

Felix Bieker, Barbara Büttner, Murat Karaboga

To cite this version:

Felix Bieker, Barbara Büttner, Murat Karaboga. Smart Cars Cruising on the Road Paved with Good Intentions? – Workshop on Big Data Applications and Individual Rights Under the New European General Data Protection Regulation. Anja Lehmann; Diane Whitehouse; Simone Fischer-Hübner; Lothar Fritsch; Charles Raab. Privacy and Identity Management. Facing up to Next Steps : 11th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Karlstad, Sweden, August 21-26, 2016, Revised Selected Papers, AICT-498, Springer International Publishing, pp.59-75, 2016, IFIP Advances in Information and Communication Technology, 978-3-319-55782-3. 10.1007/978-3-319-55783-0_6 . hal-01629152

HAL Id: hal-01629152

https://inria.hal.science/hal-01629152v1

Submitted on 6 Nov 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Smart Cars Cruising on the Road Paved with Good Intentions? – Workshop on Big Data Applications and Individual Rights under the New European General Data Protection Regulation*

Felix Bieker[1], Barbara Büttner[2], Murat Karaboga[3]

[1] Unabhängiges Landeszentrum für Datenschutz (ULD, Independent Centre for Privacy Protection) Schleswig-Holstein, Kiel, Germany
fbieker@datenschutzzentrum.de

[2] Department of Sociology, University of Kassel, Germany
barbara.buettner@uni-kassel.de

[3] Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe, Germany
murat.karaboga@isi.fraunhofer.de

Abstract. In this workshop we addressed the protection of individuals in the EU General Data Protection Regulation with regard to threats posed by big data applications. Using smart cars as an example, the workshop focused on the individuals' rights under the new Regulation. After an introduction to these topics, participants were invited to discuss these issues in groups and draw general conclusions on the effectiveness of the rights for individuals under the General Data Protection Regulation.

Keywords: Smart Cars · Individual Rights · Big Data · General Data Protection Regulation · EU law

1 Introduction

After years of political struggle, the General Data Protection Regulation (GDPR) has finally been adopted. Ever since the reform process was announced, questions arose on whether and to what extent the regulation would address the requirements of emerging technologies and applications. Among these, the topic of big data and its implications for data protection were particularly contentious.

The purpose of this workshop was to analyse the effectiveness of the protection of individuals under the new European General Data Protection Regulation, which implements the fundamental rights to private life and the protection of personal data, with regard to big data applications. In order to introduce participants to this complex issue and to provide a basis for the discussion, we focused on one specific case of big

* This work is partially funded by the German Ministry of Education and Research within the project 'Forum Privacy and Self-determined Life in the Digital World'.

data applications, namely smart cars. The ultimate goal of the workshop was a contribution to the question how personal data protection should be regulated in order to address the privacy challenges of big data applications while still preserving its benefits.

In the following we will give a short introduction to smart cars in the context of Big Data applications and their potential threats (section 2). We will then show how the EU data protection law protects individual rights (section 3). The next section presents the five smart car scenarios of the workshop and the discussion of the participants (section 4). We will discuss the results of the workshop (section 5), ending with a final conclusion (section 6).

2 Smart Cars and Big Data

The use of computerized systems in cars is not new. Features for safety or driver assistance began appearing in the 1970s with the anti-lock braking system (ABS) followed by the electronic stability program (ESP) and the standardization of on-board diagnostics (OBD) in the 1990s. These systems were already able to collect data and process this information to check the performance of various car systems (e.g. emission control; early warning of malfunctions by way of the dashboard "Check Engine" light). Since then, numerous additional in-car technologies like event data recorders (EDRs) or OBD-II standards were developed and are fitted almost as standard nowadays. Connectivity often complements these existing in-car technologies and also maximizes the data collection capabilities of a car [1, 2].

2.1 What is Connectivity of Smart Cars?

The connectivity of smart cars refers to their ability to exchange information between the car and its surroundings. It can be differentiated between the data collected and stored inside the car which is only accessible through a physical connection and data that are transmitted. The interactions range from car to car, car to infrastructure, car to devices up to car to service providers and manufactures, usually referred to as car2x connectivity. Thus, connectivity describes the digital exchange between cars. The idea behind the concept is to send relevant traffic or road information to other cars around. The car can also communicate with the infrastructure and receive information about road conditions (e.g. construction sites) or other external objects (e.g. traffic lights or traffic signs). Furthermore, cars can set up a wireless connection to other devices, for instance helping the driver to navigate. Moreover, the car can connect with service providers and manufactures and send errors reports or get a reminder for the next check-up [2-4]. Consequently, car2x connectivity produces a vast amount of data and exacerbates the issue of data collection.

2.2 Which Data are Collected?

Typically, three groups of collected data can be differentiated: data of the car, data of the car occupants and data about the environment of the car.

Car. Every car has several identifiers which are transferred with every communication of the respective device. This can include the vehicle identification number (VIN), mobile device identifiers, SIM-cards, media access control (MAC) addresses, Bluetooth identifiers and radio frequency identification (RFID). The so called telematics data of a car include information on the location and changes of the location (e.g. geo tracking data, route, speed). Telematics can be compared to a black box that records information about the driving behaviour on how, when and where a person drives. Cars are also equipped with many sensors which collect the operational state and functionality of the single components during the drive (inter alia the engine, gear, brakes, tire pressure, fumes). In addition cars can be equipped with event data recorders (EDRs). They collect data shortly before, during and after a car accident and, for instance, store the direction of movement, longitudinal acceleration or the status of the brakes [1, 5, 6].

Occupants. The car also collects a multitude of information referring directly to the occupants of a car. Using the connected components of the car for example requires registration with the provider (car manufacturer) and the creation of a user account. For registration, data such as name, address or date of purchase can be required. Additionally internal sensors might obtain information about the physical or biological characteristics using biometric detection systems to identify the driver. The car can keep personalized information about the voice or data communication from text messages and remember habits of the driver, for instance music choice or seat and mirror position. The car might even be able to test the physical fitness of the driver by analysing the heartbeat, breathing or head- and eye-movement [1, 6].

Environment. The car also collects information about its environment, be it the physical surrounding or the human environment. This includes information about upcoming obstacles, blind spots, traffic sign analysis or even the social network of the driver. Including, for example, if drivers connect their phone with the car, it might gain access to their address book. Smart cars can also function as Wi-Fi-Hotpots and through this, collect the identification and use data of other devices and their users and owners [1, 2].

Although many of the collected data are not directly linked to a person, in many cases personal details can be revealed through other information (e.g. workplace information through geo tracking data). From a legal point of view, personal data are any information that relate to an identified or identifiable natural person according to Article 4(1) GDPR. Under this legal definition, a person is identifiable when he or she can be identified by reference to an identifier such as name, an identification number,

location data or one or more factors specific to inter alia the physical, genetic, economic or cultural identity of the natural person in question. As smart cars use several identifiers for communications, these, in consequence, constitute personal data [1, 7]. Furthermore, the combined analysis of several attributes, which by themselves do not make a person identifiable, can turn the information in question into personal data [1]. This is especially true where location data, as explicitly referenced in Article 4(1) GDPR, are used.

These types of data collected and the purposes of use receive new dynamism in the context of modern technologies of data collection and processing that can be subsumed under the term of big data which will be the topic of the next section.

2.3 What is Big Data?

Big data is a controversial buzzword which is used by a variety of stakeholders (e.g. private sector, public sector, science, and press and media) to characterize modern tendencies of data collection and processing in the networked, digitized, information-driven world. It is not a precise scientific concept, but rather a highly contested idea that differs depending on the context [8].

Although there is no uniform definition of big data, many definitions revolve around an understanding which involves three major aspects of the phenomenon: *volume*, *variety*, and *velocity*, with *volume* referring to the vast amounts of data that are being generated and accumulated, *variety* referring to the different types of data and data sources that are brought together, and *velocity* referring to the ability of real time analyses based on elaborate algorithms, machine learning and statistic correlations. Over the time, the three V's were expanded to cover other important aspects, including particularly: *veracity* and *value*. The former refers to the correctness and accuracy of information, the latter to the assessment of the societal *value*, big data analyses may or may not offer [9, 10, 11].

The types of data included in big data analyses might comprise any type of structured or unstructured (text, image, audio, or video) data. These data might be collected from public datasets (e.g. administrative data and statistics about populations, geography, economic indicators, education etc.), from businesses, web pages, newspapers, emails, online search indexes, and social media, or from any kind of sensors (mobile, such as sensors carried on the body or drones as well as stationary sensors such as CCTVs or Wi-Fi/Bluetooth beacons) [12].

Big data analyses are used for several purposes that can be grouped under the terms of descriptive statistics and inductive statistics. The former relates to big data analyses that are based on the elaborate analysis of data sets with high information density to measure things, or to detect trends. The latter relates to the analysis of large data sets with low information density in order to reveal relationships and dependencies, and to predict outcomes and behaviour. However, one important characteristic of big data that spans all areas of application is that its analyses are not limited to specific purposes. Instead, the continuous analysis of data is supposed to generate new purposes for which the existing data can be used [13].

As a result, many observers agree that big data is a disruptive technology with possible implications for all economic and policy areas (transport, energy, education, security, health, research, taxation, etc.) and that it represents a particularly weighty shift that will affect society as a whole [12, 14, 15].

2.4 Who Profits from these Data?

Regarding smart cars, many promises are made to the public about the potential benefits of big data.

Users. New technologies in cars promise drivers advances in safety and convenience. Through intense car2x communication and background analyses of the collected data, the prevention of accidents and better traffic management (better traffic light control, avoidance of traffic jams, and so on), indications of discounts (special deals at a nearby petrol station, or restaurant, etc.) and many more potential benefits are promised not only to allow more secure travelling, but also to return monetary benefits to the car owners, allow more comfort and at the same time being less damaging to the environment [16, 17].

The State. Big data opens new prospects of control for the state. Courts, financial authorities and law enforcement agencies could use the generated data for purposes of criminal prosecution, hazard prevention or the collection of public revenue. Very similar to how many other big data applications are framed, smart mobility concepts focus on emphasizing the societal surplus promised. Such promises include that traffic controls enhanced by big data analytics will be more economic, ecological, efficient, cost-effective, comfortable and secure. This may be achieved by an array of sensors that are spread all over a city and which allow the continuous collection of various data [16, 17]. In the meantime, many cities around the world have already introduced smart city concepts to innovate and enhance city life through lower costs and less environmental pollution. These concepts, however, vary in scope and depth and range from pioneering cities such as Stockholm and Amsterdam which rely on individual agencies or research bodies to comprehensively networked and highly centralized smart cities such as Singapore [18, 19]. For many years, the rise in the numbers of cars caused problems regarding the maintenance and expansion of city infrastructures, especially regarding automobile traffic. In times of strict budgets, municipalities and government agencies welcome these new opportunities as means of a more cost-effective and ecologically sound urban infrastructure and land use planning.

Industry. The interrelation of big data applications and smart cars needs to be understood in the broader context of digitized, networked, sensor-laden environments. Therefore, the development of smart car services should not only be understood in the isolated context of catchwords such as smart mobility and smart traffic controls.

Rather, the whole environment, including all its artefacts such as infrastructures, buildings and inhabitants, should be regarded as both the provider of data and user of data-driven analyses [17]. The main interest of the industry lies in the monetarization of the data that is generated in such environments either to improve their current business or to develop new business models. Manufacturers and garages can use the car's diagnostic and performance information to improve their products or develop new business models (e.g. customer relations management, marketing and after-sales services). The use of data surfaces also offers new business fields like traffic information, fuel price data banks, driver-apps, or hotel booking systems. Service providers might offer real time navigation or maintenance services based on telematics. Also, the advertising industry can profit from the vast amounts of data and initiate personalized advertising. Insurance companies may offer their customers personalized insurance rates based on their tracked individual driving behaviour [2, 20-22].

2.5 Potential Risks

The generated data offer a variety of information about the users and therefore are open for misuse. These data are collected inter alia in the interest of car manufacturers, suppliers, garages, insurances, courts, financial authorities, law enforcement agencies, and municipalities. Interfaces unnoticeably transfer the data outside the connected car. The user cannot avoid this and/or is not aware of this fact. Every car will leave a digital trace which allows the deduction of detailed profiles of every movement, behaviour and the personality of the driver, passengers and any other person within range of the sensors. It offers potential for surveillance activities and unauthorized persons might be able to gain access to the car by exploiting security vulnerabilities. Furthermore, companies might use this data for their insurance or credit decisions or use it to reject warranty or guarantee claims of customers [6, 22 23].
However, these characteristics apply not only to smart cars; rather they can be seen as an illustration of the potential risks of big data in the age of the internet of things. The ability of smart devices to connect and the resulting system of systems (thinking for example of smart homes or smart cities) offers many opportunities to collect personal data and to use it for further purposes. And while data protection is still predominantly considered as an individual right, proponents of big data analyses often frame their initiatives by means of the societal benefits that big data promises in a variety of sectors (aside from traffic management, a special focus is on the health care sector) [15, 24].

Regardless of whether personal data are included in the underlying datasets [which may or may not be the case, cf. 25], the results of any big data analysis might very well impact certain individuals[1] as well as groups or even society at large. The Article

[1] Recital 75 GDPR lists some risks that may result from data processing and may "lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data sub-

29 Working Party draws particular attention to the issues of insufficient data security, loss of transparency for users, inaccurate, discriminatory or otherwise illegitimate analysis results as well as increased possibilities of government surveillance [26]. Group discrimination along racial lines, for example, as opposed to obvious and nowadays illegal racial profiling practices of past decades, might simply result from (for example, credit scoring or risk assessment) decisions based on algorithms that evaluate the data in a biased and inaccurate way [27, 28].

When the legislative procedure for the GDPR officially started in January 2012, critics of big data hoped it would provide a legal solution. The following section will provide some insights if the GDPR achieved this and how it tries to protect individual rights in the digital age.

3 EU Data Protection Law and Individual Rights

The GDPR will become applicable in May 2018. It aims to further harmonize the EU data protection law. At its core, data protection addresses the imbalance in power between the data subject and the controller who offers services that require personal data. Thus, the raison d'être of data protection law is to protect the rights of the individual, as is stipulated by Article 1 para. 2 GDPR. In order to achieve this, the processing of personal data is not allowed, unless there is an explicit legal basis according to Article 6(1) GDPR and Article 8 CFR. Special categories of personal data, such as inter alia on ethnicity, sexual orientation, political opinions, as well as genetic or health data demand special safeguards under Article 9 GDPR. Generally, the data may only be processed for the purposes for which they were collected, as prescribed by Article 5(1)(b) GDPR.

3.1 Fundamental Rights to Private Life and the Protection of Personal Data

The protection of personal data on the EU level is also enshrined in the Union's primary law: the EU Charter of Fundamental Rights protects the right to private life in its Article 7. It also explicitly provides for a right to the protection of personal data in Article 8 CFR. According to the settled case-law of the Court of Justice of the EU (ECJ), any processing of personal data is an interference with these fundamental rights of the individual [29-32]. While such an interference may be justified under the

jects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."

conditions of Article 52(1) CFR, this provision requires that any processing has to be permitted by law and proportionate.

Further, Article 8 CFR imposes requirements as to the storing of the data and access rights: the purpose of the data collection must be sufficiently clear, access to and use of the data have to be limited on a technical and procedural level and the relevant provisions have to provide sufficient safeguards against abuse and unlawful access or use [32].

3.2 Individual Rights in the General Data Protection Regulation

These abstract principles are implemented in the rules of the GDPR. Chapter III of the GDPR includes various specific rights of data subjects vis-à-vis the controller.

As all personal data has to be processed lawfully, fairly and in a transparent manner, as stipulated by Article 5(1)(a) GDPR, Article 12 GDPR generally requires that all information and the modalities for the exercise of these rights have to be transparent for data subjects and presented to them in a concise, transparent and comprehensible way. When data are collected, the data subjects must be informed of the controllers, the purposes and legal basis for the processing, the recipients of the data and the transfer to third countries. Access to this information is also enshrined as a right of the data subject in Article 15 GDPR. While these rights are applicable for any data collection, this information is particularly important in cases where the legal basis of the processing is the consent of the data subject. According to Article 4(11) GDPR consent is any freely given, specific and unambiguous indication by the data subject. Thus, without the appropriate information, consent is not possible. The data subject may withdraw his or her consent with regard to future processing according to Article 7(3) GDPR at any time. If there is no other legal basis for the processing, it has to be ceased. However, this does not affect the lawfulness of the processing prior to the withdrawal of consent.

When there no longer is a legal basis for the processing, the purpose of the processing has been achieved, the data subject objected to the processing or data have been processed unlawfully, the data subject has the right to demand the erasure of the data from the controller under Article 17 GDPR.

In addition to erasure of data and restriction of the processing, the data subject under Article 20(1) GDPR now has a right to data portability. The right applies whenever automated processing of data is based on consent or a contract with the controller and concerns data provided by the data subject him- or herself. It entitles the data subject to receive his or her personal data in a structured, commonly used and machine-readable format. Data subjects may also demand that the controller transmits the personal data directly to another controller.

4 Can the Data Subject's Rights Resolve the Concerns for Individuals with Regard to Smart Cars?

The third part of the workshop was aimed at identifying and analysing the rights of individuals relevant in the legislative process for the GDPR with regard to smart car scenarios.

4.1 Application of Individual Rights to Smart Car Scenarios

Participants were divided in small working groups in order to assess different scenarios with regard to the effectiveness of data subject's rights in a smart car and big data context. The scenarios touch upon issues which arise in smart cars with regard to data processing and the rights of data subjects (e.g. collection of data, acquisition of the data subject's informed consent in the car, managing various drivers, right to data portability, right to deletion, exercise of right to withdraw consent, objection to direct marketing, notification of breaches, transfer of data, categories of data stored and who has access to which data). The scenarios furthermore strove to test the limits of data protection law with regard to the protection of individuals by raising issues such as societal disadvantages that might be the result of big data processing in a smart car context and demonstrate its limitation with regard to the practical implementation in everyday situations.

After the group work session, participants discussed whether the new EU data protection legislation adequately addresses and effectively resolves the identified issues and if these could be resolved in a more appropriate manner.

Scenario 1: Owning a Smart Car. After six months of driving her new smart car without any incident, A suddenly receives a call from the dealership's garage, asking her to bring her car in for repairs. When A inquires as to the nature of these repairs, the garage replies that her car has been sending error messages and therefore needs to be taken in for a check-up. Please consider the following alternate scenarios:

- A does not want to receive further calls. She tells the garage to delete her personal data, as she wants an independent garage to take care of necessary repairs. The garage refuses, as
  - the error messages relate to an issue with the airbag deployment, which may occur at random. Due to this potentially life-threatening situation, the garage states it had a responsibility to inform A.
  - the error messages relate to an issue with the infotainment system, but a repair at the dealership was necessary if A wanted to keep the manufacturer's warranty.
- A does not take the car for repair at the garage. However, three weeks later she has an accident due to a failure of the electronic stabilization programme. The garage links the failure to the error messages and, stating that A had been informed of the need for a repair, the manufacturer whose erroneous programming caused the failure refuses to pay for the necessary repairs, which resulted from the accident.

After these experiences, A considers buying a smart car by another manufacturer. However, as she has personalized many of her current cars features, she is reluctant to switch brands, until she reads about the right to data portability in a tech blog. After ordering the new car, she requests that all of her data stored in her old car is transferred to the manufacturer of her new car. Please consider the following alternate scenarios:

- The old car's manufacturer refuses to submit the data to the other manufacturer, arguing that the systems are not compatible. When A insists she is provided with a text file including the code containing her data
- The old car's manufacturer states that it can only transfer certain types of data, relating to the infotainment system, but not all personal data. For instance it is not possible to transfer the data concerning the seat adjustments, as another manufacturer has different specifications and the data can thus not be converted.

Discussion among the Participants. Regarding the first part of the scenario, the participants pointed out that A can generally request the deletion of her data in case she turns to an independent garage for the necessary repairs. However, if the contract included a valid service contract with the dealership's garage, her right to consult another garage could be limited. In the case at hand it was only a warranty offered by the manufacturer, which A is free to waive and choose another garage. If the processing of A's data is dependent on her consent, she can freely revoke it and the garage must not contact her anymore. When the data are processed for the purpose of direct marketing, as is the case here, the data subject may object at any time and the controller has to cease the processing immediately (Article 21(2) GDPR). However, in the case of a life-threating situation, the manufacturer may continue to use her data under Article 6(1)(d) GDPR, independent of her consent. Another danger for data subjects highlighted in the second indent of the first part is that the manufacturer might use data of the car against the owner in order to limit its own responsibility. This illustrates the importance of transparent data processing and informed consent of the data subject.

Regarding the data portability part of scenario 1, the participants indicated that the Article 20 GDPR only specifies that personal data have to be provided in a structured, commonly used and machine-readable format. The question of compatibility, however, is not solved in the Regulation as Article 20(2) states that the transmission of personal data directly from one controller to another should only occur where technically feasible, which leaves much room for interpretation.

Scenario 2: Renting a Smart Car. B rents a car with his local car rental company. Arriving at the company, he is pleasantly surprised to find a brand new car. The rental company agent informs him that the car is fitted with a telematics device, which electronically transmits data on the car's location, the speed and acceleration. The agent assures B that the device does not store any personal data. B signs the contract, including a separate section where he consents to the use of the telematics device.

As B gets in the car, he connects his smartphone via Bluetooth to listen to his music. On the way he receives a phone call from his friend. B is surprised to find that the call is relayed through the car's infotainment system using the built-in microphone and speakers. When B returns the car after two days, he is in a hurry to get to his appointment and just grabs his phone as he leaves the car. After two days, he remembers the phone call and wonders whether the contact information is still stored in the car. He calls the rental company and asks them whether his data was deleted from the car, however, the rental company does not answer his question and instead refers B to the manufacturer of the car. In turn, the manufacturer claims that this is the rental company's responsibility.

Two months after the return of the rental car, B receives a letter from the police relating to a hit-and-run accident, where a witness saw a black car of the same model as the one rented by B swerve on the road and hit a parked car's side-view mirror, before speeding away. The police then requested the data from the telematics device of the rental company's car as well as their costumer database and found that B had been at the site of the incident. B is surprised that his data was handed to the police so easily, especially as the agent had specifically told him that the telematics device collected no personal data. He thinks the car rental company had no legal basis to submit his data.

Discussion among the Participants. The participants argued that the collection of personal data is only lawful in case that the consent of the user was obtained on the basis of the principles of fairness and transparency which includes the provision of specific and unambiguous information about the processing operation and its purposes (Article 4(11); Article 5(1)(a) and Article 13 GDPR). It was stressed, that in the scenario at hand, the specific contents of the contract are crucial in order to assess whether the controller met his obligations under the relevant provisions. However, the misleading information by the agent suggests that this was not the case. Participants also stated that the contract would have to specify the purpose of collection in order to be lawful. If the data were lawfully collected they would have to be deleted after a certain time. In case the data were collected unlawfully they would have to be deleted right away. However, as the scenario suggested, it may be difficult in practice for the data subject to find the controller and have his or her data deleted. Especially in the context of smart cars it can be a challenge even for lawyers to determine who is responsible for the data processing.

Regarding the request of information by authorities, it was stated that such provisions are specified in the context of national laws, but that the collection of data, and especially telematics data, could induce the national legislator to pass provisions for access of public authorities, which intensified the risks for the individuals.

Scenario 3: Lending a Smart Car – without the Ability to Distinguish between Individual Drivers – to a Friend. A, the owner of a smart car, lends his car to his good friend B who wants to use the car to visit her mother at a retirement home several times a week. Since her mother suffers from various illnesses, B sometimes has

to rush to help her and assist the nurses at the retirement home or at the nearest hospital. A chose an insurance company which analyses his driving habits. While this may serve to offer special conditions and financial benefits, the opposite may also be the case under the contract's conditions: as a result of the dangerous driving style of B (driving fast, approaching other cars too fast, and driving too close to others cars), and as there is no method to assess whether A or B was the one driving dangerously, the insurance company increases the annual fee of A.

Further, B, a tech-enthusiast with an information science background, – as opposed to A, who never does that – regularly uses the integrated infotainment system (with Internet functionality) of the car (for example, sometimes when her mother undergoes special medical treatment that she is not allowed to attend or when she has to wait for her children when picking them up from school, etc.). She researches information on hotshot technologies such as virtual reality glasses and high-speed computers to use the glasses and on specialized computer-issues. As the car's search history relates to A and not B, and with the help of cookies and third-party cookies, the customer profile of A changes considerably due to the search input which indicates that A is quite wealthy. Subsequently A is regarded as a tech-affine person, not only resulting in a change of the advertising displayed to A, but also in higher prices for flight tickets and for several kinds of devices, he buys online. The price-conscious A is irritated by the increasing prices and contacts one of the shops, why he has to pay more for a flight than other customers have stated on online-comparison websites. The shop's customer service assures that there is no discrimination, as prices may change from minute to minute.

Discussion among the Participants. Regarding the inability to distinguish between different drivers it was stated that this scenario poses a serious issue as only more surveillance would help to solve the problem, but which would also raise new privacy issues. The insurance company would have to collect even more data to differentiate between the two persons.

Regarding the issue of profiling, Article 15(h) GDPR was mentioned which requires the data controller to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject in cases of automated decision-making, including profiling. However, the definition of meaningful information remains unclear: it has not been decided on a European level what kind of information this involves (i.e. the whole algorithm list or only parts). Concerning this question, it was stated that trade secrets, as mentioned in recital 63 GDRP, are protected right of others and may restrict the right of access to personal data.

Further, the question arose whether A had been discriminated against. In the Regulation discrimination is not an independent category. It has to be related to other characteristics which is not the case in scenario 3. Article 9(1) only prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Additionally, the lawfulness of processing personal data depends on the content of the insurance contract. The insurance company can prescribe that only A can use the car and that B would need an extra insurance package. The insurance contract could also include a lifelong tracking consent, which, however, would have to be transparent for the user. Nevertheless, in case that personal data of another person was erroneously used for profiling of the user, he or she has the right to either demand rectification of the data or even to object such processing according to Article 15(e). However, although there is the same difficulty to distinguish between different persons, as in the first part of the scenario, detailed information on which products were bought and which websites were visited might help to distinguish between different users. Yet, this would also raise the potential threat of revealing personal data of B to A.

Scenario 4: Lending a Smart Car – with the Ability to Distinguish between individual Drivers – to a Friend. A, the owner of a smart car, lends his car to his friend B. B, the proud upholder of public transportation, tells him that he needs the car to buy larger quantities of goods from the wholesaler. The smart car is a pretty new model and has – among several other high-tech features – facial, voice and haptic recognition technology on board in order to distinguish different drivers. The majority of these features, however, are only accessible when the system recognizes the car owner, A. Although details like photographs and voices of other drivers are not stored, A is able to access the routes driven by any other driver.

After shopping, B calls his friend A and asks him whether the car stores any information on routes and destinations. A thinks that his friend sounds particularly nervous and finds his behaviour suspicious. A assures B that no such data is stored by the car. Out of curiosity, A opens the route of his happily married friend B. This is when he realizes that his friend was not driving to the wholesaler, but to a remote brothel with poor public transportation connections. Following the shock of the unveiling and as he is also friends with B's wife, he decides to inform her about her husband's infidelity.

Discussion among the Participants. The participants especially discussed whether A might be regarded as a data controller in the context of this scenario. Article 4(7) defines the controller as 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. Opinions, however, were divided: some participants regarded A as responsible for providing all the information that needs to be provided by a data controller and that it is unlawful to link information of A (marriage status) with the information that is unlawfully obtained by accessing the route of B and using the conclusion for the purpose of telling another person about it. Other participants stated that the responsibility also lies with the car/service manufacturer that has to shape its products in a way that such an abuse is not possible. From a legal perspective it depends on whether A is actually the person determining the purposes and means of the processing. It is thus a crucial factor whether B could potentially also turn it off. Certainly, his influence on the means of collection is rather limited. These two factors

point to the car's manufacturer as the actual controller. However, it was pointed out that this is one of the yet unresolved legal issues of smart cars.

Scenario 5: Car Manufacturers and Service Providers as Part of Road Traffic Management. A lives in a small town that suffers under a chronic budget deficit. After an intense public debate on the economic opportunities and privacy risks, which traffic monitoring would impose on citizens, the municipalities eventually decide to introduce the new smart city concept. However, due to limited financial resources, the responsible members of the city's smart mobility working group decide not to distribute expensive sensors around the city. Instead, a traffic management system is introduced which is based on low-priced sensors that use Bluetooth technology. By connecting with car drivers' smartphones or directly with smart cars via Bluetooth, this new system promises to collect anonymized data on which routes are preferred most amongst the city dwellers. By this, municipalities strive to provide a better and evidence-based traffic management and lower the costs of building new roads or maintaining existing ones. In the meantime, the municipalities reduced staff numbers in the traffic office to compensate the smart city concept's costs. As a result of staff shortages and following the idea of "smart regulation", the maintenance and construction of roads is increasingly based on the data generated from the Bluetooth sensor network.

However, A and most of his neighbours are privacy-aware citizens who opposed the smart city concept in this form and would have preferred either none or at least a more ecologically oriented concept that could have provided alternatives to driving by car but which, due to budget problems, were rejected by their municipality. Thus, many people in his district turn off the Bluetooth functionality of their smart cars and smartphones so that they are not detected by the city's Bluetooth sensor arrays. Thereby, the district inhabitants' driving habits are no longer registered by the municipality as they are not recorded by the Bluetooth sensors. Thus, in contrast to other districts, where a lot more inhabitants agreed to the data policy and allowed the automated Bluetooth connections of their phones and cars, the district's roads are not maintained in a proper way and the much needed construction of new roads is currently not in sight. From the newspaper, A learns that similar problems also occur in other districts of the city. Accordingly, the situation is even worse in poor districts.

Discussion among the Participants. In the discussion it was pointed out that it is not possible to anonymize route data in a small town and that the Bluetooth solution has fundamental problems, as it raises several privacy issues. According to the participants, it is basically an engineering problem which could be solved by using appropriate technology. A less privacy-invasive low-tech solution minimizing the collected data would thus be preferable.

In contrast, some participants stressed that, apart from the concrete technology used, the action of the municipality does not really meet the requirements of good democratic governance, while other participants indicated that municipalities do not have to initiate referenda on such matters as the introduction of traffic surveillance

and CCTV prove. It was furthermore stressed that data protection rights of the mentioned groups (privacy-aware citizens and citizens of poor districts) might have been violated even in case of a referendum if the vote was in favour of the municipalities' proposal.

5 Results of the Workshop

The discussion showed that the upcoming GDPR still leaves several issues relating to big data applications in a smart car context unresolved. From the discussions of the participants, the following general themes could be identified:

The discussion of the importance of specific contents of contracts (see discussion of scenario 1 and scenario 2) shows that some issues are difficult to solve with rather general data protection laws. At the same time, it highlights the lack of transparency in current contract clauses, especially with regard to obtaining the consent of the data subject. Consumers are confronted with opaque consent forms on a regular basis. In many instances, the clauses cannot be the basis of a valid consent. However, the requirements for valid consent had already been addressed in the Data Protection Regulation. While this is therefore an issue that has been solved legally, it is not properly implemented in practice. With regard to smart cars, manufacturers have to be sure to properly inform customers of the capabilities of their cars and obtain valid consent for processing operations which cannot be based on another legal basis. The data subject must be aware of processing that takes place in a smart car. However, this legal requirement is not easily implemented in such an environment. While ideas like a privacy dashboard [33] have been put forward, it has to be borne in mind that the driver also has to be able to focus on the driving itself.

Similar to the issue of valid consent, the problem of identifying the controller of data processing operations is also inherited from the former legislation. However, it can be seen that concepts such as the question of who controls a data processing operation may be difficult to answer in practice, especially in complex environments with many data flows, such as in the context of smart cars. Especially with regard to such new technology, a definition of data flows, as it is required by a data protection impact assessment under Article 35 GDPR, is essential. Furthermore, while the GDPR follows a technology neutral approach based on the risks for the individual [34], specific complex technologies such as smart cars may also require more detailed risk adequate provisions, either in the form of codes of conduct or sector specific regulation.

The discussion on the new right to data portability (see scenario 1), the difficulty of distinguishing two persons that use the same car (see scenario 3) and the question of responsibility in case of multiple controllers (see scenario 4) point to the necessity of specific decisions of the supervisory authorities, which will coordinate their efforts in the upcoming European Data Protection Board (EDPB), as well as judgments of the European Court of Justice on the interpretation of specific legal terms and concepts.

In scenario 3 the issue of discrimination based on data processing was discussed. The discussion showed how difficult it is to prevent or prove discrimination through

scoring activities and to supervise the use of such technologies while respecting the interests of businesses, such as trade secrets. The GDPR does not answer this question, but instead resorts to the abstract legal definition of 'meaningful information', which will have to be interpreted by those applying the law in practice. For the individual, in most instances, the only possibility may be to provide additional personal information in order to rectify the data. However, this creates a privacy conundrum, as the data subject has to reveal even more information.

The discussion concerning scenario 5 indicated that the balance of the needs of individuals (data protection rights) and of the needs of society (more efficient and cost-effective road infrastructure management) might regularly be decided in favour of the greater societal benefits. However, rather than choosing one option over another, an actual balancing of positions has to reconcile both positions as far as possible. Furthermore, it should be emphasised that data protection in itself is a value for society as a whole: to determine what others know about a person is part of their autonomy in a free society. Data protection thus is at the heart of democratic processes [24, 35].

6 Conclusions

As has been shown, the GDPR does not exhaustively solve all issues relating to the protection of individuals with regard to big data analyses in the context of smart cars. While the Regulation offers some new solutions, such as the right to data portability, these will have to be interpreted and implemented in a meaningful way in practice. Further, the new legislation inherited some of the problems of the old legislation, such as the proper implementation of a valid consent or the question of responsibility for data processing operations. Especially the latter becomes relevant with regard to the specifics of smart cars. Moreover, it remains to be seen whether some member states will make use of opening clauses (including in particular Art. 6(2) but also Art. 9(4) and Art. 22(2) GDPR) to establish more accurate sector-specific rules and if other member states will harmonize their legislation accordingly (maybe in tandem with the EDPB and CoJ rulings) or if this, in contrary, will lead to a patchwork of different rules [36]. In conjunction with legal regulation, and especially in complex data processing structures, as is the case with smart cars and big data, the development and application of Privacy by Design (PbD) and Privacy Enhancing Technologies (PETs) remains an important but not yet effectively implemented cornerstone.

All in all, the workshop has served both to raise awareness of individual rights under data protection law in general and also to show some of the deficits in practice. However, in order to address the challenges of big data to society in a more democratic way, we need societal debates and further development of institutional structures addressing the power imbalances of different voices and interests. The debates on the GDPR and the ongoing discussions on the review of the e-Privacy-Directive can be regarded as a good starting point, but an expansion of these discussions both within the member states and within non data protection-affine communities is essential.

References

1. Hansen, M.: Das Netz im Auto & das Auto im Netz. Datenschutz und Datensicherheit **39**(6), 367-371 (2015)
2. Future of Privacy Forum: The connected car and privacy. Navigating new data issue**s.** White paper (2014)
3. Cohen, A., Arce-Plevnik, L., Shor, T.: IoT in automotive industry: Connecting cars. Unpublished paper (2016), `http://works.bepress.com/luis-arce-plevnik/2/`
4. European Commission: Business Innovation Observatory. Internet of things. Connected cars. Case Study 43 (2015) `http://ec.europa.eu/DocsRoom/documents/13394/attachments/2/translations/en/renditions/pdf`
5. Hornung, G.: Verfügungsrecht an fahrzugbezogenen Daten. Das vernetzte Automobil zwischen innovativer Wertschöpfung und Persönlichkeitsschutz. Datenschutz und Datensicherheit **39**(6), 359-366 (2015)
6. Lüdemann, V.: Connected Cars. Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück. ZD **6**(2015), 247-254 (2015)
7. Kremer, S.: Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz? Recht der Datenverarbeitung **5**(2014), 240-252 (2014)
8. Bennett, C.J., Bayley. R.M..: Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments. In: Van der Sloot, B., Broeders, D., Schrijvers, E. (eds.): Exploring the Boundaries of Big Data, pp. 205–227. Amsterdam University Press, Amsterdam (2016)
9. Klous, S.: Sustainable Harvesting of the Big Data Potential. In: Van der Sloot, B., Broeders, D., Schrijvers, E. (eds.): Exploring the Boundaries of Big Data, pp. 27–47. Amsterdam University Press, Amsterdam (2016)
10. Ward, J.S., Barker, A.: Undefined by Data: A Survey of Big Data Definitions. *arXiv Preprint arXiv:1309.5821*, (2013)
11. Gartner, Inc.: IT Glossary: Big Data, `http://www.gartner.com/it-glossary/big-data/`
12. Poel, M., Schroeder, R., Treperman, J., Rubinstein, M., et al.: Data for Policy: A Study of Big Data and Other Innovative Data-Driven Approaches for Evidence-Informed Policy-making (Report about the State-of-the-Art). Amsterdam: technopolis, Oxford Internet Institute, Center for European Policy Studies, (2015), `http://www.data4policy.eu/#!state-of-the-art-report/cjg9`
13. Gandomi, A., Haider, M.: Beyond the Hype: Big Data Concepts, Methods, and Analytics. International Journal of Information Management. 35(2), 137–144 (2015)
14. Executive Office of the President: Big Data: Seizing Opportunities, Preserving Values. Washington, DC: The White House, May 2014
15. Mayer-Schönberger, V., Cukier, K.: Big Data: A Revolution that will Transform how we Live, Work and Think. John Murray, London (2013)
16. DIVSI, and iRights.Lab. "Big Data." Hamburg, January 2016.
17. Xu, F.: Smart Data for Mobility (SD4M): Eine Big-Data-Analytik-Plattform Für Multimodale Smart Mobility Services, Presented at the Bitkom Big Data Summit 2015, Congress Park Hanau, 25 Feb 2015
18. Watts, J.M., Purnell, N.: Singapore Is Taking the 'Smart City' to a Whole New Level. Wall Street Journal, 25 Apr 2016 `http://www.wsj.com/articles/singapore-is-taking-the-smart-city-to-a-whole-new-level-1461550026`

19. Albino, V., Berardi, U., Dangelico, R.M.: Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology. 22(1), 3–21 (2015)
20. DeBord, M.: World Economic Forum: Who owns connected car data? (2015) https://www.weforum.org/agenda/2015/09/who-owns-connected-car-data/
21. Derikx, S., de Reuver, M., Kroesen, M.: Can privacy concerns for insurance of connected cars be compensated? Electron Markets **26**(1), 73-81 (2016)
22. Stöhring, M.: Mein Auto, meine Daten? Fahrzeuggeneriertes Datenmaterial: Nutzung und Rechtsansprüche. c't Magazin für Computer und Technik **11**(2016), 128-133 (2016)
23. Federal Trade Commission: The Internet of Things: Privacy and Security in a Connected World. FTC Staff Report (2015). https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
24. Van der Sloot, B.: The Individuals in the Big Data Era: Moving towards an Agent-Based Privacy Paradigm. In: Van der Sloot, B., Broeders, D., Schrijvers, E. (eds.): Exploring the Boundaries of Big Data, pp. 177–203. Amsterdam University Press, Amsterdam (2016)
25. Clavell, G.G.: Policing, Big Data and the Commodification of Security. In: Van der Sloot, B., Broeders, D., Schrijvers, E. (eds.): Exploring the Boundaries of Big Data, pp. 89–115. Amsterdam University Press, Amsterdam (2016)
26. Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation. Brussels, 00569/13/EN, WP 2013, 2. April 2013
27. Angwin, Julia, Jeff Larson, Surja Mattu, Lauren Kirchner, und ProPublica. „Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks." *ProPublica*, 23. Mai 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
28. Yu, Persis, Jillian McLaughlin, und Marina Levy. „Big Data: A Big Disappointment for Scoring Consumer Credit Risk". Boston, MA: NCLC, National Consumer Law Center, 14. März 2014.
29. ECJ, Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294
30. ECJ, Joined Cases C-92/09 and 93/09 Schecke and Eifert, ECLI:EU:C:2010:662
31. ECJ, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238
32. ECJ, Case C-362/14 Schrems, ECLI:EU:C:2015:650
33. "Security and Privacy in your Car Act" by the Senators Markey und Blumenthal from 21.7.2015, https://www.congress.gov/bill/114th-congress/senate-bill/1806/text
34. Boehme-Neßler, V.: Big Data und Demokratie – Warum Demokratie ohne Datenschutz nicht funktioniert. Das Deutsche Verwaltungsblatt, pp. 1282-1287. (2015)
35. Roßnagel, A.: Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags (2016), https://www.bundestag.de/blob/409512/4afc3a566097171a7902374da77cc7ad/a-drs-18-24-94-data.pdf
36. Roßnagel, A., Geminn, C., Jandt, S., Richter, P.: Datenschutzrecht 2016 „Smart" genug für die Zukunft?: Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts. Bd. 4. kassel university press GmbH, Kassel (2016)