COMMUNICATION OF IN-VEHICLE DATA AND DATA PROTECTION

Wouter van Haaften / Tom van Engers

Ph.D. researcher, University of Amsterdam, Leibniz Institute
Nieuwe Achtergracht 166, 1018 WV, Amsterdam, NL
vanHaaften@uva.nl; http://www.LeibnizInstitute.nl

Professor, University of Amsterdam, Leibniz Institute
Nieuwe Achtergracht 166, 1018 WV, Amsterdam, NL
vanengers@uva.nl; http://www.LeibnizInstitute.nl

Keywords: IoT, self-driving cars, data protection, C-ITS, personal data, legal basis, subjects' rights

Abstract: *One example of IoT implementations is the introduction of self-driving vehicles. All major OEMs (car manufacturers) have announced to put a self-driving model on the market in due course. In most cases in-vehicle sensor information will be combined with car2car communication via DSRC. This paper will address a number of questions that arise when regarding cooperative intelligent transport systems technology in relation to data protection, like: are the data broadcasted by the vehicle personal data? And if so, who would be the controller, and what legal basis should it have? And last but not least, what are the data protection risks of C-ITS, and what does this mean to data protection in the IoT?*

1. Introduction

In this paper we explore further the interaction between C-ITS as a road-safety enhancing technology and data protection being a human right while looking ahead towards future developments like the rise of the Internet of Things (IoT). The latter has growing interests as vehicles transporting sensors potentially could provide useful sensor data that can be used for many applications including, but not limited to applications for mobility management. This makes the introduction of self-driving vehicles that are typically using sensors for their car control software, as well as for other functions, e.g. rain sensors controlling window wipers, temperature sensors controlling the breaking system and motor management, gps receivers, etc. one of the most challenging examples of IoT implementations.

In previous papers[1] we examined the Opinion 3/2017 of the data protection WP 29 and we analyzed the system properties in the framework of the GDPR. Many OEMs have announced their commitment to self-driving vehicles in the years to come. Most of them will, in order to achieve safe autonomous driving, depend on a combination of smart in vehicle technology and communication with other vehicles and road side operators. Data protection will be one of the main legal issues that will have to be dealt with during the development of cooperative self-driving vehicles. In this mix of technology, commerce and public interest it is important to bear in mind that data protection problems are not caused by technology alone, but primarily through *activities* of people, businesses, and the government. [2]

[1] W.F. van Haaften / T.M. van Engers, Cooperative Intelligent Transport Systems and the General Data Protection Regulation, Proceedings of the 21st International Legal Informatics Symposium IRIS 2018 and W.F. van Haaften / T.M. van Engers, Data Protection and C-ITS, a personal data proposition Proceedings of the Amsterdam Privacy Conference 2018.

[2] Daniel Solove, Taxonomy of Privacy, 2006, The University of Pennsylvania law review.

2. Scope of the paper

In order to be able to look at the data protection risks of C-ITS, the first step is to describe what C-ITS is within the context of the management of in-vehicle data. We will look at the data position of the OEM, and other service providers and the user of the vehicle (subject, art. 4.2 GDPR), also regarding the main communication protocols; Wifi-p and cellular. Then we will map the technical and social reality of C-ITS on the requirements of the GDPR. Finally, we will look at the data protection consequences when considering vehicles as «things» being part of the IoT. We will not address security issues, neither the security measures taken within C-ITS using pseudonymized certificates, nor risks and security measures related to distant control. The latter obviously will play an important role in future collaborative autonomous driving.

3. Types of in-vehicle data

Modern vehicles are big data processing devices. Most of them have one or more computers on board in order to control the functioning of the vehicle. The data from the vehicle is collected and transported by the CANbus[3]. The data is produced by sensors reflecting the current state of the vehicle. The CANbus data can be divided into three layers:

- Driveline data,
- Comfort data,
- Infotainment data.

The driveline data provide information on the functioning of the vehicle in terms of technical performance. How is the engine running, what is the state of the transmission and the breaks, and are there any aberrations that may need immediate attention? Furthermore, these data can be used for performance statistics and design purposes. Although the state of the vehicle is closely connected to user behaviour it has to be distinguished from user data.

User data reflect the actions of the user, like breaking, putting the lights or windscreen wipers on or off, changing direction, accelerating etc. This type of data will be used for user services and road safety-purposes, e.g. C-ITS data will be collected from this category.

The third layer, entertainment data, include data from radio, telephone, navigation etc. This data does not have a direct connection to the functioning of the vehicle.

4. Who is processing?

Now we have established that the car is processing data the question arises who is processing data in the vehicle and what data is being processed? When it comes to the technical data from the first layer this data is processed in the vehicle for maintenance and design purposes. It can be read at the repair shop by the maintenance crew in order to get a good picture of the state of the vehicle and of possible malfunctions that need to be taken care of. These days however technical data are also being send to the OEM via sim-chips, installed in the vehicle. In that way the OEM has a good view on the technical state of the vehicle in between servicing at the workshop. The data will often qualify as personal, since they are related to the VIN[4] of the vehicle and the OEM knows who bought the car. The status of personal data will be less self-evident however when the buyer is a company, or the car has been sold again[5].

[3] CAN bus protocol theorie en algemene eigenschappen, Bart Huyskens 2012 LED/RTC Antwerpen, https://e2cre8.be/wp-content/uploads/2015/12/CAN-BUS.pdf (all websites last accessed on January 2019).

[4] Vehicle Identification Number.

[5] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data , 20 June 2007, Example 8, Taxi case illustrating relative approach of personal data, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136en.pdf.

Less transparent is the access to user data. These data are even more personal in the sense that they are a direct result of actions of the driver, in fact the data reflect his or her behaviour. As far as the data is being sent to the OEM, the situation is about the same as with drive line data, depending on the information position of the OEM. If the OEM has no connection to the owner/driver of the vehicle, nor is it «reasonably likely»[6] that it will obtain this information, then the data are not personal to the OEM.

The third set of data, the infotainment[7] layer, can have a connection with the OEM, but it can also have a connection with other providers of services like navigation and traffic information. Via the cell phone and the car-kit also the telecom provider could be involved. To these providers at least the owner of the vehicle, being their customer, will be known.

So far, we only have looked at the data as food for potential data consumers like the OEM and Service providers. Generally, their legal basis for processing personal data will be informed consent since they have a service relationship with the vehicle owner/user, but also other legal basis may appear. The data usually are sent to the back-offices of the controllers via the cellular network using the regular point to point encrypted connections, a controlled way to transport personal data. Another technology relevant to our research is short-range communication used in the C-ITS, making in-vehicle data available e.g. for road-safety purposes.

5. What is C-ITS?

C -ITS is a protocol for communication between vehicles and between vehicles and roadside stations (V2V and V2I). The chosen way of communication is via Wifi-P, the ETSI 802.11.p protocol for broadcasting at a short range of approximately 500 meters. Eventually C-ITS will find its ultimate purpose in facilitating the communication between self-driving vehicles additional to in-vehicle sensors. By using C-ITS vehicles and infrastructure will communicate fast, without latency, and everywhere, independent of the coverage of a telecom network. These two features are the reason that cellular communication is not being used. The cellular network doesn't have a 100% coverage, and the transmission of data to a back-office and back to the road in some situations will take more time than the direct communication via the short-range C-ITS.

But not only self-driving cars can drive more safely with the support of C-ITS. Also, current traffic could benefit from the capabilities of C-ITS short-range communication for road safety purposes. A list of so called «day one» applications is being made containing road safety services. These applications (see fig 1) could provide for more road safety in the short term. It is the intention to give these applications a legal basis in a Delegated Act as foreseen in Article 7 of the ITS Directive[8]. In order to achieve these road-safety results vehicles will broadcast a set of data via a Cooperative Awareness Messages (CAMs) that are permanently broadcasted in a frequency of, approximately, 10 per second. The data are not encrypted due to the fact that it does not make sense to encrypt messages that all other road users should be able to read anyway. Eventually, C-ITS is expected to be a necessary link in the safety scheme of self-driving cars. These will probably need V2V communication on top of their own sensor-based intelligence thus extending the reach of the vehicle's sensor space.

[6] W.F. van Haaften / T.M. van Engers, Data Protection and C-ITS, a personal data proposition Proceedings of the Amsterdam Privacy Conference 2018, Elaboration on Recital 26.

[7] A contraction of the words information and entertainment expressing the character of this layer serving both purposes.

[8] European Parliament and Council, Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040.

Source: ACEA

Day 1 C-ITS services list	Road safety	Latency sensitive
Hazardous location notifications:		
· Slow or stationary vehicle(s) & traffic ahead warning;	x	x
· Road works warning;	x	x
· Weather conditions;	x	x
· Emergency brake light;	x	x
· Emergency vehicle approaching;	x	x
· Other hazards.	x	
· Shockwave damping	x	
Signage applications:		
· In-vehicle signage;	x	
· In-vehicle speed limits;	x	
· Signal violation / intersection safety;	x	x
· Traffic signal priority request by designated vehicles;	x	
· Green light optimal speed advisory;		
· Probe vehicle data;		

Fig. 1 List of «Day one» applications

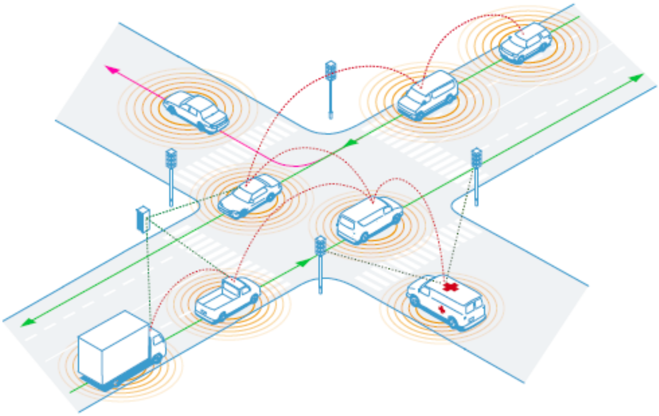

Fig. 1 C-ITS Intelligent Traffic Lights

6. C-ITS and data protection

In a recent paper [9] we argued that in-vehicle data broadcasted by a vehicle within the framework of C-ITS should not be considered personal. The decisive argument was that the broadcast is conducted by the vehicle, i.c. by the driver of the vehicle also being the subject. As long as the CAM data are in the vehicle legally they are being processed under control of the driver of the vehicle[10]. When the CAM is being broadcasted it does not change status until the data is being received by another entity, either in or outside the scope of C-ITS. In the discussions held thus far in WP4 of the EU C-ITS Platform[11] the broadcasted data were considered to be personal data, which posed the unsolvable problem that a controller had to be found that could take responsibility for the broadcasting process. However, the group did not succeed in finding such controller, in our opinion because the broadcasting itself does not (yet) include personal data, and thus does not require a controller in the first place. This argument is supported by the fact that the purpose and means of the processing[12] will not be determined by any operational party but will be prescribed in the C-ITS Regulation. A receiving vehicle will process the data for road safety reasons within the legal framework for C-ITS as is foreseen. When the other vehicle is processing the data it will still not become personal data because no personal aspects are likely to be added.

Another participant within the C-ITS system is the road infrastructure as managed by the road Authority. At the moment traffic lights receiving messages from vehicles that are being used to improve traffic management and traffic flow through on intersections are being tested (Fig 2). The received data in road side units (RSUs) will qualify as personal data, even more since most road operators are public entities with access to the vehicle registration.[13] In order to make their position transparent and accountable the role of the RSUs should be specified in the
C-ITS Regulation in order to create a controllable framework when it comes to data protection.

7. Personal data by singling out

CAMs will be personal data to the RUCs and not to the participating vehicles unless these are functioning as receivers from private companies collecting the data for their own commercial purposes. These receivers may be able to single out a vehicle, and thus inevitably also single out the driver, as long as there are no level 5 self-driving vehicles around. This singling out is considered to transform the data into personal data due to the fact that it will be possible to approach the individual(s) in the «singled out» vehicle with targeted messages, like advertising even when the identity of the natural person(s) is unknown, and also will not be known by the receiving entity. This purpose for which they single out the natural person(s) in the vehicle will often be described as «behavioral targeting»[14]. Reception of a CAM on one spot along the road may only facilitate advertising that is very location- and time framed, like an advertisement for a restaurant further down the road.

[9] Van Haaften / van Engers, Data Protection and C-ITS, a personal data proposition, Proceedings of the Amsterdam Privacy Conference 2018.

[10] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), Berlin, 26 January 2016.

[11] Group of interested parties chaired by EU Commission consisting of representatives from the automotive industry, insurance companies, telecom companies and administrations of Member States.

[12] Artikel 4.7 GDPR.

[13] European Union Court of Justice, Case nr. ECLI:EU:C:2016:779, Breyer vs BRD.

[14] Frederik J. Zuiderveen Borgesius, Online Price Discrimination And Data Protection Law, Amsterdam Law School Legal Studies Research Paper No. 2015-32 Institute for Information Law Research Paper No. 2015-02.

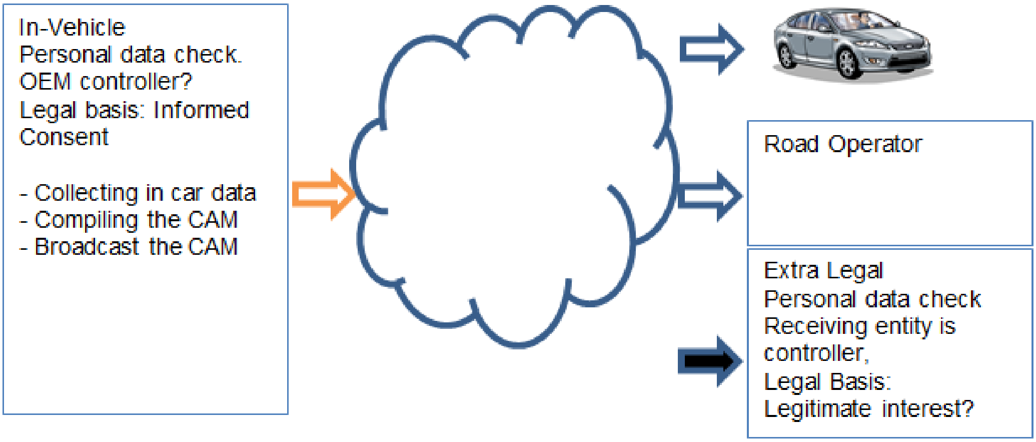

Fig. 2 Broadcast of CAMs

8. Non-C-ITS qualified processing

The aforementioned non-C-ITS qualified data processors are receivers of CAMs without being part of the C-ITS infrastructure. One could think of commercial parties that build a network to be able to follow vehicles broadcasting in a certain area for instance for marketing reasons. It has been shown[15] that it is possible to build such a network at relatively low costs thus enabling the collection of data that in first instance would single out the vehicle but could eventually even lead to a full identification of the subject by the non-C-ITS qualified processor. It is this ability that drove the Working Group 4 of the EU C-ITS Platform and thereafter the Working party art. 29[16] when appointing the CAM as personal data. Since these receivers of the CAM actually do process personal data, the requirements of the GDPR will have to be fulfilled. The received data will become personal once they are being captured by the non-C-ITS qualified processor. This means that the processor will have to be considered a controller in the sense of art. 4.7 GDPR obliged to find a proper legal basis for its processing and offering all the legal guarantees to the subject granted by the GDPR. It seems that the most obvious legal basis that could be applied would be a legitimate interest of the controller. However, that would demand a balance of interest between the subject and the controller. Since the subject can only be identified after the processing has started, and even then, at first instance only by singling out, such a test up-front is not possible. From the CAM itself no identification of a specific subject can be derived since the CAM does not contain identifiers that could lead to identification by others then the parties that already have other data e.g. stemming from a relationship with the owner/driver, like OEMs and contracted service providers (see for CAM content[17]) or big data companies.

[15] Leonid Reyzin / Anna Lysyanskaya / Vitaly Shmatikov / Adam D. Smith, Comments on NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications (Docket No. NHTSA-2016-0126), link: https://cdt.org/files/2017/04/FMVSS150CommentsOnPrivacy-as-submitted.pdf.

[16] Now known as the Data Protection Board, art 68 GDPR.

[17] W.F. van Haaften / T.M. van Engers, Cooperative Intelligent Transport Systems and the General Data Protection Regulation, Proceedings of the 21st International Legal Informatics Symposium IRIS 2018.

9. Enforcement

Thus, it seems that the processing of CAMs by an unknown processor outside the C-ITS framework, generally will be illegal. That raises the question how enforcement should be arranged for, and what will be the position of the subject? To start with the first question, the actual enforcement of non-compliance with the GDPR is delegated to the national Authorities. They will be operating under national legal and policy (priority) conditions.[18] It will not be easy to have a communitarian enforcement strategy implemented throughout the EU since no community wide interventions are to be expected.

But how profitable will it be to illegally obtain vehicle data from C-ITS broadcasts while these data can also be obtained legally (via informed consent) from the smartphones on board of the vehicles?

If a non-C-ITS qualified processor wants to follow vehicles in a certain environment, it may be easier and cheaper to obtain these smartphone data from companies that already have access to big smartphone data like Google, Facebook etc. In this respect the significance of the CAM as a data leak should not be overrated, especially since the fines can be high. Most people are very visible due to the way they are using their smartphone these days and seem hardly aware of their position as data subject.

10. The position of the data subject

So, what can the subject do to limit the chances of abuse of personal data in case that enforcement is at least an uncertain factor? Unlike in the case of his or her smartphone, the broadcast of the CAM is (yet) not designed to be switched on or off by the subject. What does this mean in terms of data protection? Broadcasted CAMs may not be personal data, but received CAMs will be, they become personal data at reception since the CAM consists of a data package that may single out the vehicle. If CAMs could only be received by recipients involved in the system, like admitted road side stations contributing to the provision of road-safety information to the subject, that might not have been a problem. But since the CAMs can be received and read by anybody it is impossible to tell if the CAM is being received by other entities, and if so, who they might be. This uncertainty means that the subject has no way to tell whether his or her personal data are being processed or not. The risk of abuse is there, and in the current system the subject has no way to mitigate the risk because the system is switched on by default. This is a serious threat to the subjects» privacy, as also the WP 29 concluded in its Opinion on C-ITS[19]. One of the main objectives of privacy protection is practical obscurity[20], the ability to remain relatively unobserved in the public domain. In order to achieve that a subject should not be forced into a position where the subject can no longer control its personal data and only can hope and pray that no one is abusing it. This means that although the broadcasted data as such may not be personal data, the system is not privacy proof as long as there is no choice to switch off the C-ITS broadcast in order to prevent its leakage of personal data.

11. Weighing privacy and road safety

Looking at this situation, and the Opinion of the WG29, it seems logical to change the design and thus give the subject the possibility to switch off the broadcast of CAMs from the vehicle, thus providing the subject with a choice. So how would this on/off switch influence the pursuit of the road-safety objectives with day-1 services? Road-safety as such is a public interest, and in specific situations it can be a personal interest too. It could even be a vital personal interest for the subject itself in certain dangerous traffic situations. Yet it is hard to see how such an interest in a safety threatening event that may – or may never – occur, justifies the

[18] Art. 50 and 57 GDPR.

[19] Article 29 Data Protection Working Party, Opinion nr 3/2017 on Cooperative-Intelligent Transport Systems, October 2017, http://ec.europa.eu/newsroom/just/document.cfm?docid=47888.

[20] Daniel J. Solove as cited and by Henk Griffioen, in: Privacy en «intelligente» vormen van mobiliteit Amsterdam University Press 2011.

breach of an individual right to protection of his or her private family life as established in the EU Convention on Human Rights[21]. In order to balance the road-safety and the data protection objectives the first question that arises is; could these road-safety enhancing services also be delivered without using Wifi-p? If the answer would be yes, then it is obvious that finding a legal basis for prescribing a CAM broadcast to car users will be virtually impossible.

So, let us assume that for the «Day one» services of C-ITS cannot be performed with other, e.g. cellular, technology. After all, cellular technology with its point to point encrypted character would solve the data protection issue to a large extend. But for a number of services full and reliable coverage and the insurance of a low latency cannot be done without. What elements are there to be weighed in the balancing test between road safety and privacy?

Although the broadcast of the CAM itself will not be regarded personal data, the GDPR is applicable at least as far as it comes to the risk of processing personal data by non-C-ITS qualified processors. This risk is hard to quantify and could be substantial when such non-C-ITS qualified processors would really present themselves. This means that also security and Privacy by Design requirements must apply with a view on eventual non-C-ITS qualified use. Since the GDPR is not applicable on the broadcast itself, this means that the GDPR is not applicable on at least a part of the C-ITS data processing (fig 2). And if, in those circumstances, legislation (i.c. the ITS Delegated Act) were to prescribe C-ITS as an obligatory road-safety feature, then the legislator will also have to take responsibility for the data protection consequences of that prescription. The legislation will have to come with an explanation of the obligation to use C-ITS and perhaps even with a balancing test, using GDPR milestones in order to verify compliance with data protection principles.

When the obligation to use the current version of C-ITS is balanced with the principles of data protection in Art 6 of the GDPR it becomes clear how hard it will be to fulfil the requirements following from GDPR, for the following reasons:

- Lawfulness and fairness may be upheld within the C-ITS context, but not for third party use of CAMs after broadcasting,
- Purpose limitation is only possible as far as the CAM is concerned, extended use by non-C-ITS qualified operators cannot be prevented nor controlled,
- Data minimisation is not under control of the legislator,
- Storage limitation is not guaranteed in the legislation. C-ITS CAM use itself does only imply a very brief storage of CAM data in the RSU,
- And last but not least the broadcasted data cannot be secured, it is broadcasted unencrypted.

It is obvious that the legal obligation to use C-ITS will not be accompanied by a balanced privacy framework. Most of the principles of data protection cannot be fulfilled outside the specific C-ITS context. This negative score on data protection must be neutralized by a (very) positive effect that this technology may have on road-safety in case of the «Day one» services. These services enhance road-safety, in a general and not very precise way. Whether, and to what extend», better road-safety can be achieved is hard to predict. If it would be possible to actually point out the situations where the services would most likely safe lives, that would at least lead to a solid, factual consideration. But such a consideration is not available in this case.

Overlooking the Wifi-p picture it does not seem reasonable to prescribe obligatory use of C-ITS. Like WP 29 in its Opinion 3/2017[22] stated, the driver should at least have the opportunity to switch the device off, or better still, the device should be off by default and the driver should switch the system on whenever desired:

[21] Article 8 of the European Convention on Human Rights, https://www.echr.coe.int/Documents/ConventionENG.pdf.

[22] Article 29 Data Protection Working Party, Opinion nr 3/2017 on Cooperative-Intelligent Transport Systems, October 2017, p. 13, http://ec.europa.eu/newsroom/just/document.cfm?docid=47888.

Privacy by Design. In case of a free choice for the driver to switch the C-ITS off or on the impact of C-ITS is still uncertain, but the driver can make his or her own choice whether or not to participate. Although this could lead to a devaluation of the road-safety abilities of the system, it may appear to be the only way to get the system on the road in the current situation where human drivers will be the addressees of C-ITS traffic recommendations.

The balancing test may turn out different once fully automated cars will enter the stage. On the road safety perspective, they will be more depending on C-ITS to cooperate with on board sensors in order to be able to drive safely. From the data protection perspective, self-driving vehicles have no driver and may occasionally even have no occupants at all. Data protection could be less problematic in those circumstances. For this moment however, the OEMs should be advised at least to provide for an on/off switch for the C-ITS device.

12. The vehicle as part of the internet of things

In this paragraph we consider the vehicle as a part of the IoT within the framework data protection, the application of the GDPR. Since the term Internet of Things (IoT) was first used in 1999[23] several definitions of the phenomenon have arisen. Most basically the Internet of things (IOT) is a network of physical objects. This network, even if it is called «internet», should not be confused with the host to host internet as we know it. The IoT is independent of any type of communication technology. As Patel et al describe «Internet of things (IoT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies»[24]. It can use any kind of communication technology, be it wired, short-range or cellular technology as long as it can communicate. The next questions are: what's is communicating? What is a «thing»? Within the framework of this paper we will define a thing as an object, or an assembly of objects (system) with communication capabilities. Since we are focusing on vehicles this means that i.e. breaking disks are no «things» but break claws can be, e.g. when they are equipped with sensors and communication abilities. A tire is not, but a tire pressure sensor is, as soon as it is connected. Apart from the individually communicating objects (things) in the vehicle also the vehicle itself can be defined as a «thing», a multi object system.

13. The vehicle as smart object

Things come in all sort and sizes, but they have one thing in common, they understand and communicate with their environment, they are Smart Objects (SOs)[25]. When we look at the vehicle, we must conclude that it has all properties to be a SO, but also its components can be SOs as long as they, to a certain extend, can understand their environment and are able to communicate. A SO is an autonomous, physical digital object augmented with sensing/actuating, processing, storing, and networking capabilities. SOs are able to sense/actuate, store, and interpret information created within themselves and around the neighboring external world where they are situated, act on their own, cooperate with each other, and exchange information with other kinds of electronic devices and human users.

14. Data management

Within the framework of data protection SOs require a data management layer that is capable of managing the data in a proper way, living up to the GDPR. This will lead to questions like: whom will take the data

[23] Jayavardhana Gubbi et al., Internet of Things (IoT): A vision, architectural elements, and future directions, , Future Generation Computer Systems 29 (2013) 1645–1660 Elsevier.

[24] Keyur K Patel / Sunil M Patel, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, DOI 10.4010/2016.1482 ISSN 2321 3361 © 2016 IJESC, Research Article, Volume 6 Issue No. 5.

[25] Gerd Kortuem et al., Smart objects as building blocks for the Internet of Things, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5342399.

management role, and how does it relate to the role of the controller within the GDPR framework? As far as in-vehicle data is concerned the OEM will have installed a data management system within the vehicle. Also, the data that is withdrawn from the vehicle by the OEM will be under its control. Up to this moment data management and controllership are in one hand. However, data that is coming out of the vehicle in e.g. via Wifi.p will not be controlled by the OEM. There may be a responsibility to the OEM for the functioning of the device towards the owner, but not for the data processing itself.

15. Privacy by design, interoperability and standardisation

The fact that not all data transfers within the IoT will be covered by a responsible controller demands for a built-in data protection architecture, i.c. Privacy by Design. To achieve this type of general architecture both facilitating the data flows within the IoT while preserving data protection, one issue will be leading: Interoperability. From our analysis of the impact of the movement of in-vehicle data from a data protection perspective it has become clear that decisions with heavy impact on the eventual compliance of the internet of things to the GDPR have to be made by an OEM in an early stage of vehicle development. These design decisions will also be PbD decisions that OEMs should not want to make all by themselves. Interoperability can only be achieved with many participants which means that OEMs should be stimulated to join forces on this issue. That is the only way to come to an adequate level of standardisation.

16. Conclusions

In this paper we have analysed the data protection aspects of the C-ITS Wifi-p protocol. The broadcasted CAMs contain data, like location and car size, that could lead to singling out the vehicle and thus the subject. This can occur as soon as the CAM is being received. At broadcast however, CAMs are not to be considered personal data, since the broadcast is conducted from the vehicle, under control of the subject itself. At the reception of the CAM three potential controllers have been looked at, two within the C-ITS and one outside the system. Within the C-ITS the CAMs are being received by other vehicles (V2V) and by RUCs (V2I). This processing will be covered by the C-ITS Regulation. In case of the V2V the data normally will remain non-personal since the purpose of the data transfer does not require any handling of the data that could lead to a single out. That may be different for the V2I broadcast. The RSU will process and even store the data for some time and may be able to single out the passing vehicles. Also, it may be able to collect additional information in order to come to a full identification of the vehicle. Singling out is also possible with the V2X communication due to the fact that the broadcast admittedly is local, but still can be read by anyone picking up the CAM.

So even when the CAM at broadcast is not to be considered personal data, in the aftermath of the broadcast, at reception that status can change. This arises the question of how to protect the subject? Is the general purpose of C-ITS, road-safety, reason enough to deprive the subject of sufficient data protection? In our view this is not the case. The subject in C-ITS, i.c. the driver of the vehicle, should be given the opportunity to switch off the CAMs. In that way he or she will be able choose not to spread data that might become personal in hands of unknown entities. This perspective may change once self-driving vehicles will be depending on C-ITS for operating safely.

The positioning of a vehicle as SO in an IoT environment adds another dimension to the management of the sharing of in-vehicle data. In order to make sure that the IoT in case of vehicles meets the obligations of the GDPR the automotive industry should introduce Privacy by Design and standardisation as basic vehicle design principles. Only then an interoperable data protection environment will be created that will comply with the GDPR. How this data protection design should be conducted and how this will work out for other areas within the IoT will be subject to further research.

17. References

European Parliament and of the Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJEU L119, 4 May 2016.

European Parliament and of the Council Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEU L281/31, 24 October 1995.

Article 29 Data Protection Working Party, Opinion nr 4/2007 on the concept of Personal data, 20 June 2007, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136en.pdf.

Article 29 Data Protection Working Party, Opinion nr 13-2011 on Geo location services and smart mobile devices,16 May 2011, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185en.pdf.

Article 29 Data Protection Working Party, Opinion nr 3/2017 on Cooperative-Intelligent Transport Systems, October 2017, http://ec.europa.eu/newsroom/just/document.cfm?docid=47888.

Cooperative Intelligent Transport Systems Platform C-ITS), Final Report Data Protection & Privacy Analysis of Data Protection & Privacy in the context of C-ITS, Recommendations and guidelines, Based on the work of WG-4 of the C-ITS Platform Annex to Final Report Version 1.2 – January 2016, https://ec.europa.eu/transport/sites/transport/files/themes/its/road/actionplan/doc/c-its-platform/2016annexestothec-itsplatformfinalreport january2016.zip.

European Standard ETSI EN 302 637-2 on Intelligent Transport System V1.3.0. 2013-8 ITS vehicle comm. Specs. Cooperative awareness service, August 2013, https://www.etsi.org/deliver/etsien/302600302699/30263702/01.03.0130/en30263702v010301v.pdf.

European Standard ETSI EN 102 638 on Intelligent Transport Systems V1.1.1. 2009-6 ITS Vehicle comm. Basic set application definition, June 2009, https://www.etsi.org/deliver/etsitr/102600102699/102638/01.01.0160/tr102638v010101p.pdf.

Leonid Reyzin / Anna Lysyanskaya / Vitaly Shmatikov / Adam D. Smith, Comments on NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications (Docket No. NHTSA-2016-0126), link: https://cdt.org/files/2017/04/FMVSS150CommentsOnPrivacy-as-submitted.pdf

W. van Haaften / T. van Engers, (2015) Data Protection And Cooperative Driving, in: *Proceedings of the 22nd World ITS Conference* (ITS-2665), Bordeaux.

W. van Haaften / J. Wennekers / T. van Engers, Data Protection and C-ITS – A Use Case, Proceedings of the 11th EU ITS Conference , Glasgow.

W. van Haaften / T. van Engers, Data Protection and C-ITS – Personal Data, 12th EU ITS Conference, Strasbourg.

Henk Griffioen, in: Privacy en «intelligente» vormen van mobiliteit, Amsterdam University Press 2011.

European Union Court of Justice, Case nr. ECLI:EU:C:2016:779, Breyer vs BRD.

Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), Berlin, 26 January 2016.

Kevin Ashton, That «Internet of Things» Thing, June 22, 2009– RFID Journal.

Keyur K Patel / Sunil M Patel, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, DOI 10.4010/2016.1482 ISSN 2321 3361 © 2016 IJESC Research Article, Volume 6 Issue No.5.

Gerd Kortuem et al., Smart objects as building blocks for the Internet of Things, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5342399.

CANbus protocol theorie en algemene eigenschappen, Bart Huyskens 2012 LED/RTC Antwerpen, https://e2cre8.be/wp-content/uploads/2015/12/CAN-BUS.pdf.

W.F. van Haaften / T.M. van Engers, Cooperative Intelligent Transport Systems and the General Data Protection Regulation, Proceedings of the 21st International Legal Informatics Symposium IRIS 2018.

W.F. van Haaften / T.M. van Engers, Data Protection and C-ITS, a personal data proposition Proceedings of the Amsterdam Privacy Conference 2018.