Data Protection and C-ITS - Personal Data

Wouter van Haaften[1*], Tom van Engers[2]

1. Leibniz Center for Law, University of Amsterdam, The Netherlands, vanhaaften@uva.nl

2. Leibniz Center for Law, University of Amsterdam, The Netherlands, vanengers@uva.nl

Abstract

Under the influence of massive data collection both by commercial parties and by public authorities the protection of personal data is getting more and more under pressure. The data protection authorities justly take a strong stand against abuse of personal data. However in the case of C-ITS it seems to lead to restrictive interpretations of the data protection legislation. Such interpretations may have an inhibitory effect on innovation. In this stage of development industry would benefit from legal certainty. In this paper we will argue that Cooperative Intelligent Transport Systems (C-ITS) using the 802.11p. wifi protocol do not necessarily process personal data. The arguments are based on the legislation, opinions of the EU Data Protection Authorities and recent jurisprudence of the EU Court of Law. Now the implementation phase of C-ITS is approaching and the technical specifications are to a large extend developed this seems a good moment to bring our opinion forward.

Keywords: Cooperative driving, automated driving, data protection, personal data

Introduction

The intensive and widespread use of the internet and more specific of mobile devices providing and collecting data inevitably leads to privacy questions and concerns. Drivers of these concerns are the available technical abilities and on-going developments enabling data coupling and analysis, and the fact that very large US companies like Facebook and Google dominate the market of internet services. Their operations collect massive amounts of data from computers and smart phones. The subjects, computer and smart phone users, can hardly get any insight into the use and possible abuse of their data. The gap between data processing practice and data protection seems to get wider. It is a gap between for instance the EU and the US since the European Court of Law rejected the safe harbour agreement, thus blocking the processing of EU personal data in the US[1] arguing that EU personal data were not similarly well protected in the US. Also a gap exists between the individual user's perception of privacy in relation to his or her smart devices and the collective value of having 'our' personal data protected. The newly established GDPR[2] tries to keep up with the very rapid developments by emphasizing the necessity of well-designed data collection and processing operations combined with

[1] Judgment in case C-362/14, 6 October 2015

[2] Regulation (EU) nr. 2016/672 applicable as of 25 May 2018.

serious enforcement embodied in substantial fines for offenders of the regulation. Apparently the individual user of devices like smart phones are not in a position to overlook all the risks involved in their use of mobile apps and their participation in social media. The vast list of conditions that has to be agreed to when opening a new app or service is often clicked away mechanically. Still it is widely agreed that 'respect for a person's private and family life, his home and his correspondence[3]' is an important attainment in our free and democratic society. This fundamental right has been translated into EU data protection legislation thus providing for a solid bases for the protection of individual citizens using smart devices. Nevertheless both commercial companies as well as public authorities responsible for public safety seem to be allowed to be privacy evasive as long as respectively personal convenience or public safety are at stake. The massive use of the commercial services as well as the loud call for permanent camera surveillance after the Berlin Christmas market attack[4] seem to illustrate the ambiguity of our relation to privacy.

One of the fields where it is challenging to find the balance between the protection of personal data on the one hand and applying new technology on the other hand is Cooperative-Intelligent Transport Systems (C-ITS). This is one of those areas where the choice for a more or less extensive application of the data protection legislation can directly influence the possibilities of the application of new technology. In such conditions it would help if the data communication could be set up in such a way that no personal data are involved. Scrutinizing this presumption is the main objective of this paper. It is formulated from the presumption that no personal data need to be involved considering public road safety use cases. For commercial services however the processing of personal data may be inevitable. To that end also paid, commercial services have been left out since these services often mean to identify the user in the first place, for instance for invoicing purposes. In this paper we will focus on public road safety applications.

This paper will be exploring the issue of data processing in a C-ITS Wifi p. environment using in car equipment. It focuses on the question if the data broadcasted by the vehicles should be considered as personal data and which elements will prevail in that consideration. Other communication networks like the mobile telecom network have been excluded because at this moment within the EU Wifi p. (still) is the leading technology. Also not vehicle specific personal devices like smart phones or tablets are not included in this paper.
In the first paragraph the risks of the gap between the protection of personal data and the use of in car vehicle data within C-ITS applications is being addressed. Clarity on this issue is necessary to help investments being done in order for innovations to move on. Then the long term perspective of self

[3] Art 8.1 EU convention on human rights.

[4] On 19 December 2016, a truck was deliberately driven into the Christmas market beside Kaiser Wilhelm Memorial Church at Breitscheidplatz in Berlin. The terrorist attack left 12 people dead and 56 others injured.

driving, cooperatively communicating, vehicles is set out, the Wifi p. protocol is explained and the application of data within C-ITS is being disclosed. Finally the concept of personal data from the EU Directive, as analysed by the EU data protection commissioners[5] and plotted on the C-ITS environment, is being looked into. The outcome is confronted with the data protection principles that play a leading role in the data exchange process. The conclusions will reflect the findings of this search.

Closing the gap

There is a remarkable gap between the determination of the authorities to protect personal data and the carelessness with which we give away our personal data. In our view this gap is worrying and raises questions like: Why do people give away their personal data so easily? Is it ignorance, laziness or infinite confidence in the companies collecting the data? As was pointed out in our paper in 2015[6] it cannot be expected from the average citizen to have a serious understanding of the impact of a consent given to a commercial party on the use of his or her personal data, even if the consent was given after receiving the relevant information. Closing this gap may appear to be one of the major issues in the coming years. A balance will have to be found between the protection of privacy on the one hand and the legitimate purposes of personal data processing in compliance with basic principles like transparency, proportionality, subsidiarity and accountability on the other. Can these principles be sufficiently met in C-ITS applications, and how should the legal framework be applied regarding the balance between the protection of the personal environment of the individual and the development of cooperative applications especially those supporting a common good like road safety? In that respect it is important not to let the legitimate and well-documented concern about the protection of our privacy to develop into a suffocating intervention of the data protection legislation in day-to-day life. By labeling data extensively as personal not only the data protection will be established, but also less intrusive applications will become submissive to the, sometimes quite evasive, data protection legislation. Since the authorities on data protection will be carrying a big stick[7] the utmost will be acquired of their abilities to use that stick in a proportionate way. The rapid development of data processing techniques, such as data mining and artificial intelligence seem to invoke a response that, however understandable, can easily lead to unforeseen and unintended side effects. C-ITS is one of the technologies where the application of the data protection legislation should be very well scrutinized since it could appear to be a potential showstopper in cases where the assumed conditions for the processing of personal data cannot be met. This paper focuses on one of the moments where a data protection relevant decision has to be made: at the start of the designation of a data processing

5 Named after the Article 29 in which the group has been established: Working Party art. 29

6 Data protection and cooperative driving Van Haaften-Van Engers 2015, Henk Griffioen WRR 2011

7 Potential Fines on breaking the data protection rules will go up to 10 mln euros or 2% of the annual turnover of the offending company (Art. 83.4 GDPR)

operation. One of the first questions that will have to be answered is; what data does the new application require? Directly followed by the question if these required data are to be qualified as personal data? In relation to the various C-ITS use cases this issue has to be settled, because the answer given by the authorities could have huge impact on the practicability of the system, and thus on the willingness of the industry to invest in this kind of innovation.

Long term perspective: Self-driving/Cooperative vehicles

Before looking at the specific application of the data protection rules on C-ITS applications it is necessary to introduce the long-term perspective: self-driving vehicles. In the testing of autonomous vehicles it has become increasingly clear that self driving cars will have to communicate with their environment, road side stations, but particularly other road users (V2X). This means that self-driving vehicles will use C-ITS technology to be able to communicate with other vehicles at short range. The self driving cars will sent and receive messages related to their position aimed at improving their performance. This communication is now foreseen as continuous. Since the vehicle will eventually be able to drive without a driver or any other person in the car, messages from the vehicle will in principle not have to contain personal data. When looking at C-ITS as a stepping stone towards self driving cars it would be sensible to avoid the processing of personal data also in this preliminary phase. The WP 29 has given a number of instructions on which issues the data should be scrutinized in order to achieve that[8].

Personal data and C-ITS

First of all it should be stated that this search is not about avoiding the protection of the privacy altogether. Data protection will be the starting point, also when the data protection legislation appears not to be applicable. Principles like transparency and accountability will remain important to the operation and in order to check whether the claim for not processing personal data is still valid. But also data- and storage minimisation and other data protection principles will have to be strived for. If not because of the applicability of the Directive, at least to make sure the data do not become personal data anyway.

Related to C-ITS this means answer to the question: Can C-ITS do without personal data? And if so, can the processing of personal data be avoided altogether? The answer to this last question will determine whether the data protection legislation will be applicable or not and therefor has to be scrutinized.

Starting point is that the data coming from the vehicles in C-ITS are prescribed CAM[9] or DENM[10] messages. The data are coming from the car via either a device installed by the car manufacturer or via

8 From the opinion nr 2007/4 of the WP 29, p 6-25

9 Cooperative Awareness Message

10 Decetralized Emergency Notification Message

an aftermarket provider. The CAM itself consists of a header and a container for which a wide number of potential data fields have been defined. In the container the service data are collected, like location, speed, direction, dimensions of the vehicle etc. Depending on the use case other groups of data could be involved. In order to comply with the data minimisation principle the data sets should be kept as small as possible for the service concerned. The header of the CAM message contains two possible identifiers that are both optional depending on the choices made by the users. The message identifier may be required for the functioning of the service but it is to generic to lead to a subject. The station/ID however, for instance the MAC address[11] of the transmitter, may be connected to the vehicle. Since the MAC address does not have to be connected in any way to the vehicle identification it seems safe not to use the station/ID in the CAM header at all. In this way the CAM message will actually be anonymized.

C-ITS and the 802.11p Protocol

Cooperative Intelligent Transport Systems (C-ITS) use broadcasting technologies that allow road vehicles to communicate with other vehicles, with traffic signals and roadside infrastructure as well as with other road users. The systems are also known as vehicle-to-vehicle communications, or vehicle-to-infrastructure communication[12]. These technologies come with a lot of data exchange to and from vehicles, both with other vehicles and with roadside units involved in the system. In this paper we choose to focus on the cooperative system broadcasting via the 802.11p. wifi protocol although also cellular technology, via the mobile phone infrastructure may be possible in the future when latency times of the telecom infrastructure will drop to, traffic speed safe, values of milliseconds. The 802.11p. technology implies that the vehicle broadcasts a signal via short range (wifi) communication that can picked up by anybody within the range of the transmitter (ca 500m). No encryption will be applied, since everybody must be able to understand the message for road safety reasons. This implies complete visibility of the vehicle both visually and electronically at a certain location. However the messages are being pseudonomised, so that the electronic identification of the sending vehicle will be hampered still allowing verification that the data come from an authentic source. Using the 802.11p. broadcasting technology means that only the location of a vehicle could still appear to be an identifying element in the anonymized CAM message. How do all these elements relate to the concept of data protection?

The Concept Of Personal Data

In order to get a view on the way personal data are being perceived in the EU a good starting point is WP 29, the EU data protection commissioners. In its opinion on personal data (WP29 2007-4) it is stated that ' The Directive contains a broad notion of personal data', implying that data that may be

[11] Mac address is the media access address connected to a hardware device (f.i. on-board-unit, smart phone PC, etc.)

[12] Final report EU C-ITS Platform January 2016

associated with a natural person should not be easily qualified as non-personal. In that same opinion however it is also stated that ' The scope of the data protection rules should not be overstretched'. This paradox underlines that Data Protection Law consists of open norms, that have to be filled in case by case. It means that an overall approach on C-ITS level can only be indicative. That also goes for one of the most important steps in the process, establishing whether or not the data involved are to be considered personal data. It seems worthwhile to elaborate some more on the scope of the concept of personal data.

Likely and Reasonably

One of the points that WP 29 also makes is that 'in recital 26 and 27 of the Directive EC 46/95 restrictions on the applicability of the directive have been formulated'. Recital 26 states: "Another general limitation for the application of data protection under the Directive would be processing of data under circumstances, where means for identifying the data subject are not “likely reasonably to be used”. WP 29 concludes that "In those cases where a mechanistic application of every single provision of the Directive would at first sight lead to excessively burdensome or perhaps even absurd consequences, it must be first checked:

1) whether the situation falls within the scope of the Directive, in particular in accordance to Article 3 thereof; and

2) where it falls within its scope, whether the Directive itself or national legislation adopted pursuant to it do not allow for exemptions or simplifications with regard to particular situations in order to achieve an appropriate legal response while ensuring the protection of the individual’s rights and of the interests at stake. It is a better option not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data."

In case of doubt whether data are to be considered as personal data, from a data protection perspective it is better to use the flexibility within the data protection legislation than to have the processing of those data outside the legislation. However there may be situations where this alleged flexibility is lacking, even when the means for identifying the data subject are not “likely reasonably to be used", or in cases where personal data is not at all required for delivering the service, as may be the case in public safety C-ITS use cases.

Use case

In most safety related use cases, like collision warning, where vehicles send or forward a received message from a roadside station or from another vehicle the message does not have to contain any identifying data. The procedure could go as follows: the vehicle sensors spot the tail of a traffic jam just behind a hill, not visible for traffic coming from behind. It sends the message and the oncoming vehicles can anticipate on the situation by slowing down gradually. In this situation no identifying

personal data, and also no data like license plate- or vehicle identification number that could make the owner of the car identifiable, are required. Not even the MAC-address of the transmitter in the vehicle has to be revealed since the messages from the vehicle are packed with a pseudonomyzing certificate in order to make sure that the data is coming from an authentic source.

Personal

In order to establish whether the messages broadcasted from the vehicle with Wifi-p protocol should be considered personal data, these messages should be mapped on the legal definition of personal data: any information related to an identified or identifiable natural person.

Any information

The first part of the legal definition is information, any information to be precise. The information involved in C-ITS is packed in the messages broadcasted from the vehicle. What data are will be sent? For the functioning of the C-ITS scheme at least the CAM message has to be broadcasted. The CAM message could contain the MAC-address of the broadcasting device, but it doesn't seem to be necessary.

The WP 29 notes that: "The term “any information” contained in the Directive clearly signals the intention of the legislator to design a broad concept of personal data. This wording calls for a wide interpretation. In the wording of the WP 29: 'Location data, for instance could well qualify as personal data, provided it facilitated identification'.

So the next step is to establish whether the natural person involved (we are still in the pre-self driving age) can be identified from the information directly. Does the CAM-message contain any identifier of a natural person? Could a MAC-address in the header of the CAM qualify as such for a data subject, or the location data from the CAM messages? And if so for which data subject, the driver, the owner or the user, being a family member or an engineer from the repair shop making a test drive after maintenance?

Regarding the list of data in the CAM message[13], it looks like the CAM message doesn't need to contain any personal data. Other information in the CAM message that could be revealing is the location data and the dimensions of the vehicle but since there is no additional element that could lead to identification this seems unlikely. Studies on the (ab)use of location data point at the combination of smart phones and apps as the most vulnerable combination. It will be hard to gather large amount of data from broadcasts from a moving vehicle that are so limited in range of max. 500 metres as the Wifi 802.11 p. broadcasts.

Related to

The second part of the legal definition reads: The way the information will be related. "In general

13 Document ETSI 2013 on vehicle communication Specifications of the Cooperative awareness service

terms, information can be considered to "relate" to an individual when it is about that individual." This raises the question whether the CAM message from a vehicle is about an individual? Will identification in case of a C-ITS broadcast be possible by other means, like sharing the CAM-message data or putting in any other efforts that could be reasonably expected.

Example No. 8[14]: monitoring of taxis' position to optimize service having an impact on drivers.
A system of satellite location is set up by a taxi company allowing this company to determine the position of available taxis in real time. The purpose of the processing is to provide better service and save fuel, by assigning to each client ordering a cab the car that is closest to the client's address. Strictly speaking the data needed for that system is data relating to cars, not about the drivers. The purpose of the processing is not to evaluate the performance of taxi drivers, for instance through the optimization of their itineraries. Yet, the system does allow monitoring the performance of taxi drivers and checking whether they respect speed limits, seek appropriate itineraries, are at the steering wheel or are resting outside, etc. It can therefore have a considerable impact on these individuals, and as such the data may be considered to also relate to natural persons. The processing should be subject to data protection rules.

This is an interesting case because it resembles C-ITS to a high extend because the purpose of the data collection is related to the vehicles and not to the drivers. Yet the data eventually are regarded as personal because the data can tell a lot about the drivers once the controller seeks to connect the vehicle data with the identifiers of the drivers. In this case that was considered likely and reasonably because the company as employer of the taxi drivers had all the identifying data. The case shows however that if such a connection cannot be made within reasonable effort, the vehicle data may not be considered to be personal data because the drivers will not be identifiable.

WP 29 has given three possible indications as to if information is related to a natural person. The first is content; the information contains identification of the subject. The second is purpose; the purpose of the information is to identify the subject. The third is result; identification is a result of the processing of the information. It seems that neither of these relations occur in the processing in order to get real time positioning of the taxis, nor it will occur in C-ITS public road safety applications. The information as such was not to be considered personal data. It only became personal data because the employer could match the data with the personnel files of the company. Will such a matching possibility be available in C-ITS? The CAM-message does not contain a direct identifier. The only possibly identifying element might be the MAC-address, and that doesn't contain identification of the subject, or even the vehicle. Also purpose will not be an identifying element since the purpose of the broadcast of the CAM message, even when including the MAC address, is not identifying any subject. So will identification, for instance by singling out a natural person be the result of the processing of

14 From the opinion nr 2007/4 of the WP 29.

data within C-ITS? To us it seems that the MAC address, even when added to the CAM message, or a set of location and dimensions data will not provide enough data to the processor in order to make it likely and reasonably possible to single out a subject related to a vehicle. However a combination of static vehicle data, like MAC address and dimensions may best be avoided to minimize the risk of the data becoming personal in the course of time.

Identified or identifiable

According to WP 29 in general terms, a natural person can be considered as “identified” when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is “identifiable” when, although the person has not been identified yet, it will be possible to do that at a later stage (that is the meaning of the suffix "-able").

Further clarification is given in the commentary to the Articles of the amended Commission proposal[15], stating that "a person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.)". The terms of this statement clearly indicate that the extent to which certain identifiers are sufficient to achieve identification is dependent on the context of the particular situation.

Directly

Concerning "directly" identified persons, the name of the person is indeed the most common identifier, and, in practice, the notion of “identified person” implies often a reference to the person’s name. But even a name does not always help identifying a person. Within the C-ITS community a name like Johnson may be pretty distinctive, but at a reunion of the Johnson family this name will appear to be a lot less identifying. The question that has to be answered here is whether the data is such that the natural person can be singled out and identified on the basis of the information.

If the identity cannot be revealed by reasonable efforts than the data will not qualify as personal data.

How thin this line between identifying and not identifying is within C-ITS becomes clear when an optical registration of the licence-plate is added. The licence plate number is considered personal data because it can 'easily' be related to the owner of the car. How easy will depend on the way the registration of cars is organized. In some EU countries anyone can get the owner data from the car registration. In other EU countries only authorities and specific stakeholders, like insurance companies, have access to those data. The combination Cam-message, Mac-address and licence plate will single out the vehicle owner in most cases, even be it at vehicle level. But is vehicle level personal enough? Someone else may have been driving the car. The Working Group 4[16] position in its 2015 Report was

15 WP 29 Opinion 4/2007 p. 12

16 WG of the EU platform for C-ITS installed to look into data protection aspects of C-ITS.

yes. It was amongst others based on the WG art. 29 Opinion regarding smart phones. Concerning vehicles the question is whether the bond between the car and its user is just as intimate[17] as the bond between the smart phone and its user. Looking at the specific characteristics of the smart phone, like being held on the body all the time and even left on the nightstand when sleeping it seems a lot more personal than the characteristics of a car. Even more so when the continuous exclusivity of the use of a smart phone is compared with most cars that either are left on the street for the greater part of the day, or are being used by others like colleagues or members of the family.

Indirectly

In its opinion on Personal data WP 29 has elaborated on the issue of indirect identification.

'In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information, combined with other pieces of information (whether the latter is retained by the data controller or not), will allow the individual to be distinguished from others. Without even enquiring about the name and address of the individual it is possible to categorize this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data reflects this fact.

Recital 33 refers to this sort of data as "data which are capable by their nature of infringing fundamental freedoms or privacy".

Recital 26 of the Directive pays particular attention to the term "identifiable" when it reads that "whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." This means that a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable". If, taking into account "all the means likely reasonably to be used by the controller or any other person", that possibility does not exist or is negligible, the person should not be considered as "identifiable", and the information would not be considered as "personal data". The criterion of "all the means likely reasonably to be used either by the controller or by any other person" should in particular take into account all the factors involved[18].

In a recent judgment the EU Court of Law considered a pre judicial question on the scope of the

[17] A smart mobile device is very intimately linked to a specific individual. Most people tend to keep their mobile devices very close to themselves, from their pocket or bag to the night table next to their bed. It seldom happens that a person lends such a device to another person. Most people are aware that their mobile device contains a range of highly intimate information, ranging from e-mail to private pictures, from browsing history to for example a contact list. (WP 29 Opinion 2-2013)

[18] The taxi case was a clear example where the coupling of personnel data to vehicle data was considered to be reasonably likely.

concept of personal data[19]. The case was that websites of the German administration stored the IP addresses of their visitors after the visit was completed for security reasons. The relevant visitor used dynamic IP addresses that could only be linked to his computer by the internet service provider. The question was whether the IP addresses were to be considered personal data. The EU Court considered the following:

"The Court considered that the first question concerns the situation in which it is the online media service provider that registers IP addresses of the users of its website without having the additional data necessary in order to identify those users. The visitor on top used 'dynamic' IP addresses, that is to say provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made, and not 'static' IP addresses, which are invariable and allow continuous identification of the device connected to the network. In that connection, the Court noted, first of all, that it is common ground that a dynamic IP address does not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer. Furthermore the question arose whether a dynamic IP address registered by the service provider may be treated as data relating to an 'identifiable natural person' where the additional data necessary in order to identify the user of a website that the services provider makes accessible to the public are held by that user's internet service provider.

To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person[20].

This means in the consideration of the Court that it is not required that all the information enabling the identification of the data subject must be in the hands of one person.

So the question is under what circumstances the data subject can be identified in this case. The fact that the identifying data is not held by the online media service provider does not exclude the dynamic IP address from being constituting personal data as such. However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject.

In this case the purpose of collecting the IP addresses was the prevention of and the fight against cyber attacks. On the basis of criminal law, the authorities were allowed to get the identifying information from the internet service provider because:"it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored. Therefor a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means

19 Case C-582/14, judgment 19 October 2016

20 Recital 26 Directive (EG) nr 95/46

which enable it to identify the data subject with additional data which the internet service provider has about that person."
What does this mean for the C-ITS use cases and the CAM messages? In this German case eventually the legal means were available to make the dynamic IP addresses identifiable, and thus personal data. One could say the purpose of the registration, public security, provided for the means to identify the subject. This kind of power will not easily be generated in C-ITS. This would imply that any party receiving a Wifi p. signal from a vehicle within the framework of C-ITS, without the means to identify the subject behind the signal, does not receive data that can be regarded as personal data.
In our opinion, it is clearly indicated that unconditionally qualifying CAM messages from cooperative vehicles as personal data is at least questionable, and should be subject for further research.

Transparency and accountability

It is obvious that not qualifying C-ITS data as personal data requires serious guarantees against a change of the status into personal data during the processing. The WP 29 uses the security measures when processing personal data (Article 17 of the Directive) also to guard the status of data being non personal. ' Where identification of the data subject is not included in the purpose of the processing, the technical and organizational measures to prevent identification are essential. In this case, the implementation of those measures will not be the consequence of a legal obligation arising from Article 17 of the Directive (which only applies if the information is personal data in the first place), but rather a condition for the information precisely not to be considered personal data and its processing not to be subject to the Directive.'
This statement confirms that dealing with data on the edge of personal will never be an easy ride, but in all cases will require the care, transparency and accountability that dealing with personal data itself requires, only without the compelling legal obligations.

Conclusion

Balancing the many different interests while managing enough data protection in the current big data information society is not easy. Privacy has never been an absolute right, as public interests as criminal investigations and collecting taxes were always given priority over individuals' right to data protection. The Internet and further promulgation of mobile devices however made the issue of balancing the various interests more problematic and more urgent at the same time. Internet companies collect an enormous amount of personal data for commercial reasons and public authorities collect a considerable amount of data in the name of security and fighting cybercrime and terrorism. It is not easy to maintain the data protection standards these days although it becomes more important to do so every day. However a firm commitment to the data protection cause should not lead to an interpretation of data protection that is too restrictive. In that case innovations that might involve the processing of personal data could be seriously hindered. C-ITS is a good example where these days data protection is drawing a lot of attention, and so it should. This paper is by no means seeks to attenuate the importance of data protection. However data protection should not become an

unavoidable show stopper for C-ITS. In this paper we hope to partly clarify the relation between C-ITS and data protection. We have argued that the CAM message that is sent via the 802.11 p. protocol doesn't necessarily have to be considered personal data. Looking at the technical specifications for C-ITS used for the first series of road safety applications it should be possible to run C-ITS applications without personal data, which would not be in conflict with current EU legislation and jurisprudence. This interpretation must lead to clearly defining at what technical designing point the transition from non-personal data to personal data is perceived. A common effort of all parties involved to determine this transition point would help to create the legal certainty that is necessary for the further development of C-ITS by the industry. Awareness with the industry of the risks of processing personal data will encourage technical choices with a minimum privacy impact. Adopting Privacy by Design as a basic element for designing C-ITS services providing for the required transparency and accountability by the industry on the other hand will help the Data Protection Authorities to give room for innovative developments to be conducted either within the legal framework, or by leaving it outside that framework all together.

In our view the operation of C-ITS does not have to imply the processing of personal data provided that the use of identifying data elements is being avoided. It means that choices should be made on the use of CAMs considering the data protection issues involved. The Data Protection Authorities and the industry and public authorities involved should cooperate in order to find legally sound, workable solutions to enable C-ITS industry to go full speed in the development of the so much wanted and life-saving C-ITS road safety applications, while still respecting the privacy of the C-ITS users.

References

1. Opinion nr 2007/4 of WP 29 on Personal data
2. Opinion nr 6-2013 of WP 29 on Smart phones
3. Report EU platform WG4 2015 Data Protection & Privacy for Cooperative Intelligent Transport Systems (C-ITS) 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 – Dec. 2015
4. ETSI EN 302 637-2 V1.3.0. 2013-8 ITS vehicle comm. Specs. Cooperative awareness service
5. ETSI EN 102 638 V1.1.1. 2009-6 ITS Vehicle comm. Basic set application definition
6. W. van Haaften & T. van Engers (2015) Data Protection And Cooperative Driving.In *Proceedings of the 22nd World ITS Conference* (ITS-2665), Bordeaux.
7. Directive (EG) nr. 95/46 on data Protection, 24 October 1995
8. Privacy en vormen van 'intelligente' mobiliteit, de impact van ict-applicaties door de weg en het spoor Henk Griffioen WRR 2011