Working Conference Data Protection and C-ITS

University of Amsterdam, 21 and 22 March 2016

Leibniz Foundation For Law

UNIVERSITY OF AMSTERDAM

Leading partners in Smart Mobility

DITCM Innovations

Holland.

Table of Contents

Introduction

The report of EU Cooperative-intelligent Transport System Platform Working Group 4 has presented a number of issues and possible remedies. In order to validate the outcome of WG 4 a more in depth scrutiny of the results is being proposed for this Working Conference. Below the issues are presented that will be discussed in the Working conference. This list is by no means exhaustive. During the process of analysing and the interdisciplinary discussions any turn may be taken. Since most issues have both a technical and a juridical aspect, which will influence one another, it is hard to separate technical and juridical issues. Nevertheless, a distinction will be made in technical and juridical issues on the basis of the origin of the item.

The following issues have been identified as in need for further scrutiny:

Technical:

- Telecom developments, Wi-Fi-P, 3G, 4G, 5G: Legal implications? Where are technical developments taking us, and what does it mean for the application of the data protection legal framework?
- Data security, what data is being sent, pseudonymisation: Legal implications? How far should data security go? What is an acceptable balance between data security and costs? How to define data insecurity?
- How do CAM and DENM messages relate to the data protection legal framework?

Juridical:

- What are personal data in the context of C-ITS? How does 'identifiable' match with the current technical solutions? What is the role of vehicle geo-data? Is C-ITS possible without processing personal data?
- What will be the appropriate legal basis for the processing of personal data? What properties play which role while establishing the legal basis? Informed consent seems hard to implement, what are the options?
- How do special legally arrayed public services like e-Call and traffic safety messages relate to the data protection legal framework?

General:

- How to find the balance between legal requirements and technical abilities thus avoiding showstoppers?
- How do we come to compliance to the applicable rules in a way that trust in the C-ITS environment can grow?

Agenda conference

Monday March 21st, 2016

9:30 Registration and reception with coffee/tea

10:00 Plenary Opening Session
- Welcome by Mr Wouter van Haaften
- Introduction 'Data Protection' by Dr. Frederik Zuijderveen Borgesius (UvA)
- Introduction 'Telecom and Developments' by Prof. Dr. Robert Meijer (UvA)
- Introduction 'In-car Technology' by Dr. Ben Rutten (TUE)
- Kick-off conference by Prof. Dr. Tom van Engers (UvA)

11:30 Coffee break, Group Photo

12.00 Start multi-disciplinary working group sessions:
- *Technical service group*
  Reporter: Ben Rutten
  Which services? Which data? Which service providers? What data protection issues arise?
- *Legal group*
  Reporter: Wouter van Haaften
  What data protection framework? What are the key protection elements? Possible showstoppers?

13:00 Lunch

14:00 Multi Disciplinary-groups start with discussing issues for C-ITS and data protection Law. Reporters: pm

15:00 Tea break

15:30 MD-groups work on assigned issues and questions

16.45 Plenary session: Presentation MD-groups outcome of scrutiny of the assigned issues

17.00 Snacks

17.30 Preparing presentations, initial document first draft within the MD-groups on the assigned issues

19.00 End of day 1

Collective dinner

20:00 Welcome drinks

20:30 Conference Dinner

09.30 Plenary session: Presentation Working groups, discussion and identification of gaps
10.40 Coffee break
11.00 MD-groups continued writing sessions on the assigned issues and filling the gaps
13:00 Lunch
14:00 Plenary session - Presentation summary of findings
15.15 Tea break
15.30 Review findings in other MD-groups
16:30 Plenary closing of work conference
17:00 End of day 2, end of the conference

Nb. The number of groups depends on number of conference participants and the available expertise. Also the procedure of the meeting can be adjusted to the number and the expertise of the participants. Each working group will have a chair/reporter, responsible for conserving the group output.

Wi-Fi

As a guest, you have several options for using the wireless network at the UvA.

1. **Eduroam wireless network:** for guest users from other educational institutes. Log in using the account of your own institute;
2. You can log on to the UvA Open Wi-Fi network, which does not require registration or passwords. At the Science Park you can connect to the network '**Amsterdam Science Park**'.

Participants

Wouter van Haaften
Consultant and Researcher, Strategic (Legal) advisor, i-Government,
Road Pricing, Intelligent Transport Systems-Legal.
Senior researcher at University of Amsterdam.
Chair

Frederik Borgesius
Researcher with focus on technology, law and privacy at University of Amsterdam.
Key note speaker.

Robert Meijer
Sr. Strategist at TNO, lecturer applied sensor networks at the University of Amsterdam.
Key note speaker.

Tom van Engers
Programme manager Business Information Systems at UvA.
Head of the Leibniz Center for Law at the University of Amsterdam.
Key note speaker

Ben Rutten
Program Manager Strategic Area Smart Mobility at Technical University Eindhoven.
Key note speakers

Hans Looijen
Engineer with a focus on electronic manufacturing and testing, hardware engineering traffic light controllers, embedded software and GUI for traffic light controllers and project engineering for speed control systems at Siemens.

Martijn van der Veen
Project leader Privacy First Solutions at Privacy First.

Gilles Ampt
Chairman of the DiTCM Smart Mobility Round Table Security.

Simon Hania
Vice President Privacy & Security at TomTom

Tijmen Wisman
Researcher at VU in Amsterdam, with expertise in ICT & Law, Privacy, Data protection & Personal data. Published a paper on the data protection aspects of e-Call.

Angélique Oortmarssen
Consultant Privacy & Security at Privacy Management Partners.

Martina Schollmeyer

Data privacy protection officer at BMW.

Florian Springborn
Daimler.

Henri Kujala
Chief Privacy Officer at HERE Deutschland GmbH.
Lamprini Gyftokosta
Policy advisor for anti-discrimination and data protection at Insurance Europe.

Günter Wildmann
Information Security Analyst at Kapsch.

Anna Zee
President of the Federation of Motorcyclists Associations (FEMA).

Maurice Schellekens
Senior researcher with a focus on Computer Science Law, copyrights, Information Law, Intellectual Property Law, law and informatisation/computerisation and patents at Tilburg University.

Arjan Geluk
Managing Consultant at UL Software & Security.

Jennifer Wennekers
MSc. Information Sciences student at the University of Amsterdam.

Summary of the results of the Working Conference

Introduction

On 21 and 22 March 2016 a Working conference was held at the University of Amsterdam. The conference was an initiative of the University in association with the Dutch Ditcm 'Round table for legal aspects on C-ITS'. From the discussions at that table, conducted research on the issue and the document produced by WP 4 of the EU Platform on C-ITS the picture on the Data Protection aspects of C-ITS is still not clear. However, within the framework of the development and deployment of Cooperative ITS in the Netherlands data protection has been identified as a phenomenon with the potential to become a showstopper if not properly and timely addressed. For instance within the A58-Dutch Shockwave Traffic Jam project participating vehicles are foreseen to send their speed, position and direction continuously along with some 'identification' to a roadside system. This raises the question how to deal data protection issues using this kind of technology in the future?

In order to avoid a too rigid approach strictly based on proven technology and the proven interpretation of current laws, recommendations and jurisprudence the Leibniz Centre for Law at the University of Amsterdam has organized a two day working conference with experts and academics in the field of data protection values, data protection laws, in-car communication technology, telecommunication technology and artificial intelligence.

The goal of the conference was to confront the various disciplines with the challenges in Data Protection and C-ITS that have occurred already and probably find new challenges along the way. The discussions were aimed at bringing about a variety of considerations thus creating an overview of related issues in both technical developments as in legal reasoning. Also an open discussion on technical choices in relation to data protection and vice versa was envisaged. Input for the Conference was, along with two papers on the data protection aspects of the A58 shockwave traffic Jam Project, the publication on the data protection within C-ITS EU platform on C-ITS, in particular in Working Group 4 covering data protection.

The objective of studying the data protections of C-ITS in general is to take away legal, i.c. data protection, obstacles as much as possible and to deal with the remaining issues in such a way that the legal data protection risks are being minimized and at least are being commented on by data protection experts.

In order to come to Privacy by Design practices within the EU the establishment of a dynamic lists of do's and don’ts will be prepared that can be conceptualized both in the technical as in the juridical sense.

Working conference plenary presentations

The conference opened with a number of presentations during the kick off of the conference.

- Data protection Law and background (Dr Frederik Zuijderveen Borgesius, UvA)
- C-ITS technology (Dr Ben Rutten, TUE)
- Telecom developments (Prof. Dr. Robert Meijer)

Working groups

After the kick off the group divided into two sub groups, each with its own theme, respectively 'What is personal data within the C-ITS framework' and 'What should be the legal ground for processing personal data'?

During the sessions in the working groups it became clear that this focus on the themes was not sustainable. Due to the diversity in background, knowledge and interests of the participants

a variety of discussion themes entered the discussion. The report will reflect this variety by not holding on to the original themes but will be corresponded with the issues that were brought up during the discussions.

Issues

Legal grounds

In order to be allowed to process personal data a legal ground is required. In the conference two legal grounds were adopted as potentially applicable in C-ITS: Informed consent and a legitimate interest of the service provider.

- House hold exemption

  The suggestion was made to use the household exemption as an escape route from the processing of personal data altogether. The household exemption however only is applicable to true private household processing of personal data by natural persons.

  Directive 95/46 recital 12 article 3.2

- Note: one entity may have more than one role.

  Another suggestion was that one entity could have more than one role.

  For instance a subject could also be a controller. This doesn't make sense. Why should you be a controller over your own personal data? The definitions in Art 2 of the Directive do not indicate this possibility. It is possible that several players have several roles in relation to a dataset coming out of an OBU. However, in that case the dataset will probably be divided, for instance per purpose that is being pursued.

- What constitutes legitimate interest?

  This is an important question when trying to get away from informed consent as the only legal ground for the processing of (location) data within C-ITS. It covers a wide range of interests. WG29 has already stated in the past that, for instance, e-marketing can be a legitimate interest for the service provider. The only restriction is that it should not jeopardize the fundamental rights of the subject.

  Directive 95/46, recitals 30/45/50/58 articles 7f 15.2 a/b

- Will a law be needed for processing personal data in C-ITS?

  In this stage of C-ITS a law will not really help, because it not yet developed enough. In a later stage however legislation, or at least an opinion of the WG29, could help to reduce uncertainty on the application of data protection law in C-ITS services.

Personal data

Data protection is all about personal data. In the Directive 95/46 the definition of personal data has been given:

"(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

- When vehicle related (location) data enables identification of the driver-owner or owner (data subject), such data is personal data, even if no direct identifying data has been transferred to the service provider. The German data protection Commissioners and the OEM's have concluded that data are at least to be considered personal if the are in any way connected to the Vehicle Identification Number and/or the License plate number.

- Data are no longer personal data if the have been encrypted or aggregated. Eventually in a pure V2V communication with automated vehicles all data coming out of the vehicle should be anonymous. Location data from the car however will always involve the risk of constructing routes per vehicle, thus becoming personal data again. A distinction should be made between location data content, being part of the broadcasted data and the data that can be derived from the broadcasting itself, even if no personal data is being sent. In the latter case the personal data could arise from just collecting location data of a vehicle over a long distance and a long time. It seems that the question if this kind of collection will be considered personal data has not been clearly established yet.

- The cooperative functions in the car, communicating with the environment, will eventually enhance the decision support systems that OEMs will build in their vehicles for the purpose of automated driving. In that situation no personal data need to be involved in car-to-car communication.

- An option to guarantee the privacy of personal data that is encompassed in C-ITS, could be the cooperation with the ABC4Trust project, which receives funding from the 7th Research Framework Program (FP7) of the EU as part of the Trust & Security Program. ABC4Trust addresses the interchangeability and federation of technologies that support privacy-preserving and trustworthy Attribute-based Credentials (ABC). By using Attribute-based Credentials, the owner of the data (for example, a C-ITS vehicle) reveals only the minimal required information to an inquiring application, without revealing its full identity. ABC4Trust strives to define a common and unified architecture for ABC systems, and deploy them in actual production pilots to gain anonymous feedback from communities.

Controller

The role, position and nature of the controller caused a lot of discussion. In this paragraph the elements from the discussion are matched with the legal definition of 'controller' and some elaborations where appropriate. First of all the legal definitions of the players in the data protection Directive should be clear. These are according to Article 2 of Directive 95/46:

"(a) 'personal data' shall mean any information relating to *an identified or identifiable natural person ('data subject'*); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or

Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

"(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct

authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;".

Looking at relations between various actors: controller, processor and subject.

- Who is the controller? From the definition in Art. 2 d) of the Directive it is clear that the controller is the natural or legal person that defines the purpose and the means of the processing of personal data. This legal person can operate on its own, or jointly with others. Does that mean that these others become controllers too? This is possible as long as they jointly define purpose and means of he processing. In that case the WG 29 has stated that they will be individually accountable towards the data subject for the entire controllers responsibility. It is also possible that they are controller regarding only a part of the data set. In that case a combination of several controllers could be possible. However a lack of clarity as to whom is responsible towards the data subject can never be held against the data subject.

- Can de OBU be the controller? Although this will sound familiar in the IT business, from a legal point of view it doesn't make sense. Since the controller is defined as subject to the data protection Law, it can only be a natural or legal person.

- If the Service Provider is selected by an OEM; who is the controller? In this case we have to go back to the purpose and means of the data processing. Are they being established by the OEM or only by the Service provider? And does the OEM actually process data that could be defined as personal? It seems that in most cases where a service provider is involved, the OEM will not be qualified as a controller.

- What is the role of the communication service provider? Usually a telecom service provider is playing this role. The telecom provider will process location data primarily as traffic data, under the e-Directive conditions. When however the telecom provider starts delivering the same services as other service providers also for the telecom provider the same rules apply as for the other C-ITS providers.

- Can the receiving party (recipient) be the controller? Unlikely, in that case it should reveal the data as a controller to itself. Legally this does not make sense. (see also at Legal issues)

- Can the OEM be the controller? That depends on whether the OEM defines the purpose and means of the processing of personal data and if it actually processes personal data, or if it leaves the procession of personal data to a service provider.

- This means that the consent an OEM needs for starting up transmitting to and from the vehicle does not imply the processing of personal data.

- Car to car communication, who is the controller? In this case the first question should be: are personal data being processed. It seems possible to anonymize the car to car data traffic in order to avoid the use of personal data all together.

- Software manufacturer or service provider is the controller? This will very much depend on who is defining the purpose and the means of the data processing and who will actually process personal data?

Open issues, to be investigated

Issues that were brought up but not further discussed during the conference.

During the two conference days many topics related to data protection and C-ITS were briefly discussed in the working groups, but not further elaborated on. In the final hour of the conference a list was composed of issues that were supposed to be scrutinized further. In this paragraph these issues are being recorded.

- First of all the conditions under which the data in the Cooperative Awareness Messages and Decentralized Event Notification Messages should be considered personal data should be further looked into within the framework of the forth coming General Data Protection Regulation. One of the issues related to that question is whether the vehicle and the on board unit can be looked at as separate entities.
- Can the data be sufficiently anonymised or pseudonymised? Do we need identifiers altogether? Or can they be removed without loss of functionality? And how can the aggregation of data lead to anonymity?
- If personal data will be processed then the CAM and DENM design may have to be reconsidered. Also the use of these messages may have to be regulated.
- During the conference it became clear that it is not always easy to find an appropriate purpose for the processing of personal data. This point should be further elaborated on; specifically composing a list of acknowledged purposes at an operational level would be helpful.
- Another issue was the permanent character of the broadcast. This may not have to be the default mode. Activation could take place in situations where other vehicles are at a certain distance.
- When it comes to pseudonymisation, as is foreseen in the ETSI standard, the question arose what the frequency and life time of the change of certificates should be, who would decide on these issues and who will be issuing the certificates. And are there alternatives for using pseudonymised certificates? Or could the PKI be extended to prevent unauthorised entrance of the system?
- It seems that in order to have the system work properly throughout the EU a delegated Act should be established so that the C-ITS system will get a legal basis.
- The question who is the controller in the C-ITS system was not concluded during the conference. As it comes to the position of the Data Protection Authorities the question arose whether all DPAs will take the same view on the non-controllership of car manufacturers as the German DPAs did.
- More practical was the question what happens if an EU car, broadcasting C-ITS messages leaves the EU. Should the broadcast stop?
- Finally it was suggested to prepare a Horizon 2020 proposal with ABC4Trust and multi-brand platooning in real traffic conditions.

Paper 1 - Data Protection and Cooperative Driving

Authors: W. van Haaften, T. van Engers

Introduction

ITS (Intelligent Transport Systems) are drawing a lot off attention these days. Entire conferences are being devoted to it and all over the world projects and programs are running involving authorities, service providers, automotive industry, ICT suppliers and infrastructure managers. The rapid development of automated driving, with the Google car as an important eye-catcher, but also of cooperative systems such as 'platooning' raise all kinds of questions in various legal fields.

For cooperative systems, in which cars will be communicating their data almost permanently to a large number of different parties, data management, and the privacy aspect in particular is ultimately important. In this paper we look into the relation between the preservation of the fundamental right on privacy and the build up of a cooperative driving service. What is the impact of cooperative driving on our privacy? How can we fit the data needs that come with cooperative driving in our current legal framework? How do participants in cooperative driving comply with the legal obligations? Although cooperative driving will not stop at the national border[1], we will restrict the European perspective in this paper to the European legal framework. This framework has established serious harmonisation of data protection within the European Union, thus reducing complication while crossing internal borders.

In this first cooperative driving project in the Netherlands, that went life in summer 2015, cooperative driving is not yet directly linked to the controls of the vehicle, as is the case with 'platooning'[2], but is producing recommendations to the driver in the vehicle in a cooperative way. This means that the data from and to the vehicle will be transferred via fast short range Wi-Fi-p communication. In the project design legal aspects including demands from privacy regulations were gradually taken into consideration. In the developing process it became increasingly clear that these elements should play a role in this early design stage as the complex technology and the supporting (social) networks are being developed right now. When these legal issues would be addressed later they could not only slow down future developments, but the entire enterprise could come with much higher costs or legal issues may even turn out to be a show stopper. Timely recognition of these aspects suits the desire of the joint parties to have a solid basis for the establishment of cooperative

[1] The Corridor project is establishing cooperate driving facilities between Rotterdam and Vienna.

[2] Platooning is in a convoy of vehicles where as the front vehicle is leading. Each vehicle measures distance, speed, and direction end adjusts to the vehicle in front. All vehicles are virtually linked, but can leave the convoy at any time. (...) (Definition ERTICO-Sartre project-2012)

[3] Wetenschappelijke Raad voor het Regeringsbeleid, 2011, Henk Griffioen.

[4] Knotts Supreme Court 2 March 1983

[5] Deventer murdercase 1999

[6] This public resentment can more of a threat to the operation of cooperate driving than the possible fine for not obeying the rules, like the privacy officer of TomTom stated: "Privacy is our licence to

Platooning is in a convoy of vehicles where as the front vehicle is leading. Each vehicle measures distance, speed, and direction end adjusts to the vehicle in front. All vehicles are virtually linked, but can leave the convoy at any time. (...) (Definition ERTICO-Sartre project-2012)

driving, and not run the risk of missing essential conditions regarding the legal requirements in the basic design. Overall the common efforts of both the administration and the market parties involved are aiming at preventing data protection issues that might lead to newspaper headlines, thus ruining the basis for the development of C-ITS and the A58 project altogether.

Why data protection?

Why data protection? When so many issues arise people will tend to ask, can't we do without data protection or at least with a lot less of it? The simple answer is no! Apart from privacy being an undeniable fundamental human right, history shows that in the past decades collecting and processing of data has deeply changed due to the increasing possibilities both in data transfer, data storage, the uptake of meta-data standards and the possibilities of semantic web technology. Searching for data in a library catalogue and collecting data that is geographically spread used to be time consuming activities.

A quick comparison between paper data collections was, and is up till now, not possible. How different that is in the electronic age, in which the collection of shear unlimited amounts of data is being combined with the linking of data collections that at least share a part of their dataset.

In many cases these datasets consists of personal data, relating to an identifiable natural person. Personal data are provided to public authorities at different sorts of occasions. Typically this data delivery is due to legal obligations or data are provided in order to get certain public services. At an even larger scale people provide data to private companies, for instance when buying goods via the internet, in order to win prices within the framework of well oiled marketing campaigns, when gathering air miles, when participating in loyalty programs or for being able to use 'free' apps.

Personal data are everywhere and the protection of these data does not seem of much concern to the average citizen. Only once in a while a news item on the use of personal data does the eyebrows frown. Most of the time this happens when personal data has been collected or used without the consent of the natural person involved. In those cases often the linking of the personal dataset to another dataset has provided information that is being perceived as threatening. Linking of personal data with location data, as will be the case in cooperative driving, can potentially be such a privacy threat.

The sensitivity of data protection in the field of road traffic can be illustrated in a few cases that recently made it to the press, or even to a court of justice, in the Netherlands. The first one was a court case in which the police used permanent Automatic Number Plate Recognition (ANPR) on a highway heading towards the eastern border, that registered every passage. In the data base that was built up the police searched for cars that were possibly involved in criminal activities. The argument of the administration to justify this method was that in fact they also could have put an officer with a paper notebook along the highway, writing down every registration number. They argued that the ANPR was, like the paper notebook, nothing more than a device for technical assistance.

The judge however stated in the verdict that, the shear scale of the ANPR-registration, combined with the opportunity to link the records automated to other data collections and the possibilities of the spreading of the information at nearly no effort or costs, must lead to the conclusion that this way of collecting information was disproportionate.

Another example of the sensitivity of personal location information was the use by the police of aggregated TomTom traffic-information on certain roads. With these data the police could establish where speeding was most frequent and plan their speed controls accordingly. In the latter case the information had been anonymized and could not be led back to any individual driver, so the Dutch Data Protection Commissioner concluded it was no longer personal data. Nevertheless the Commissioner fined TomTom because insufficient information had been given on the purpose for the collection of the data when the informed consent on the use of the personal data was given.

Definitely traceable indeed were the data of lease car users that were sent by their leasing companies to the Dutch national road authority in order to facilitate a survey of this authority amongst these car users. In this case the licence plate numbers and the owners, the leasing companies, were provided by the car registration authority to the road authority, with the explicit restriction not to pass them on.

By asking the leasing companies, despite this restriction, for the names and addresses of the car users an entirely new link between licence plate numbers and car users was created, without the required legal basis.

These examples show that one should not think lightly on personal data access and usage.

The consequences of violating legal requirements can be serious: ending up in court cases that result in a prohibition to use the data for the intended purposes, damaging the reputation of the organization(s) involved and having to compensate parties for damage. From these examples we can learn that serious data protection risks can be likewise involved in road traffic assessment schemes.

Notions of privacy in relation to ITS

Taking into account the EU legal framework the Dutch Scientific Council for Government Policy (WRR)[3] has issued a study on the subject of data protection in ITS in 2011: 'Privacy and forms of intelligent transport'. This report decidedly points out the role of location data as a dimension of privacy, in enhancing our traceability. The smart phone, the public transport smart card, but also location-based services like cooperative driving are leading to a massive amount of digital traces. How does the user keep control over his or her personal data? One of the ways to live up to this demand for control is in terms of selective disclosure. As the study report stated 'Even in our most intimate relations the notion applies that the human interaction is as much characterized by 'reserving' as by 'sharing' information. This means that control over the way in which, as well as to which extend we show ourselves is an important asset'.

Which role does location play within the concept of privacy? In 1983 a judge in the USA, while comparing a pursuing police officer with a transmitting tracking device mounted to a car, simply decided that privacy on public roads does not exist[4]. In other words: if you want privacy, don't go on public roads. This is not the legal situation in the EU anno 2015.

[3] Wetenschappelijke Raad voor het Regeringsbeleid, 2011, Henk Griffioen.
[4] Knotts Supreme Court 2 March 1983

The available technologies and applications combined with their commercial and administrative popularity have propelled the thinking about location-based privacy. We have become conscious of the fact that digital data registration is by no means trivial. In a famous Dutch murder case[5] the evidence consisted largely of the tracing of the mobile phone of the alleged killer, which afterwards appeared to be so inaccurate that the location he claimed to have been at the time of the murder, on the high way many miles away from the crime scene, eventually could have been within the margins of the survey.

It seems sensible to be aware of the on going development of traceability while designing a cooperate driving service, since a lot of information from the car will be necessary to reach the collective goal: better coordinated use of the road. To enable real time in-car speed recommendations the vehicles concerned must be sending their data with a high frequency. The inventory of the possibilities of new technologies could lead to the question if the current data protection rules are sufficient, to wide or to tight?

Personal data exposure

To keep a grip on 'the way one exposes him- or her self' amongst all these new technologies, a combination of factors that facilitates the selective disclosure is involved. In the WRR report these factors are being inventoried and explained. The factors are: technical reliability, sustainability and reusability of the data, the possibility of secondary use and above all the transparency of and the accountability in the processing of these data.

First of all the technological reliability of the systems generating and storing personal data is of utmost interest, regarding the sensitivity of the data. With flawed technology it is impossible to maintain the subtle balance between privacy of the user on the one hand and the interest of commercial and administrative stakeholders on the other hand. After all flaws in the registration of personal data can appear to be seriously harmful when inaccurate data are being used at a later stage. For that reason, high quality standards must be applied to technical solutions.

The desired practical obscurity - being actually invisible in public space - that was mentioned is being challenged by the sustainability of the data and the consequent re usability. The visibility of the car driver will be stretched from one single moment on the road to a virtual recording with longstanding consequences by storing the data of a vehicle and of its location and using it at a later stage. Even if the storage periods will be kept limited, people will become a lot more visible than without such data storage.

Nearly all parties involved, public and private, are very specific on the benefits of the collection of car location data. Within cooperative driving the necessity of the collection of data is self-evident, without location data no cooperative driving service. This collective goal could be an important legitimacy for processing personal data on the one hand, and for limiting the amount of data being collected on the other hand. This limitation is important because private parties also see commercial perspectives like value added services and targeted advertising.

[5] Deventer murdercase 1999

As long as this practice is regulated, the data set has been restricted and the data subject has given his or her explicit permission this will be legally correct. But the service providers must be aware of the fact that structural re-use can increase the risk of illegitimate use. Secondary use of the data if they have been made anonymous may seem less sensitive at a glance, but in certain cases they can be combined with other anonymous data and thus lead to results that may well be identifiable.

Transparency and accountability

To be able to protect the legitimacy on the one hand and to fulfil all the demands and to use the possibilities when it comes to re-use of location based personal data on the other hand transparency is vital. This transparency is required both at policy level and at the level of the relationship between the individual user and his service provider. Transparency will create trust and confidence with the users in the manageability and the actual management of the system and thus in the protection of their privacy. A lack of transparency turns data protection into an illusion and is there for not acceptable.

Closely related to the required transparency is the accountability. Like transparency also accountability is required on both policy and operational levels in order to determine whether a controller, responsible for the processing of location bound personal data, is actually able to comply with the legal provisions with regard to the processing of these data. To the outside world the correct application of the restricted data sets, the retention periods and authorizations are not observable and thus it is important to address this topic by (independent) monitoring.

Conditions for data protection

“Location Based Privacy is a complex overlapping of roles between public and private, reliability and profitability, technological and administrative legal solutions", is one of the conclusions in the WRR report. The report additionally indicates some notions that illustrate the tension that can arise between the individual interest and the public interest: the interest of an individual to be invisible, and especially to be no longer visible than necessary, and the general, collective interest to, in some cases, dispose of the privacy sensitive location data.

It should be remembered that when digital tracks are more numerous it is necessary to pay more attention to the access to that information: what data should be available to whom? When it comes to location-based privacy perhaps a change in thinking is needed because in cooperative driving the amount of floating car data will increase rapidly. The traceability of persons using their smartphone is already substantial. It is an illusion to think that the large amount of data that is available can be managed easily. Limitation of the amount of data involved when driving cooperatively could be helpful in this respect.

A second reason for the change in thinking is that the current ‘notion of control over self revelation’ somewhat assumes that the individual himself is primarily responsible for his or her digital whereabouts'. This could be true for users with an over average knowledge and interest in ICT, however in the current 'branched information universe' it is not possible to leave the data-protection of civilians entirely to their own knowledge and willingness to take action.

One could say that although informed consent is necessary to be able to process the personal data legally, it should not be the only criteria in order to protect individual participants from abuse of their data.

Finally, the shift in thinking is needed to win back some of the lost practical obscurity again.

Being 'invisible' when walking in the street instead of constantly being recorded by the cameras of public and private security systems.

As a result of the technical and social development the notion of practical obscurity has degenerated from a natural condition to a principle worthy of emulation. Therefore, it is time to facilitate the opportunity to 'use the available data sparingly, carefully and legitimately" and to eventually guarantee this both institutionally and technologically. Only in this way the right to the protection of privacy can be implemented adequately in the future.

Legal Framework

When it comes to the institutional guarantee on data protection legislation will be indispensable.

The basis for the data protection and its legislation lie in Article 8 of the European Convention on Human Rights establishing the fundamental right to privacy. Being a fundamental right means that it touches the very heart of our human existence and that violation of the privacy right will easily lead to public resentment[6]. The notions of Article 8 have been translated into European law in the Data Protection Directives 95/46/EC of the European Parliament and the Council and several others of which Directive 2002/58/EC is the most relevant within the cooperate driving framework. In the first the definition of personal information has been given as 'information relating to an identified or identifiable person'. In the Directive 2002/58/EC[7] the privacy provisions for the telecom sector have been established. Within the framework of this Directive cooperate driving services qualify as value added services[8].

Three entities play an important role when processing personal data: The subject, the person whose personal data are being processed, the controller, the entity that is responsible for the processing, and the processor, the entity processing the data on behalf but not under the authority of the controller. In article 9 of the latter Directive privacy provisions have been established for the use of location data other than traffic data, like in the cooperative driving service. These provisions are a *lex specialis* to the general legal provisions of Directive 95/46/EC (art 7 sub a.).

In that respect Directive 2002/58/EC specifies the legitimate ground for processing location data other than traffic data as by means of an unambiguously given informed consent. The location related personal data are to be considered as sensitive data[9] because individual movements can be derived from these data.

These movements can provide a pattern, which could reveal specific sensitive personal information.

Example: By following a particular vehicle at certain attendance, for example to a hospital, church or mosque, information could be derived with respect to the health condition or the religion of the relevant vehicle holder. That risk means that the location data in the event of a basis for in-car services must be regarded as sensitive.

[6] This public resentment can more of a threat to the operation of cooperate driving than the possible fine for not obeying the rules, like the privacy officer of TomTom stated:' Privacy is our licence to operate'.

[7] Amended by Directive 2009/136/EC

[8] Art 2 sub g of Directive 2002/58/EC

[9] WP29 185, Opinion 13/2011 of the European Data Protection commissioners on Geo location services on smart mobile devices, 16 May 2011.

By qualifying location related personal data as sensitive the EU Data Protection Commissioners have confirmed[10] that the most obvious way to be allowed to process the data is with an unambiguous and freely given informed consent of the subject. The burden of proof for this consent lies with the controller, who would do well to keep the confirmation of the user as evidence. The subject may withdraw his consent at any time, although not retroactively. Of interest is that the customer can be reasonably expected to understand the meaning of his consent, in other words, he is aware of the explicit and implicit impact of his consent.

Example: That the consent must be given freely can be problematic in an employer- employee relationship. Recently the Court in Vienna has forbidden Coca Cola to equip its service cars with on-board units that showed the route of these cars. The judge decided that following the staff during service required an unambiguously informed consent. The employee's consent was given within their hierarchic relationship with the employer and thus was not freely given in a way that it could be deemed to be within the law. The case had been brought to the court by Coca Colas employees' council.

A key measure in the processing of personal data is the purpose for which the data may be processed. This purpose must be specified, explicit and justified[11]. Processing of data within the framework of cooperative driving can be regarded as a legitimate aim. If a service provider wants to use the data for other value-added services, it should be ensured that this is not incompatible with the purpose for which the data were obtained in the first place. This means that there will need to be a relationship between the original purpose and the intended purpose of the new processing. So called 'function creep' is on the prowl here. Also, the nature of the data plays a role in this context. The more sensitive the information, the sooner the processing will be incompatible with the original purpose. Given the sensitivity of location information in the case of cooperative driving one should be very cautious.

The controller has an obligation to provide information to the subject. Not only the subject must be well informed about the purpose of the processing, also the identity of the controller must be clear. Regarding the obligation to provide information two situations can be distinguished, one where the data come directly from the subject[12], and one where the data are collected in a different way[13]. In these articles, the 'principle of transparency' is being shaped. This principle means that the controller concerned should make clear which data are being processed, and for what purpose. In the case of the cooperative driving service the data will in the first instance come from the OBU or smartphone in the vehicle of the subject. But other data sources can also play a role in the cooperative driving system. When personal data has been received from other sources, the subject should be informed afterwards.

When it comes to the quality of the data the Directive[14] has put forward a detailed interpretation of the concepts properly and carefully. For example, the collection of personal data must not be excessive, which means that no more data should be collected than necessary for the legitimate aim. Furthermore the data must be correct. In this respect one should distinguish two forms of

[10] WP29 185 Opinion 13/2011 on geolocation services on smart mobile devices, 16 May 2011.
[11] Art. 6 Directive 95/76/EC
[12] Art. 10 Directive 95/76/EC
[13] Art.11 Directive 95/76/EC
[14] Art. 6 Directive 95/76/EC

correctness: a formal correctness and a material correctness. The first is when there is data integrity without input errors (eg. Is the entered address an existing address?). The second is when the information in the database is factually correct (eg. does the person live at the entered address?). To protect the privacy of the subject optimally the controller should provide confidentiality by all who are engaged in the processing of the data in any way, or otherwise might have access to the data.[15] The controller must ensure that confidentiality is respected. This has implications for the organizational and technical infrastructure of data processing systems. Any person responsible for the whole or a part of the automated processing of personal data must report this processing to the monitoring authority[16].

In the case of the cooperative driving this report will be required.

At this moment a new data protection regulation is in a preparatory phase, expected to be adopted by the end of 2015 and to enter into force in 2018. The data protection system will not be changed that much, but for C-ITS two elements are important. Firstly it will be a regulation, which means it will be directly enforceable law in the Member States.

This will reduce the differences between Member States that exist now due to the fact that the current Directives have to be implemented in national law. In that process national elements are bound to influence the final national law text. For an internationally operating system as cooperative driving that definitely is a plus. The other thing is that the sanctions on non-compliance will be much more severe than in the national schemes. This also will help making data protection a serious issue when designing cooperative driving.

The Shockwave Traffic Jam A58 Project

Shockwave Traffic Jams are traffic jams not due to lack of road capacity, but the result of driver behaviour on busy roads. Within the Shockwave Traffic Jam A58 Project (A58 project), that aims to decrease this type of congestion on the A58 in the south of the Netherlands, for that purpose a cooperative driving service has been developed. At local level 'vehicle to roadside' communication is being shared in order to bring information, traffic management and traffic safety services together into the vehicle. Within the project various companies have been brought together in a pre-competitive setting in order to realize this cooperative system. Within this completely new cooperation, apart from paying attention to the administrative, technical, organizational and commercial aspects, also the legal requirements including data access and use and privacy aspects of cooperative driving have been addressed.

The overall process is consequently built up out of a chain of processes involving different parties.

The chain starts with acquiring on-going traffic data from the vehicle. These data, containing location and direction of the vehicle, are then being transferred via the roadside equipment to the data-collection service provider, which will enrich the data with other traffic data that is available regarding the same section of the highway. This aggregated data is the input for the production of the recommendation by again another service provider. That recommendation will be sent via the roadside service provider to the driver within seconds. The system therefor requires technical components such as an on-board-unit (or smartphone) in the car and a telecom platform.

This chain can be depicted like this:

[15] Art. 16 and 17 Directive 95/76/EC
[16] Art. 18 Directive 95/76/EC

Vehicle (vehicle) Vehicle-> road-side SP -> data-collection SP -> data-delivery SP -> recommending SP -> road-side SP -> vehicle Vehicle (vehicle)

Responding to this recommendation the driver can adjust his speed and his positioning relating to the other vehicles on the same section of the high way, with the purpose of preventing congestion to occur or to decrease an already emerging congestion. If the other drivers on the same road act in the same way, the collective speed will be adjusted so that (shockwave) congestion can be prevented.

Since the data set from the vehicle, however small[17], will contain sensitive personal information the protection of data in the entire data chain, including both data transfer and data processing, should be guaranteed. The service provider that is acting as the controller gives this warranty to the subject, being the driver and/or owner of the vehicle. The other service providers in the process could perform as processors, in the context of the Directive. The controller has the responsibility to ensure that the right recommendation, based on the information provided, is being presented in the car and that data is protected against unintended or illegitimate use. How can these legal requirements be established within the A58 project? A few observations from the project regarding data protection may illustrate the hurdles that have to be overcome.

Developing a data policy

When the project kicked off in June 2014 most of the basic services in it self had already been developed. The emphasis in the project was the architecture and the interfaces between the various service parts and parties. Data protection in that phase was looked at from a technical perspective,

as data security. So when the legal issue had to be addressed it was appointed to the Security working group. Within that group the technical approach was confronted with the legal obligations. One of the challenges for the legal advocates in a highly technical dominated environment was to convince the engineers that privacy requires security, but that security on the other hand does not imply privacy. Eventually state of the art technology will have to be used in order to fulfil the requirements of privacy by design and privacy by default.

As far as external data protection was concerned the legal input enhanced the privacy awareness and technical adjustments were made to serve external data protection. To secure the data traffic from the car to the roadside and vice versa technical solutions as pseudonymisation (regularly changing the identifying keys) and PKI[18] were set up along with a joint application and road side service providers. The PKI, still lacking a Long Term Certification Authority, is handling certificates and pseudo-certificates available for changing during the ride, thus hampering the possibilities to follow a specific vehicle. With this PKI also the data security, necessary for data protection can be tested. One of the roadside service providers has taken up the role of Certification Authority for the duration of the A58 project.

Another issue however was the internal data protection. Since many service providers are involved in the A58 project service, achieving adequate data protection in the whole chain is a challenge.

[17] The minimum personal dataset will consist of, e-mail address, password, MAC-address of the OBU or smartphone.

[18] Public Key Infrastructure based on certificated issues by an independent (trusted) Long Term Certification Authority.

Also here privacy by design makes sense. First of all to create the awareness necessary for an adequate design of the data protection within the several organisations involved. Secondly to build the information chain in a way that data protection will be guaranteed throughout the chain,

thus preventing privacy leaks from occurring. In the back office for instance it will be difficult for a controller to gain control over the personal data processors within the chain. Looking at the way the consortia have been shaped it even is hard to establish which of the parties involved has the role of controller in the first place. This problem particularly has come up since the consortium has no legal personality, as is the case in the A58 project. This raises the question which company should be appointed as the controller. And if none of the companies is being appointed who will be the controller by default? Most obvious would be to choose the company having the actual relation with the user. However when using a smartphone app with a consortium service logo that trace could well end at the provider of the app.

Looking at the heart of the service the provider of the in car recommendation is more likely to qualify as the controller. But even if one of the companies could be 'framed' as being the controller it will not be easy for that company to fulfil that role adequately throughout the entire chain of information. The fact that the service providers, in addition to their participation in the system, in adjacent areas also can be competitors makes a full disclosure regarding their handling of data within their business operation difficult. Moreover the cooperating companies are very different in size and in organisational maturity. Multi national corporations here cooperate with medium and even small enterprises. This fact makes it hard to develop one standard for data protection within the consortium. A standard that is not 'safe' enough for a multi national company can already be a showstopper for a small company that has to comply with it. Also the orientation of a company is very important. Is the company technically oriented or does it orientate on the customer? Also these differences will influence the point of view on customer privacy. It is clear that data protection within a consortium will in many cases not be easy to organise, and it will certainly have an effect on the business case in terms of costs. In fact the loosely coupled relation between the service providers in the information chain could appear to be a thread when it comes to data protection.

Nevertheless, the risk of the processing of sensitive personal data is evident and the discussion about who will be responsible within the consortium should be conducted. Moreover the position of the controller in cooperative driving will have to be looked into in more detail. Within that discussion the costs involved in the protection of privacy must also be included. Furthermore possible choices will still have to be checked against the legally required quality of the data protection. All these considerations will have to be put together by the consortium members in an A58 project service data protection policy. In this process also a managing controller could be appointed. He will have to be enabled to take the responsibility for the realization of the organizational and technical measures for the legal protection of the data within the consortium. The (managing) controller has the task of bringing all relevant factors together into a coherent data protection policy document.

Monitoring and enforcement of the implementation of the policy through audits should be part of the data protection process.

The audits, conducted by an independent third party could also take away the objections of the consortium members trying to protect their internal business confidentialities from exposure to possible competitors.

Within this realm the big question obviously is, do the service providers in the A58 project comply with the legal obligations? Do they take privacy into account when designing their apps and do they inform the user before he or she will give consent? Although for the time being none of

these questions can be answered with a straight yes, the privacy awareness has been growing rapidly in the preparation phase. But from a data protection perspective still a lot has to be done before the apps will fully comply with data protection law. In the project a lot of elements bringing the data from and to the vehicle are still in an experimental phase. This should not be a problem as long as the early adopters joining the service are aware of these imperfections. This requires transparency while managing the expectations of the users.

Role of the (managing) controller

In order to guarantee the quality of the process the (managing) controller will have to be able to take suitable action both at technical and organizational level. These two elements should always be consistently used in relation to the data that has to be protected. The use of pseudonymisation and PKI in the A58 Shockwave project is an example of the special protective measures required. The controller shall take appropriate measures after analysing the need for data protection. In addition, he has to take into account three weighting factors:

- State of the art,
- Cost of the measures,
- Risks, arising from the processing and the nature of the data.

When it comes to applying technology, the legislation demands state-of-the-art technology. The first step is to determine what that state-of-the-art technology is. Next step is to replace out dated technology that is still in use. All this means that the technical assessment in the light of technical developments should be made periodically. The controller must be alert to sudden changes in circumstances, such as the successful performance of hackers or updates by his technology suppliers responding to an increased security risk.

Regarding the financial considerations a costs and benefits analysis will be necessary. The costs must be proportionate to the importance of the object that is to be secured, i.e. the system in which personal data is being processed. These costs cannot be seen separately from the third element: the perceived risks.

Costs should be considered on the basis of the technology used and the nature of the data. Given the established sensitivity of the personal data within the A58 project services and the nature of the processing system - communication between vehicles and between roadside and vehicle-, there is a high risk and thus a substantial level of security will be required. This may lead to corresponding security costs.

Privacy Ensuring Technology

The A58 project so far has been revealing a number of issues that have to be addressed in a cooperative driving environment. At this moment most of the solutions are provisional, like the PKI infrastructure, or organizational, like appointing a managing controller and organize data protection within the companies involved. After the project phase and surely when it will come to true cooperative driving, more advanced technical solutions will have to be implemented. In this paragraph a brief outline of such an environment is presented.

Cooperative driving requires an infrastructure that allows the participants in cooperative driving to dynamically create the required networks. Networks typically are constructed on the flight, or

better on the ride, allowing partners in different roles to exchange the required data (both V2R and V2V). The fact that we have to deal with many different parties, in different roles and possibly different jurisdictions, combined with the fact that we deal with privacy sensitive data, makes it essential that we implement a solid technological solution that will safeguard the user's privacy.

This technological solution should make it impossible to trace data back to the individual drivers or car owners except in cases that an explicit informed consent has been given.

The major elements of the technological solution are encryption of the identification codes that enable connecting vehicles, time and locations to individuals. Only the controller should be able to connect the vehicle to the individual, for the purpose of charging. The controller will connect the vehicle identification code to a generated temporal Id that will be used during a limited time interval. The generation protocol should be complex enough to avoid possible reconstruction of the original vehicle Id. The limited time interval is to block the possibility of tracing vehicles during an entire trip. The combination of temporal Ids with short Id persistence intervals will prevent the use of big-data analytics that could be used to construct patterns that could be traced back to individuals and consequently would cause privacy infringements.

Strict separation between personal information and other data during the processing is an essential element of the secure distributed data space that only addresses those data to the processor that need to be part of the process at a specific moment. This technology will protect data against unauthorized processing throughout the chain.

The controller, that should be able to connect a vehicle Id with some individual, being either the driver, or the owner or both, will, besides the data protection that is realised by the mechanisms described above, also take the usual data-management measures, such as access security, technical shielding and limiting the number of people with access to personal data, both within its own organisation as within the organisation of its consortium partners. By taking these technical measures the level of security can be better guaranteed by the controller and the access security is less dependent on the proper functioning and implementation of security measures at the staff level in the organization.

An infrastructure as described can of course not fully protect against privacy infringements, for example if the controller's systems were hacked, or by staff members misusing access rights, but if they occur the potential breach can be only at one party and one would know were to start investigating.

What parties in the network are allowed to do with the data elements should be supported by a rule-based privacy management system that implements the privacy policies and facilitate privacy audits. This automated enforcement of the privacy policy is also an application of Privacy Ensuring Technologies, next to the encryption and Id- management mechanisms described before.

The introduction of privacy audits can be set by the controller or by a Data Protection Commissioner in order to control the level of privacy protection in the cooperative driving chain.

In this way Privacy Ensuring Technologies, become an instrument for the responsible controller in the case of cooperative driving.

Conclusions

Since the project is still running and both technology and organisation have not yet found their final form the conclusions that can be drawn are preliminary. It will be interesting to follow the developments and to keep on bringing legal awareness into the project. Cooperative driving involves processing a serious amount of sensitive personal data, which will require a freely given

unambiguous informed consent. Furthermore all other legal obligations must be fulfilled, like reducing the amount of data, limit the storage time, state of the art security etc.

By now it is clear that awareness of the importance and legal framework of data protection helps the participants to grow towards compliance. The necessity to keep intervening with the legal aspects lies in the fact that technical projects tend to choose a technical approach towards data protection for instance by putting an emphasis on security. Besides that data protection does not come for free.

It could drive costs for the service providers in the consortia.

These consortia, being loosely coupled and without legal personality, increase the complexity in the back office and are problematic from a legal perspective. It complicates making choices on the appointment and the position of the controller. Who will play this role? Will the consortium as a whole act as the controller or will the partners appoint one of them to be responsible for the data protection within the consortium? In all cases it is clear that a controller must be appointed, and that an internal procedure should be set up, maintained and externally audited to be, and stay, transparent and accountable in compliance with the data protection laws.

After the A58 project phase once again the question will be raise as to how participants in cooperative driving will comply with the legal obligations? For one a truly independent Long Term Certificate Authority will have to be put in place to complete the external security environment. The internal data protection, along with all legal requirements will best be served by seriously implementing privacy by default, both technically and in awareness, and by rule based privacy ensuring technology.

Literature

Environmental, safety, legal and societal implications of autonomous driving systems Alexander Robertsson, Anders Eugensson, et.al. 2013

Online tracking: Questioning the power of informed consent Eijk, N. van, Helberger, et. al. Paper September, 2011

Wet bescherming persoonsgegevens en ICT Mw. Mr. S. M. Huydecoper, Monografieën Recht en Informatietechnologie, 2006.

Kroniek Technologie en recht Remy Chavannes en Niels van der Laan, NJB 12-10-2012

Privacy en vormen van 'intelligente' mobiliteit, de impact van ict-applicaties door de weg en het spoor Henk Griffioen WRR 2011

Verkeersgegevens ; Een juridische en technische inventarisatie L. F. Asscher en A.H. Ekker (red.) Instituut voor Informatierecht 2003

ITS Action Plan - Action 5.2 Final Report of the Study regarding liability aspects of ITS applications and services, Berlin, 07.12.2012

Beter Benutten van Intelligente Mobiliteit

Programma Beter Benutten 2013

Much ado about data ownership, Barbara J. Evans, Harvard Journal of Law & Technology, Volume 25, Number 1 Fall 2011

Van wie is het dossier? Rechten en plichten rondom patiëntgegevens. Anton Ekker (Nictiz), 29 oktober 2010

Privacy regulations can not be hard coded. Koops en Leenes july 2013

Privacy in geding: Expliciteren, wegen en beperken van belangen Corien Prins, 2013

Eindadvies Strategisch Beraad Verkeersinformatie en Verkeersmanagement Oktober 2011

EU-Commission, Opinion 13/2011 on Geolocation services on smart mobile devices Adopted on 16 May 2011

Advies Besluit meldingsformaliteiten en gegevensverwerking scheepvaart CBP(Dutch data protection Commissioner) 24 januari 2012

CPB (Dutch data protection Commissioner) Policy Letter | 2014/04 Michiel Bijlsma et al.

Rapport van bevindingen: Ambtshalve onderzoek CBP(Dutch data protection Commissioner) naar de verwerking van geolocatiegegevens door TomTom N.V., Openbare versie 20 december 2011

Agencia Española de Protección de Datos, Mario Costeja González Hof van Justitie van de Europese Unie, Luxemb., 13 mei 2014, Arrest in zaak C-131/12

EU-Commission - Right to be forgotten ruling 2014 C131-12 Documents and interviews within the A58 project.

Paper 2 - Data Protection and C-ITS - A Use Case - Concept

Authors: W. van Haaften, T. van Engers, J. Wennekers

Abstract

In 2014 a Cooperative Intelligent Transport Systems (C-ITS) project started in the Netherlands, on the A58 motorway. The project involved an in-car speed recommendation service in order to repulse traffic jams. The project now has become operational in the autumn of 2015. In this paper we will look closer at the legal implications of the project, in particular the data protection issues involved. The data protection issue has become more visible during the building and implementation processes within the project. We will address the data protection issues by looking at the various parts and interfaces within the system and by classifying data streams from a data protection perspective.

More over we will spark the development of an evaluative framework with which future developments in C-ITS can be dealt with. To this end the A58 Shockwave Traffic Jam System will be mapped on current data protection legislation.

Key words: Intelligent Transport Systems, cooperative driving, automated driving, design options, data protection, (explicit) informed consent, compliance, conformance of IT-systems, privacy, distributed services.

Introduction

Cooperative Intelligent Transport Systems (C-ITS) are more and more considered to be necessary in combination with self-driving cars. While the self-driving car gets most of the attention of the public, experts in the automotive industry have put their cards on developing a cooperative system. Self-driving cars will become part of such cooperative system as well. Communicating with their environment, other cars and roadside stations, on a permanent basis they will be able to reduce the safe braking distance required more than by just relying on their own sensors. These smaller braking distances will lead to more available road capacity than will be viable with stand-alone automated vehicles. In the current state of C-ITS, with services delivered to the driver, and not directly to the car itself a variety of techniques can be used to bring the message to the vehicle, like broadcasting for general messages or cellular or Wi-Fi-p if the message is aimed at a specific driver. Also various types of messages can be used, mostly specific 'tailor made' advice messages to the driver from a specific service provider. In the latest version ETSI standard messages are being used. *Cooperative Awareness Messages* (CAMs) provide information of presence, position of the vehicle as well as the basic status of communicating C-ITS stations to neighbouring C-ITS stations within a 500-meter range. Also *Decentralized Environmental Notification Messages* (DENMs) are used which are triggered by a cooperative Road Hazard Warning use case or function to provide information about a specific driving related event or a traffic event to other C-ITS stations. Besides connectivity and standardization issues, all this communication from and to the vehicle, and its user, raises questions about data protection. How can 'personal' data be protected and how should personal data be qualified within the C-ITS context in the first place, and how exactly do personal data run through the cooperative system?

After addressing privacy issues relating to ITS and the A58 Shockwave traffic jam project last year[19] we now will take a step further by looking into the nature of the data streams involved. Do

[19] ITS nr 2665-2015 van Haaften, van Engers Data protection and cooperative driving.

they contain personal data, and if so how to deal with that? Is it possible to avoid the use of personal data in a cooperative system altogether? In order to get to the answers, we will take a look at all the interfaces in one of the C-ITS projects currently run in the Netherlands, the A58 project, in order to find answers to these questions. Before diving into the data streams and interfaces the relevant legal notions on personal data protection will be scrutinized. When is data coming from a vehicle personal data and when isn't it? In legal terms: can a person be identified or is a person identifiable by the data involved?

And if so, what will be the legal ground for processing the personal data when the data used by cooperative systems are to be considered personal data, at least in certain cases? Also the position of the controller, as being responsible for the processing of personal data, will have to be looked at in that case. A crucial issue when processing personal data is data security. Without data security there can be no serious data protection. This means that data security within the system will play an important role. But what data should be protected to what extend and at what efforts? And how will be assured that all stakeholders will comply with the legal provisions that will be applicable to cooperative driving? Next to these legal provisions and the data streams within the A58 project this paper also is an attempt to provide new perspectives that can be scrutinized while preparing for the implementation of C-ITS services.

The Shockwave Traffic Jam A58 Project

The A58 project provides drivers on the A58 motorway with speed advice in order to get a more regular traffic flow and thus to avoid traffic jams due to driver behaviour on busy roads. The A58 project comprises a chain of processes involving different parties. The functional decomposition (fig 1.) shows the project environment and the players involved. The A58 project is not the only project running with cooperative technology. Also the Corridor project between Rotterdam and Vienna uses similar data and transmission technology. However, at this moment the A58 project seems to be in a phase where most technical choices are stabile and the data sets as well as the interfaces have been defined and are actually being used.

The business model for the SP's lies in the supply of a speed recommendation to the customer on the A58. Along with this information other location bound information - like special offers by roadside filling stations or other shops in the neighborhood - can be presented to the driver. Both the user and the suppliers of special offers and information are potential customers for the SP. For this service a minimum of information from the user will be required, depending on the business model of the SP. In one of the models, for instance, only the companies that offered products to the drivers on the A58 are paying the SP. In that case the users, whom were given an on board unit could remain close to anonymous.

Only the fact that 'someone' is driving on the A58 is relevant at that particular moment, both for the speed recommendation as for the presentation of the special offers from the sponsoring companies.

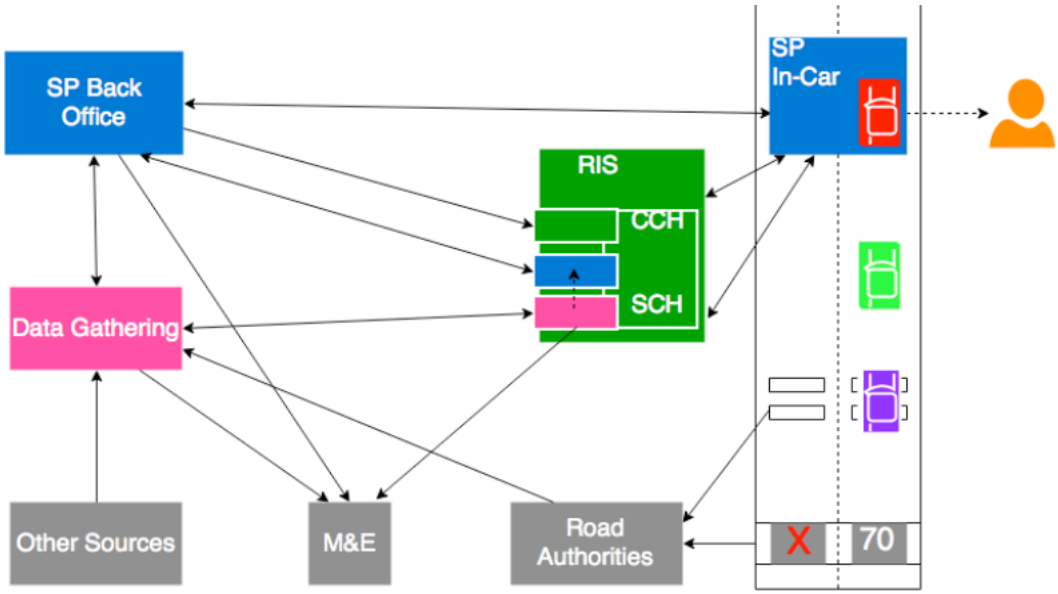

Figure 1 Functional decomposition of A58 project (CCH=Connected Channel, SCH=Service Chanel)

The SP's in the A58 project collect their data by acquiring on-going traffic data from the user's vehicle. This information is enriched with data from other service providers by the SP or by running the data from the vehicle through the data providers' system. Eventually the SP will use all data available for the relevant section of the highway for the production of the recommendation. That recommendation will be sent via the roadside service provider to the driver within seconds. The system therefor requires technical components such as an on-board-unit (or smartphone) in the car and a telecom platform. Looking at the architecture of the A58 project the question is what data the interfaces will be processing and what personal data will be amongst these data.

Multiple perspectives

Cooperative driving itself and combined with forms of autonomous driving already confronts us with many complex legal issues even in the current embryonic stage. One of the objectives of our research is to create an evaluative framework that will facilitate the development of the legal aspects of cooperative driving along with its development. Such a framework will be helpful when assessing developments in the current stage of cooperative driving, but will become absolutely vital when cooperative driving will be combined with automated driving in which case, in our view, additional legislation will be inevitable. The evaluative framework should anticipate on this future legislation in order to allow for a gradual development of cooperative driving. It is obvious that this development will involve several legal fields. New ways of dealing with the current legal concepts will influence the field of data protection, of private law, but also regulations on the vehicle requirements en vehicle user requirements.

The role of the owner of the vehicle, with all the rights and duties attached will change, and also the role of the driver and other stakeholders will change, as well as their role in the production and consumption of cooperative services. At the same time substantial parts of the functionality of the vehicle will no longer be within the control of the vehicle driver.

High standards must be maintained by all the parties involved; from car manufacturers and their suppliers via the actual providers of cooperative services, to road authorities and policymakers. To support the paradigm shift from the autonomous human driven car towards an automated and cooperative driving car, all kinds of legal solutions may be possible. These legal solutions may cover the various areas of law affected by automated and cooperative driving. One may think of issues in private law such as: what are the rights and duties of the user of an autonomous or cooperative driving car? Another issue is related to cooperative driving being a service that is granted by a cooperative driving service provider. What will be the role and the responsibilities of this service provider regarding data protection, safe driving behaviour, compliance with the traffic rules etc.?

Compliance and enforcement

Also the question of compliance and enforcement will have to be addressed. Regarding the vital interest of safe and reliable cooperative systems, a solid legal basis will have to be backed up by serious enforcement. In this way compliance with the data protection rules all over the EU can be maintained. One of the issues with the application of legal notions in cooperative driving is that in such a multi stakeholder environment, multiple interpretations of those legal notions can be adopted. This not only means that the regulations will have to be crystal clear[20], but also that the application of the regulations within the cooperative system should be monitored on a permanent basis. The risk of misuse of protected data will grow with the number of applications where C-ITS has been implemented. Surveillance of the application of the standard will be necessary in order to be able to guarantee a secure and compliant operation.

A non-intrusive compliance monitoring system could eventually be the way to make sure that data protection laws are being obeyed. Using such a system, that should be part of the (privacy) design,
we can also guarantee that technical and communication standards that will have to preserve the security of the communication and thereby the safety of cooperative driving system will be safeguarded.

In this perspective we are now taking a first step: a man-controlled cooperative driving service and the data protection aspects thereof.

[20] Hopefully the new Data protection regulation is going to help on this aspect.

Data protection implementation

How will the transformation of a very private activity like driving a private vehicle oneself into a 'cooperative inactivity', being driven by the cooperative automated vehicle, relate to our legal framework of data protection? How can our privacy be protected in a vehicle that is in constant communication with the environment? Would you, being a car driver, still want to be part of that data explosion, or would you rather be an anonymous passenger that cannot be linked at all to the car data, driving data like location, speed and direction? In-car privacy can be classified as a subjective right and as a personality right. This implies that the grantee has an exclusive claim against the others, the government included, while the others have a corresponding duty towards him (Hohfeld 1920) to respect the privacy of the subject. How to deal with this claim and corresponding duty within the framework of cooperative driving will be one of the major challenges for the years to come.

One of the best ways to avoid infringing the privacy is not to process personal data at all. In that case data will be processed anonymously. When the data are being anonymized the personal data of the subject(s) in the car will be not be attached nor will be attachable to the user data of the vehicle. If this status can be fully achieved, then the data from the vehicle will no longer classify as personal data. Data protection law will then no longer be applicable, personal data rights will be respected entirely.

Although this solution seems very attractive, practice shows that anonymity of data sent by a vehicle to a service provider will hardly ever be really anonymous. Eventually the data will be traceable to the data of the vehicle *(Vehicle Identification Number)* and the data of the owner, or the data of the participant of the cooperative service. But it remains a situation worth striving for from a data protection perspective. However, if the C-ITS data from a vehicle are to be considered personal data, then these data can only be processed with a legitimate legal ground. So what are personal data in this context?

Personal data

Personal data have been defined in the Directive (EG) nr. 95/46, Article 2a as; 'any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

In the A58 project the information sent by the participating vehicle via its on board unit will contain an identifier that will link the on board unit to the system. That means that personal data is being processed, because the information from the on board unit can eventually be matched with the customer of the service. This customer often is the owner of the car or at least a regular user of the (e.g. leased) vehicle, due to the character of the service aiming at regular users. But also situations are possible where the link between the on board unit information and the actual user of the car will be less obvious. Although this issue will not be scrutinized within the framework of this paper, a brief inventory of possible relations within the A58 project will be made.

Suppose the case that a private car owner participates in the A58 project and drives the car himself. His in-car device sends the information conditional to the C-ITS service to the roadside. Will

this information be personal data by nature, or will that depend on the content of the message sent? In other words: will the owner be identifiable from the signal that is sent to the roadside even if the message only contains in itself unidentifiable information? Or to turn the question around: will it be possible to run a C-ITS project like the A58 without processing personal data?

The following situations may illustrate the possibilities when information is running from the in-car system to the A58 system:

1. Vehicle owner = participant C-ITS = driver;
2. Vehicle owner = participant C-ITS ≠ driver;
3. Vehicle owner ≠ participant C-ITS = driver;
4. Vehicle owner ≠ participant C-ITS ≠ driver.

In these examples all entities are supposed to be natural persons. In the first example the car user owns the vehicle, is also participating in the cooperative system and drives the car himself. All three conditions coincide, probably the most common situation. In the second example the vehicle owner, is also participating in the cooperative system, but is not driving the car himself. In the third example the driver is the participant and although he is not directly coupled to the vehicle registration, he is still registered in some way at the service. More indirectly related are the owner and the driver in the fourth example. Here for instance the owner of the car could be the lessor, the user could be the employer and the driver the employee. Although in all cases personal data will be involved, participating in the service does not always reveal the same amount of personal data. In the A58 project for instance, participation does not require the submission of more personal information than an email address and an on board unit ID. The SP will receive a dataset containing the identification of the on board unit and the location and speed of the vehicle. That is all the information necessary to provide the speed recommendation service. The question to answer in all three cases is: to what extend will either one of the car related parties be identifiable from that information? In all examples the *participant* will at least be traceable back to his email address. This address is in itself traceable to the ISP providing the email service. So if the participant is the same person as the driver, the one that generates the location, direction and speed information, than the driver could be easy to identify. However, when the participant is the owner, and the driver has a more distant relation to that owner, then the driver will be less identifiable. When all three roles are with different persons identification of the driver could even be more difficult. For the moment it seems that the identification of the driver is the reason to consider the data sent from the vehicle to the roadside system personal data that requires a legal ground.

Data Protection Legal grounds

To be able to process personal data a legal basis for processing those data will be necessary. Various legal bases given in Art. 7 of the Directive could be applicable in this case. a) The most obvious one, now used within the A58 project, is 'informed consent'. With the explicit permission of the data subject a lot of processing can be done as long as legal standards are being maintained. However, this ground will lead to a vast amount of administrative handling and will therefor not be very comfortable to use. In terms of Hohfelds classification the participant will grant the right to infringe the participants' privacy, to the SP and will have the liability to tolerate this infringement until further notice. b) Less obvious but worth looking at is the processing necessary for the performance of a contract between the data subject and the controller, in this case the contracting SP. This will reduce the administrative handling, but is less strong a consent as the informed consent of Art. 7.a. As it comes to the legal classification in this case the legal relationship has already been established with the service provision agreement.

The service provider has an obligation (duty) to deliver the service and the customer has a right to that service. In order to perform its duty, the service provider will need to process the personal data of the customer. The question is whether this contract provides an autonomous right to process the personal data and whether the customer has the duty to accept the processing of his personal data merely on the basis of the service provision agreement. c) Compliance with a legal obligation is not a ground for processing personal data within the A58 project since no such legal obligation exists. However, that could be different when C-ITS services will directly be connected to the in-car management systems for steering, accelerating and decelerating. It seems logical that, in that stage of C-ITS application, legislation will be the basis for self-driving cars combined with C-ITS technology. The establishment of legislation that will force the road user to share his personal data means, in terms of legal classification, that the service provider is empowered (power) to process personal data for this particular application. On the other hand, the car driver will be disabled (disability) to oppose to such an infringement of the protection of his personal data.

d) In the current interpretation the protection of vital interests of the data subject will not easily qualify as a legal ground for the processing of personal data. Without a service provision agreement between the data subject and the controller, the data subject has no interest at all, let alone a vital one. And when a service provision agreement has been established the legal ground under b) seems to be more appropriate. One imaginable situation where this ground could be valid is when the only way to drive safely is within the cooperative system and the law does not provide for an obligation to join the system as under ground c). In that case the service provider could claim the right to process the personal data and the customer would have no right to oppose. e) This legal ground is reserved for public interest, and therefor not obvious as a legal basis in this phase of cooperative driving. However, when cooperative driving evolves in combination with automated driving this could well be the legal basis when pursuing road safety. The public interest would require legislation implementing the exception foreseen in the Directive. In this legislation a power would have to be created for the authorities and the parties running the system to use the data from the vehicle within the system context. This would lead to another legal ground, c), for the processing of personal data.

On the other hand, a disability would have to be created for the user(s) of the vehicle to exercise their privacy rights, despite their fundamental character. The road user will be granted the right to participate in a safe cooperative driving system. The cooperative driving authority will have the duty to provide that system. Eventually this could deliver an acceptable solution provided that the

personal data involved can be properly secured. f) Also worth looking at seems to be this ground covering the processing that is necessary for the purposes of the legitimate interests pursued by the controller. Regarding this ground the EU privacy Commissioners[21] have prescribed the way in which this ground could be applied. Whether processing is necessary for the purposes of the legitimate interests pursued by the controller should be balanced against the interests of fundamental rights and freedoms of the data subject. Developing this balancing test specifically for C-ITS applications like in the A58 project could be taken into consideration, thus creating an easy to use, predictable and balanced legal ground for C-ITS. In terms of Hohfelds classification the service provider would have a right to process the personal data and the customer would have the duty to accept this processing under the conditions referred to in the balancing test.

All suggestions made here will be subject to further research within the framework of the Dutch C-ITS program.

Shockwave Traffic Jam System

Being able to communicate between vehicles and service providers and between vehicles and other vehicles is essential for cooperative driving. Different communication (network) protocols and communication standards have been developed over the past decades.

Within the project developers have focused on two specific network protocols; cellular or LTE networks (2.5G-4G) that are similar to the ones we use for mobile devices such as smartphones, and the IEEE 802.11 Wireless Local Area Network Protocol (WLAN). Within the A58-project these different network protocols are the indicated as respectively *connected* and *cooperative* ITS, although no clear functional distinction between these protocols exists. Performance issues, i.e. bandwidth and speed, availability, operational structures and costs etc. however vary between them, which may make one more appropriate given some use context than the other.

Both these technologies enable vehicles to communicate with each other or with devices on the roadside, so that data can be exchanged between car and provider, and vice versa (Spookfiles A58 - OCD en Solution Design - Het gemeenschappelijke eindrapport (deliverable) van de Haalbaarheidsfase WP1 in het Spookfiles A58 Project, 2014). The data gathered can be used for collision avoidance, incident management, navigation, vehicle identification and location, etc. Within the A58 project it is only being used for in-car speed recommendation.

[21] Art 29 working group , Opinion 06/2014, 844/14/EN WP 217

In the next paragraph we aim to explain the two distinguished communication technologies, connected (3G and 4G) and cooperative (802.11 p), in more detail, as some of these details have consequences for the data exchange, the parties involved and the legal framework that defines, data ownership, protection, access and use rights.

Communicating Vehicles

In figure 2 the architecture of the A58-project is sketched. From the figure we can read that the vehicle is conceptualized as some vehicle infrastructure (VIS) that allows for applications that can run on top of this infrastructure. Details about the different layers of this VIS are left out as the focus of this paper is on the two different communication technologies that can be used between vehicles and service providers. The typical difference between the two distinct communication technologies is that the technology indicated as *connected* is based upon cellular network technology that is commonly used for mobile communication for which many telecommunication services providers already have set up networks that are also very well interconnected. For the technology indicated as *cooperative* that is based upon WLAN technologies one still has to create such interconnected networks. One of the problems for inter-vehicle communication is the required data-exchange speed, which with currently available networks cannot always be guaranteed. The cooperative technologies at this moment offer a much higher data- exchange speed, but since these technologies are only suited for short-range communication while the connective technologies are suite for long-range communication they will require a vast roadside infrastructure.

The current limitations in bandwidth and communication speed put constraints on the possible technical data-protection measures one could take as part of a secure solution. Complete public-private key encryption of data before sending it to the receiver and consequent de-encryption at the side of the receiver before processing it, would further slow down communication speed and consume more bandwidth.

For this reason the developers of cooperative driving infrastructures have decided to only consider a quite limited form of data encryption including a Public Key Infrastructure (PKI)[22], thus requiring less of the communication technology, but introducing more risks with respect to possible data infringements.

Communication for connected ITS is based on infrastructure-based communication technologies, such as cellular networks (3G, 4G, GPRS, etc.), WiMAX, DVB, etc. Referring to the architecture in 2, the vehicle will exchange data directly with the Service Provider, without any interference of other parties. In the first 'connected' phase of the project cellular networks were used, specifically the 3G and 4G (third and fourth generation) standards, as these connected technologies are most used within the applicable area of the project, the Netherlands.

[22] Public Key Infrastructure = a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption to facilitate the secure electronic transfer of information within the C-ITS system.

Within the EU Platform on C-ITS (Working Party 5) definitions have been developed on both connected and cooperative C-ITS[23].

Interfaces in the A58 project

What data protection issues arise at which A58 project interfaces? To be able to get a good picture of the personal data passing each interface in the system the interfaces will be scrutinized one by one, or grouped where appropriate and possible.

The following interfaces can be identified:

A	From Back office data collection to SP Back office
A*	From road side data applications to roadside SP applications B- To and from SP Back office and in-car applications
D1	From SP Back-office to Road side facilities
D2	To and from SP application and SP Back office
D3	From Road side system to in-car application
D5	From in-car application to roadside
D10	To and from SP applications and Road side facilities
D11	From SP and Road side facilities to Road side network and transport
F	From roadside facilities to road side data applications (=D10)
F*	To and from Road side data applications and Back office data collection
G	From SP back office to Back office data collection
H	From Road Authority traffic management centre to back office data collection
H'	From SP Back office to Road Authority traffic management centre
H*	From Road Authority road side system to road side data application
I	To and from the user to the in-car applications

[23] In WP5 of the EU Platform on C-ITS both connected and cooperative C-ITS have been defined: The definition of cooperative is the following: ' cooperative means that the data will be sent from roadside to and from the vehicles (V2I2V) and between vehicles (V2V) [by all communication means but mainly] by short/range WiFi-p (control and warnings) [and less by cellular 3/4G/LTE (for less critical services)]. In the “cooperative” situation real coordination takes place between vehicles mutually and between vehicles and roadside. This coordination can take place by a driver action (max speed; initially during day one) or automatically by the vehicle systems themselves (e.g. CACC)'.

Within the A58 project based on the EU definitions the first 'connected' version is the cellular version and the ultimate 'cooperative' version will be based on the Wi-Fi-p protocol. As is shown in fig 1. connected ITS implies a (cellular) connection between the in-car service and the back office of the telecom service provider (3G and 4G) via a (roadside) telephone tower. However, this technology cannot provide the speed and bandwidth required for fast car to roadside and car to car communication. Therefor the project will use the ETSI standardised Wi-Fi connection (802.11 P) between the in-car service and the roadside system, established for its low latency and short range communication.

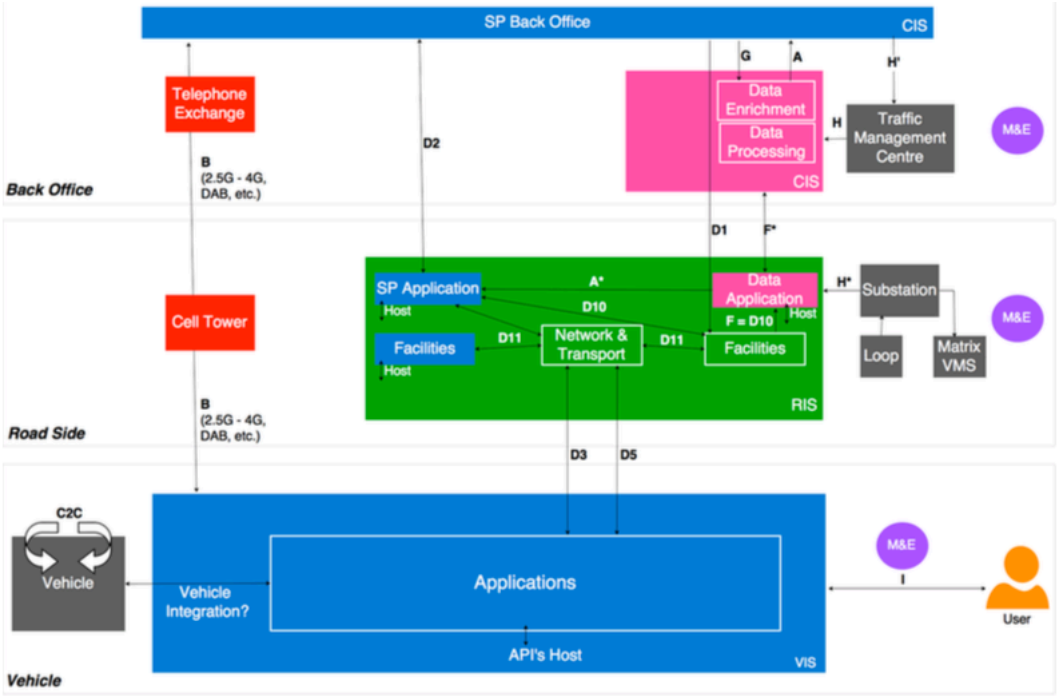

Figure 2 Architecture A58 project

The architecture consists of four different parts:

1. The Back Office, with the Central ITS Station (CIS);
2. The Road Side, with the Roadside ITS Station (RIS);
3. The Vehicle, with the Vehicle ITS Station (VIS);
4. Cellular communication network.

Within the limited scope of this paper similar interfaces will be grouped. This leads to the following groups consisting of one or more interfaces:

1. To and from SP Back office and in-car applications (B, D2)
2. Data collection and exchanging between Service Provider and in-car applications (interfaces A, A*, D10, F, F*, G) Data exchange with the road authority (H, H', H*)

When a legal ground has been found, data traffic within the system passing all the interfaces involved can start. Working outside in and inside out the interfaces will be looked at in their sequential order in the SP process. Therefor we will start with the interfaces involving the driver or the car, then work towards the SP back office, and back again.

1 - To and from SP Back Office and in-car applications

This interface has been used in the first phase of the A58 project, the connected phase. In this phase the in-car device, a smart phone, was more or less directly connected to the back office of the SP.
The data set surely contained personal data, the smart phone of the participant was registered as a mobile phone with all the personal data consequences thereof, and the SP added identifiable data as well as location data. In principle the end-to- end connection with the smart phone is well protected. It is an often used proven interface that delivers the information to the SP via the telecom provider.

Potential data protection leaks are to be looked for in the back office of the SP and its partners, not as much in the cellular connection. So why not go connected then? One of the problems with the connected version of the service is latency. The message could be underway for as much as minutes and that could be too long for an application with road safety implications. That will be even more difficult once the messages will be delivered directly to the in-car management system of a self-driving vehicle. In that case steering and breaking will depend on the system, which means that the latency should be next to none. As far as the confidentiality was concerned: the data ran from the telecom provider straight into the SP back-office.

D5- From in-car application to roadside

This cooperative interface between the car and the roadside system is the first step from the data subject into the cooperative system. The interface has been foreseen as supported by Wi-Fi-p. This technology enables very low latency between car and roadside, suitable for self-driving applications. However, in order to gain from this low latency no encryption should be applied on the messages from the on board unit or other devices. The lacking of encryption means that anyone can receive and read the signal of the car within Wi-Fi-p range. The messages sent from the car to the roadside station may not be encrypted; they are protected by a public key infrastructure (PKI). This PKI authenticates the messages, to make clear that it has come from a legitimate participant. The PKI process itself has all kinds of security rules that have to be followed, regardless the content of the message, and its possible personal character. All roadside stations and participating vehicles will have to be part of the A58 security system.

D11- From the roadside to the roadside service provider facilities and back

This interface brings the messages that are collected directly coming from the vehicle to the RIS facilities. It is merely transportation of the data coming in via interface D5. However, it could contain personal data which will be accessible to the road side service provider, so the appropriate care will be necessary.

2 - To and from the various services engaged by the leading service provider

In this interface the processed data is being sent and processed by and between the service providers that have been engaged to do so by the C-ITS service provider/controller. Whether these data contain personal data depends on the information model of the SP, in particular if personal data remain part of the dataset once it has been received from the users vehicle. If not, then these interfaces will not have to deal with personal data. If so, however, the SP will have to make sure that all parties engaged in the processing of the personal data are aware of that fact and have been instructed to obey the legal terms for the processing of personal data. This is merely an organizational matter. The controlling SP will have to make sure that all legal provisions related to the processing of personal data will be respected.

The A- and A*-interfaces serve to collect data related to traffic flows and independently moving vehicles. The collected data is sent from the Back Office data service providers to the SP Back Office, and from the roadside data application to the SP's applications. Whether these data contain personal data depends on the information model of the SP, in particular whether personal data remain part of the dataset once it has been received from the users' vehicle. If not than this interface will not have to deal with personal data.

The D10 interface exchanges information between the RIS facilities and the SP applications. It could well be processing personal data and appropriate measures will have to be taken in order to make sure that the data is not misused.

The F- and F*-interfaces collect Cooperative Awareness Message (CAM) and Decentralized Environmental Notification Message (DENM) based information, regarding incidents and warnings, and exchange it between RIS facilities and the RIS data application, and the RIS data applications and the Back Office. In the A58-project, this information would be passed on via the A- and A*-interfaces to the SP's applications and back-office.

The G-interface is used for the enrichment of the data received from the car and other sources. Currently, many SP's use 'Floating Car Data', which is sent through mobile cellular networks to customers – therefore through 'connected' technology. However, in the A58- project, this type of data could be used, and could therefore be delivered through the G- interface to data-gathering parties in order to improve the data quality.

3 - To and from the Traffic Management Centre

Interfaces H, H' and H* are the interfaces that are connected to the road authority, specifically to the Traffic Management Centre. Through these interfaces, gathered data (in raw, enriched or otherwise processed through the CIS) is offered to the Off Board functionality, and feedback can be returned to the Traffic Management Centre. No personal data will be passing these interfaces since the most of the data will be anonymized floating car data.

D1: Exclusive unidirectional channel SP - RIS

Interface D1 offers the leading SP a transparent communication channel from its back office to its own Vehicle ITS Station (VIS), through the roadside substations. D1 is a unidirectional channel from CIS to RIS. It can be seen as a connection between the software of the SP, and the application in the RIS (Roadside ITS Station). In the RIS area, coding and broadcasting of the offered information is timely performed, to every VIS within reach. When personal data will be sent the SP will have to make sure that the entire line from back office to the vehicle is well protected and all legal obligations are met.

I: Third party use

The I-interface serves in the A58-project as a connection between the user and front end on-board-unit, which has a cooperative module added.

D3 - From the roadside to the in-car application

The D3-interface links all communication from RIS to VIS. Offers support for ITS G5 (802.11p) messages, but also allows Service Providers to send from CIS and RIS Service Provider-specific information to their own VIS. Whether it contains personal information depends on the information model of the SP. In order to get the message with its customer a broadcast with a PKI security and authentication facility could probably be delivered in the car without containing personal data. If the message contains personal data however than all legal and security requirements will be applicable. This is particularly important because, in order to gain from this low latency, no encryption must be applied on the messages to the on board unit or other devices.

The lacking of encryption on the message itself means that anyone can receive and read the signal to the car within 802.11p range.

Conclusions

In this paper we have addressed a number of issues concerning data protection in C-ITS. The question how data protection can be guaranteed has no easy answers. For a successful implementation of C-ITS it is essential to look into some legal notions. It is crucial to determine if data coming from the vehicle always qualify as personal data, and if so what ground for the processing of those personal data is. We also have to find a way to organize data security when the vehicle will send out unencrypted messages with its WLAN. To get answers that will enable the development of C-ITS a new match will have to be made between current legislation and jurisprudence on data protection on the one hand and the technical developments in C-ITS on the other hand. This requires collaboration between two quite different disciplines and professional practices, law and IT engineering.

The outcome of this ongoing process should be the basis for putting into practice Privacy by Design. This practice should contain well-engineered technology and processes but should also include standards for organizing the stream of data in the various back offices involved. This will call for a closer cooperation between the legal and the data management sides within C-ITS. Only that cooperation can provide us with legally sound software. The modelling approach developed by the Leibniz Centre for Law in collaboration with others based on the Hohfeld breakdown of legal notions can help us to develop transparent and accountable services that can be monitored at software/system level without intrusion in the data processing itself. All these elements will have to be part of the Privacy by Design to prevent data protection becoming a showstopper for C-ITS.

The 7 Foundational Principles

Author: Ann Cavoukian

Introduction

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures.
It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default Setting***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default.*

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — ***Positive-Sum***, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both.

5. End-to-End Security — ***Full Lifecycle Protection***

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. ***Visibility*** and ***Transparency —*** Keep it ***Open***

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject

to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. ***Respect*** for User Privacy — Keep it ***User-Centric***

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Overview of the Telecom landscape including C-ITS .

C-ITS Case Viewpoint

❶❷❸❹❺❻❼❽❾❿