COOPERATIVE INTELLIGENT TRANSPORT SYSTEMS AND THE NEW GENERAL DATA PROTECTION REGULATION

Wouter van Haaften / Tom van Engers

Ph.D. researcher, University of Amsterdam, Leibniz Center for Law
Nieuwe Achtergracht 166, 1018 WV, Amsterdam, NL
vanHaaften@uva.nl; http://www.leibnizcenter.org

Professor, University of Amsterdam, Leibniz Center for Law
Nieuwe Achtergracht 166, 1018 WV, Amsterdam, NL
vanengers@uva.nl; http://www.leibnizcenter.org

Keywords: ***data protection, cooperative intelligent transport systems, privacy by design***

Abstract: *In 2018 new General Data Protection Regulation (GDPR) will come into effect. In 2019 the first cars with cooperative intelligent transport systems will appear on the road. Just before summer 2017 the EU asked the European data protection commissioners to give an opinion on C-ITS, using Wifi-p unencrypted random broadcast of vehicle data, in the context of the new GDPR. The opinion, which was released in October 2017, provides for the first interpretations of the GDPR and also points at serious data protection flaws in the C-ITS design. This paper will analyse a number of issues touched upon in the opinion and will try to establish the impact of the opinion on the development and implementation of C-ITS.*

1. Introduction

On 25 May 2018 the new General Data Protection Regulation (GDPR)[1] will come into effect. It will replace the current Directive, which has been serving for over two decades. The Regulation is meant to take data protection to a level which suites the current state of technology and will do so in the years to come. Since the basis of the legislation, the EU Human Rights Convention, did not change the GDPR is mainly adapted to the contemporary practice and the data protection threads that come with it.

2. General Regulation Data Protection

What are the mayor differences between the old and the new legislation? First of all the new legislation is a Regulation. This means it works directly in all member states and does not have to be transferred into national legislation, like the old Directive. It will serve legal equality in the EU. Furthermore the definition of the concept of personal data has been extended. For instance location data are added to the definition of personal data under Art. 4 of the GDPR. Another serious change is that the monitoring and enforcement has been increased with the prescription of the appointment of an independent privacy officer within companies or industry associations, directly accredited to the board. And last but not least a system of fines has been developed with sanctions up to 4% of the offending company's global annual turnover. In this paper a few of the changes relevant specifically relevant to Cooperative Intelligent Transport System (C-ITS) will be discussed.

[1] Regulation (EU) 2016/679, Article 4 (1): «*‹personal data› means any information relating to an identified or identifiable natural person (‹data subject›); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*».

3. Cooperative Intelligent Transport Systems

One of the new technological applications that will have to comply with the new Regulation is the Cooperative Intelligent Transport System (C-ITS), a system that is now being developed and according to planning will be implemented as of 2019. C-ITS is a cooperative system that supports communication between vehicles (V2V) and with roadside stations (V2R), via Wifi-p[2] short-range communication[3]. In the first phase the communication will be V2R and the usage will be via in car services provided to the driver. A first (Day 1) application, intended to provide more road safety is for instance a warning for a hazardous situation on the road that is not yet visible for the driver, but has to be anticipated on as soon as possible. In the longer run the communication will be between (high level) automated vehicles, in order to facilitate automated driving. With Wifi-p it is possible to drive relatively close to other automated vehicles at high speed because the direct and very fast communication between the vehicles enhances the vehicle sensors. In this way accidents are prevented and the road capacity can be optimized because otherwise sensor driven vehicles will keep larger distance from each other due to the safety margins, programmed by the (human) designers. The technology of Wifi-p implies that the vehicle broadcasts Cooperative Awareness Messages (CAMs) approximately every 4 meters. The range of the broadcast of a vehicle will be about 500 meters, and within that range anyone will be able to pick up and read the messages sent by the vehicle. Because the communication must be quick and open and easy to receive and to process by other vehicles as well as by road side stations, the Cooperative Awareness Messages (CAMs, see annex) sent will not be encrypted. Encryption would mean that all vehicles also should have a decryption key, so encryption does not make sense. Moreover de/encryption would also cost valuable time. In combination with the fact that the location data, being part of the CAM, are to be considered personal data this type of random broadcast truly increases data protection sensitivity. Although the CAMs will almost instantly lose their meaning when the position of the vehicle has changed, they may be stored for a short period of time. This could be for road management purposes, or in order to create an «event data recorder» file that provides for information on the last «minute» of the drive in case of an accident. It can also not be prevented that other entities, not participating in the C-ITS scheme will pick-up and read messages. Some of them may even try to use them for their own (commercial/enforcement) purposes. So the challenges trying to unite the upcoming cooperative technology with the demands of the new GDPR are serious.

4. Opinion 3/2017 of the Art. 29 Working Party

Most of the questions that arise from the confrontation of C-ITS with GDPR are legal questions regarding the design of C-ITS. Will it be possible to justify the use of personal data for road management and road safety services? What legal ground should be applied? How to implement informed consent in practice? What are the implications of a law, providing for a legal basis for public interest applications? Will an individual driver be allowed to switch off the C-ITS application even after it has become a crucial cooperative safety feature on the road?

In order to get guidance on finding answers to these questions the opinion was requested by the EU C-ITS Platform, hosted by the EU Commission. The Commission installed a working group (WG4) that started working on the data protection issues around C-ITS in 2015. At the end of phase I, early 2016, a report was produced concluding that the CAMs were to be considered personal data. Many other questions were still open and in June 2016 Phase II was started and WG4, consisting of representatives of stakeholders, produced a request to the Working party Art. 29 (WP29) in July 2017. In October 2017 the Opinion 3/2017 from the WP29 was issued.

---

2 ETSI standard TR 102 638.

3 Nevertheless a Bluetooth signal, meant to have a a range of about 10 meters was received at a distance: captured 1’600 meters away using a student-budget device.

In its opinion WP29 first of all addresses a number of issues on the basis of the WG4 request. Furthermore it raises issues that come from their understanding of C-ITS Wifi-p in relation to the GDPR. Total understanding of the system by all players involved seems not to have been reached yet. The scope of the opinion is limited by the request, only concerning the first phase of the implementation with only public traffic management and -safety services, and by WP 29 that explicitly stated that its opinion is not concerning the final phase with automated vehicles.

In this paper a few of the main issues brought up by the WP 29 are elaborated on:

- personal data/identification of data subjects;
- subjects rights to information;
- CAM Broadcasting;
- data minimization .

5. Personal Data/Identification of Data Subjects

The definition of personal data is to be found in art. 4 of the GDPR. It defines personal data as data related to an identified or identifiable natural person. The WG4 preparing the request for an opinion has had lengthy discussions on the «personal data» character of the messages involved in C-ITS during its first phase in 2015[4]. Ultimately it was decided that CAMs coming from the vehicle should be considered personal data, thus embracing the principle of singling out, being the isolation on a location of an, not further identified, subject in a way that the subject is distinguished, regardless whether his or her identity can be derived from the CAM or otherwise. Although the single out is not in the Regulations' definition of personal data it is included in the recital 26[5] GDPR. Basis for the single out is a reference to one of the data in the CAM: the location of the vehicle, and the fact that the vehicle can be approached with specific messages relating to that location. This could be the case when a third party receiving the C-ITS Wifi-p signal collects is on several occasions and at various places and thus succeeds in creating a trajectory of a certain vehicle. In this way the person will be singled out, but nt yet identified However by connecting this trajectory to other information, like type of car, home address and work address, identification of the singled out person may become possible.

The conclusion of both the WP 29 in its Opinion 3/2017 and of the request for this opinion by EU-WG4 was that the CAMs are personal data due to the fact that it singles out, at least, the driver of the vehicle, although his or her identity may never be known. That raises the question personal to whom? Who will be identified as the natural person in this case? Who is the subject whose personal data, as defined in art. 4, a), are being processed? In fact the single out moves the identification problem to another level, the data subject.

The CAM primarily can identify a device at a certain location. Information connecting the device to the car or to a natural person is not in the CAM. Nevertheless in the pre-self-driving era, we know that at least one natural person is involved, the driver. So if the CAM is personal data the subject to that personal data will be the driver. The driver could be the owner of the car, a family member of the owner or an employee driving a

---

4 C-ITS, Final Report

5 Recital 26: «*The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.*»

company car or tourist driving a rental car. In some cases it may be possible to establish who has been driving the car, in some cases that may not be possible. So what happens if only the owner can be identified, while another person is driving the vehicle? What consequences will the status of personal data have in such cases?

On the one hand single out can mean that a controller does not know the identity of a data subject it processes the personal data from. On the other hand it could also mean that one is a subject to data processing without knowing who is processing the personal data.

Here the concept of singling out as a measure for personal data may present a down side especially when the «subject» wants to exercise his or her rights[6]. This exercise could proof to be difficult if identification is not possible in the basis of the singled out data and the added information from the alleged subject.

6. Subjects' Rights to Information

The issue arises because the rights of the subject have been seriously substantiated compared to the 1994 Directive. The controller should provide for the opportunity to look into the personal data collected by the controller, allowing the subject to adjust it and to be removed from the database (right to be forgotten)[7].

This subjects' right requires for the controller to establish whom the subject is. No doubt that the subject is the one who was in the vehicle where the CAMs came from. However, if there were four people in the car, where they all four a subject? Probably yes, but it may be possible to identify the vehicle, at some cost, as Reyzin et al. have demonstrated, although it may not always be possible to identify any one of the driver/passengers individually, let alone all four of them. So how can they get access to their data, and how should a controller know that the person requesting information is truly the subject? The subject will have to prove that he or she was in the specific vehicle at the specific time. When another person than the owner is driving and the owner is the only registered subject this could also become problematic. Will he be granted access?

The good news is though that this problem will not easily occur In the case of C-ITS. Since the CAMs are very short lived and no records are supposed to be kept from them after use, presenting data kept from the subject by the controller will not be possible, and thus not so problematic after all. In the Opinion 3/2017 the WP29 is concerned about the fact that no data will be available for the subject to demand on the basis of the Art. 11. It calls upon the WG4 to make proposals on the concept of «additional information» like specific vehicle data or «the highly identifiable nature of location data». However, this call seems to be in vane given the fact that no data are kept in the first place. But even if some data should be retained, the call for additional information that could be given in order to proof actual presence on a location, where the «single out» as the basis for the qualification as personal data has occurred, will probably not be enough to convince the controller. The controller has to make sure that there is no chance that he reveals personal data to any other person than the data subject.

6 Art. 32 GDPR.
7 Art. 12 GDPR.

CAM	**Header**				**protocol Version**
					message ID
					station ID
	cam				**generation Delta Time**
		cam parameters	**basic Container**		***station Type***
				reference Position	***latitude***
					longitude
					position Confidence Ellipse
					altitude
			high Frequency-Container	**basic Vehicle-Container-High Frequency**	***heading***
					speed
					drive Direction
					vehicle Length
					vehicle Width
					longitudinal Acceleration
					curvature
					curvature Calculation Mode
					yaw Rate
					acceleration Control
					lane Position
					steering Wheel Angle
					lateral Acceleration
					vertical Acceleration
					performance Class
					Dsrc Tolling Zone
				rsu Container-High Frequency	protected Communication Zone RSU
			low Frequency-Container	**basic Vehicle-Container-Low Frequency**	**vehicle Role**
					exterior Lights
					path History
			special Vehicle-Container	**public Transport-Container**	**embarkation Status**
					pt. Activation
				special Transport-Container	**special Transport Type**
					light Bar Siren In Use
				dangerous Goods-Container	**dangerous Goods Basic**
				road Works-Container Basic	road works Sub Cause Code
					light Bar Siren in Use
					closed Lanes
				rescue Container	**light Bar Siren In Use**
				Emergency-Container	**light Bar Siren In Use**
					incident Indication
					emergency Priority
				safety Car-Container	**light Bar Siren In Use**
					incident Indication
					traffic Rule
					speed Limit

Fig. 1: Content CAM. The required fields are printed in **bold**; required fields with a value stating there are no data are printed in ***bold italic***.

7. CAM Broadcasting

The CAM and the Decentralized Environmental Notification Message (DENM) will be send randomly and unencrypted. The latter is logical because all other road users will have to be able to collect and process the data without delay. The range of the broadcast will be about 500 meters and the dataset available will not contain identifying data relating to a known natural person due to data minimization. It will contain data that will single out the driver though. Whether this 500 meter range will lead to tracking down people is hard to say. It will demand serious effort; lots of roadside receivers, and software to single out a vehicle driver. On the other hand Reyzin et al. demonstrated that a detecting network can be installed for a few cents per kilometre, and will be hard to detect.

8. Data minimization

Within the CAM the amount of identifying data is cut down to the bare minimum (see CAM, annex). In the day 1 services only data strictly necessary for those services will be broadcasted. Potentially identifying could be the latitude and longitude, and finally the station ID of the device that has sent the message. Most of the other data are voluntary and do not have to be filled in unless a special requirement addresses these data. The WP29 has a few recommendations as to how the privacy sensitivity could be reduced, like using less data in the CAM and noise injection that for instance will make it harder to see the size of a car. Also lower sample rates could be considered.

After these more general issues the WP29 has looked into the privacy risks of the scheme. It is obvious that WP29 is concerned about the amount of risk. Such a large scale broadcast from many vehicles on the road has never been seen before.

9. Privacy Risks

The mayor concern of WP29 is that the introduction of C-ITS will lead to «the collection and processing of an unprecedented amounts of location data of individuals in Europe». This imposes high demands on the systems used, according to WP29.

The following privacy risks have been detected:

- disclosure of how and where the subject drives;
- lack of transparency as vehicles will broadcast constantly;
- messages can be received and read by anyone, losing control over the data;
- kinetic and location data will be valuable to various interested parties;
- data will also be appealing to law and traffic enforcement;
- function creep will be hard to prevent in an open system like C-ITS.

The main concern remains the open character of the system. Although you can wonder if «how and where» everybody drives is really disclosed, and if so, what that disclosure, actually includes besides the location, speed and direction? The risk that trajectories will be constructed thus making the singled out identified is clear and present, according to the WP29. The lack of transparency is supposed to be caused by the fact that the data will leak away when broadcasted. The sender will not be in control of the data and cannot guarantee the confidentiality of the CAMs since anyone could pick them up and read them. This could justify the installation of an on/off switch for the driver, since interested parties could try to receive the CAMs and use them for commercial or even enforcement services. Although that will ask for considerable effort since the broadcast only has a 500m range and the PKI is changed regularly. This could become easier over time due to technological development.

10. Lawfulness of Processing

A substantial part of the opinion is dedicated to the lawfulness of the processing. Specifically the legal grounds for the processing of personal data are being scrutinized regarding the C-ITS application. As basis for the processing to WP29 informed consent is the most desirable legal ground, because the subject then will be at the gate of the data processing. For private services this should not be a problem, but it raises a lot of questions. Who will have to provide for the consent, the vehicle owner, the user, the driver? And will C-ITS have to be switched on, or will it be on by default? The WG4 also proposes some other legal grounds and concludes that for road management and -safety applications the legal basis of public interest could be appropriate. Since this public interest will probably be materialized in a law, the legal basis will be a legal obligation of the controller. The EU Commission should initiate this law making process.

Over all the criticism of WP 29 emphasises the importance of the position of the data subject. The subject should have influence on the processing of his or her personal data to a high extend. The controller, any data processor that decides upon purpose and means of the processing of personal data, will be responsible for the position of the data subject. This controller may be appointed by the law that will establish the Day 1 C-ITS services.

On the issue of security the WP29 concludes that extra effort is needed due to the open character of the system. Because the PKI certificates system was not described in the EU information document the WP29 did not give an opinion on the security system.

11. Actions Mitigating the Data Protection Issues

The opinion concludes with a list of recommended actions to the owners of the C-ITS system. By analysing the relevant issues this paper means to raise the right discussions and questions for future research. The first two recommendations are aimed at the EU-Commission:

> «*The Commission should implement sector-specific Regulations for collecting and processing data in the field of Intelligent Transport Systems;*
> *The Commission should identify a roadmap for lawful processing of location data of EU citizens in the context of C-ITS applications, where the enactment of an EU-wide legal instrument is the final goal (art 6(1)c of the GDPR).*»

These looks like sensible recommendations in the light of the fact that the Day 1 services will be public services.

> «*The adoption of these legal instruments should start with an assessment of necessity and proportionality of its provisions; moreover, a data protection impact assessment (art. 35(10) of GDPR) should be mandated in the course of the legislative process to clarify risks and mitigating measures from the start;*»

This is an interesting recommendation because EU C-ITS WG4 in its request has already tried to indicate necessity and proportionality of the processing of personal data. Obviously this was not considered enough yet. A Data Protection Privacy Impact Assessment (DPIA) is a legally binding step on the way to implementation, and the message to the EU Commission is clear: integrate the DPIA in the legislative process. While doing so, some of the risks and mitigating measures could be included into the legislation. One of those measure that seems viable, at least in this driver support phase, is to lower the frequency of the CAM's in order to reduce tracking possibilities. This will however contain a serious change in the C-ITS standard as made up by ETSI[8]. In that standard some data protection preserving measures were taken, the brand and type of vehicles were

[8] ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, broadcast and Internet technologies. Our standards enable the technologies on which business and society rely.

replaced by dimensions, but the basic Wifi-p Broadcasting system was primarily set up to function well, and not to preserve privacy. Nevertheless the opinion requires the C-ITS community to look at the CAM frequency again, whatever outcome such a re-examination eventually may have.

> «*The other legal bases envisaged in the C-ITS Working Group Document (namely, consent, performance of a contractor legitimate interest) could be relied upon only if the critical issues identified for each of them in this Opinion can be solved;*»

The WP29 approved of the choice for legislation as a legal basis for the processing of personal data[9]. It stated that other legal grounds may be possible, but that they all have down sides that have to be overcome. Furthermore considering that C-ITS will be a public service for the time being the performance of a contract and the legitimate interest of the contractor seems rather far fetched. Those are explicitly private legal grounds. So that leaves us with informed consent, probably the only ground that can be used on the way to legislation. It will lead to a limited group of friendly users, ideal for testing purposes.

> «*In any of the selected legal bases, the default setting of all installed C-ITS functionality must be switched off;*»

Thinking of automated vehicles preserving their road safety through V2V communication this could prove to be problematic. On the other hand legislation could prescribe a default setting «on» perhaps even without the off switch feature. In the phase of advisory services to human road users with friendly users participating based on consent, this condition should be made available in order to take away threats to data protection.

> «*The provisions of art. 25 of GDPR (Data protection by design and by default) should be implemented, allowing users to select the tracking options (timing, frequency, locations) that best fit their preferences;*»

Data protection by design and default is another legal obligation in the GDPR[10]. These conditions have to be met. Again in the friendly user phase this will not impose any problems. In the final phase when the broadcast becomes a V2V and M2M feature the way data protection by design and default will be implemented may have to be re-discussed. Data minimization should be performed as well as noise injection, specifically on the static properties of a vehicle. One of the ways of data minimizations will be to lower the frequency of the CAMs from one every 4 meters to e.g. one every 50 meters, provided this does not destabilize the entire system. The change (lowering) of the sending frequency will also have the effect that the vehicles become less visible. The same goes for a noise injection, for when it concerns the size of the vehicle that will become a lot less recognizable. All these data are less critical when the driver is still in charge. If it can be concluded that for the Day 1 applications no identification is required, also the station ID might be taken out.

> «*Security should be reinforced in order to limit the risk of illegitimate use of C-ITS data beyond the scope of legitimate purposes; Other privacy by design remedies such as generalization or noise injection should be introduced in order not to affect the overall picture of the environmental status and the possibility to spot a new danger, while limiting unnecessary exposure or long term tracking of the driver;*»

With unencrypted broadcasting of personal data, as foreseen in C-ITS, security is deemed to be implicitly included in technical measures to minimize the data broadcasted and to keep up with the security article in the

[9] Art. 6 c GDPR.
[10] Art. 25 GDPR.

GDPR[11], stating that the security should be 1) state of the art, 2) within proportional costs and 2) according to the nature, scope, context and purposes of processing. This article will require permanent monitoring of the state of the security concerning the data processing by the controller.

> «*Special attention should be given to the frequency with which the certificates are changed, in order to create a fair balance between the selected frequency and the risks of long term tracking;*»

By increasing the refreshment rate for authorisation tickets the traceability of the car will be substantially less, provided that the certificates in a certain area also will be changed collectively. This is a way to mask the individual certificate change. In that case a vehicle will be harder to follow being one of the many changing certificates simultaneously. This procedure would also include that no CAMs are being broadcasted during the certificate change. However, looking at the considerations made by the Car2Car Consortium on the issue, it may not be easy to convince the OEMs to put (a lot) more certificates in a vehicle.[12]

> «*Special categories of data and data relating to criminal convictions and offences should not be broadcasted;*»

It is not clear what is meant exactly, but if for instance speeding with more than 30 km/h over the maximum is considered a criminal offence in some member states, a facility that shuts down the speed field in the CAM in such a case could be considered.

> «*Data quality should be carefully assessed in order to mitigate any risk of non neutral use of C-ITS, the generation of false alarms or, on the contrary, the misinterpretation of real emergency situations;*»

A quality standard for the CAM data should be included in the ETSI standards. Furthermore a permanent monitoring system may be necessary to keep up the overall system quality.

> «*The PKI mechanism for certificate distribution should be publically documented in a detailed way and strictly monitored, in order to limit the risk of collusions between certification authorities and peers, or the intrusion of malicious players;*»

Wise advise from WP29. This should be taken on in the roadmap towards legislation.

> «*The retention periods of the processed data by all the parties involved in the C-ITS platform should be clearly indicated, and it should be prohibited to create a centralized database of the exchanged messages by any of the actors of C-ITS;*»

The system as it is designed for the Day1 applications will only require very brief retention periods for operational purposes. After these periods of minutes the data have no further use and should be deleted.

12. Conclusion

The Opinion 3/2017 of the WP29 upon request of the EU C-ITS WG4 is a first step on a new path for both sides. New for the WP29 because the GDPR has not come into effect yet, and new to the EU C-ITS WG4 because C-ITS is not on the road yet either. It is a positive and hopeful development that innovations in car mobility and the protection of personal data are being brought together in such a relatively early stage. It creates room for

[11] Art. 32 GDPR.

[12] Car2car Consortium PKI certificate policy 2017.

dialogue and for rethinking solutions on both sides of the table. For this moment, preparing the pre-legislative phase of C-ITS Wifi-p with Day 1 services, the issues put forward do not seem show stopping.

The day 1 and 1.5 services do not depend on superfast highly accurate data. Since accuracy and visibility go hand in hand also lower amount of visibility and thus higher level of data protection can be achieved when the system is technically downgraded for less visibility of the vehicles. In a later stage, specifically when autonomous driving will be introduced, the accuracy has to be brought at a higher level, thus increasing visibility of the vehicle as well. That scenario was not in the current Opinion, but it is clear that an upgrade of the system, using the currently chosen technologies, may lead to risks that could be considered unacceptable by WP29.

13. References

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

Article 29 Data Protection Working Party, Opinion 06/2013 on open data and public sector information («PSI») reuse, 5 June 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf.

Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 4 October 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888.

Cooperative Intelligent Transport Systems (C-ITS), Final Report, January 2016, «Data Protection Privacy, Recommendations and Guidelines», pp. 48–60, https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf.

European Parliament/Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23 November 1995.

European Parliament/Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

European Standard ETSI EN 302 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, Version 1.3.0. of August 2013, http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.00_20/en_30263702v010300a.pdf.

European Standard ETSI TR 102 638, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, Version 1.1.1. of June 2009, http://www.etsi.org/deliver/etsi_tr%5C102600_102699%5C102638%5C01.01.01_60%5Ctr_102638v010101p.pdf.

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