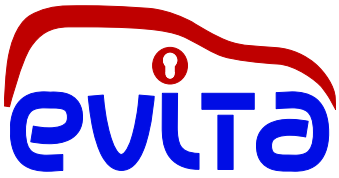

Project acronym:	EVITA
Project title:	E-safety vehicle intrusion protected applications
Project reference:	224275
Programme:	Seventh Research Framework Programme (2007-2013) of the European Community
Objective:	ICT-2007.6.2: ICT for cooperative systems
Contract type:	Collaborative project
Start date of project:	1 July 2008
Duration:	From July 2008 to December 2011 (42 months)

Deliverable D2.4:

Legal framework and requirements of automotive on-board networks

Authors:	Jos Dumortier, Christophe Geuens (K.U.Leuven); Alastair Ruddle, Lester Low (MIRA) with contributions from Michael Friedewald (Fraunhofer ISI)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.1
Submission date:	19 September 2011

Abstract

The objectives of the EVITA project are to design, to verify, and to prototype security architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise. Thus, EVITA will provide a basis for the secure deployment of electronic safety applications based on vehicle-to-vehicle and vehicle-to-infrastructure communication. This document provides guidance on legal issues related to privacy and liability encountered within the scope of automotive on-board networks.

Contents

List of abbreviations

ABI	Association of British Insurers
ABS	Anti-lock Braking System
ACC	Adaptive Cruise Control
ADAS	Advanced Driving Assistance System
AEBS	Advanced Emergency Braking System
ALARP	As Low As Reasonably Practicable
ASIL	Automotive Safety Integrity Level
AON	Automotive on-board network
AVS	Advanced Vehicle System
BAS	Brake Assist System
CAS	Collision Avoidance System
CC	Cruise Control
CMBS	Collision Mitigation Braking System
COP	Conformity of Production
DAS	Driving Assistance System
DPA	Data Protection Authority
DPD	Data Protection Directive (95/46/EC)
DRD	Data Retention Directive
DSA	Detailed Safety Analysis
DSRC	Dedicated Short-Range Communications
EAL	Evaluation Assurance Level
EBS	Emergency Braking System
EC	European Commission
e-Call	Proposed pan-European in-vehicle emergency call system
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EETS	European Electronic Toll Service
EGNOS	European Geostationary Navigation Overlay Service
EPD	e-Communications Privacy Directive (2002/58/EC)
ESA	European Space Agency
ESC	Electronic Stability Control
ETSC	European Transport Safety Council
EU	European Union
Euro NCAP	European New Car Assessment Programme
FCC	United States Federal Communications Commission
FCW	Forward Collision Warning
FIPs	Fair Information Practice principles
FMCSA	Federal Motor Carrier Safety Administration (USA)
GM	General Motors

GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GPSD	General Product Safety Directive
GSM	Global System for Mobile Communications
HMI	Human-Machine Interface
HSM	Hardware Security Measure
HU	Head Unit
IEC	International Electro-technical Committee
ISA	Intelligent Speed Adaptation
ISO	International Standards Organization
ITS	Intelligent Transport Systems
LCC	London Congestion Charge
LDWS	Lane Departure Warning System
MISRA	Motor Industry Software Reliability Association
MS	Member States
MVEDR	Motor Vehicle Event Data Recorder
NASA	National Aeronautics and Space Administration (USA)
NHTSA	National Highway Traffic Safety Administration (USA)
ND	Nomadic devices
NDPA	National Data Protection Authority
NVSR	New Vehicle Security Rating
OBD	On-Board Diagnostics
OBE	On-Board Equipment
OEM	Original Equipment Manufacturer
OJ	Official Journal of the European Union
PbD	Privacy by Design
PETs	Privacy-Enhancing Technologies
PSA	Preliminary Safety Analysis
ROSPA	Royal Society for the Prevention of Accidents (UK)
SIL	Safety Integrity Level
TCD	Toll Context Data
TEC	Treaty Establishing the European Community
TFEU	Treaty on the Functioning of the European Union
Thatcham	Motor Insurance Repair Research Centre (UK)
TPMS	Tyre Pressure Monitoring Systems
UNECE	United Nations Economic Commission for Europe
V-2-X	Vehicle to environment (i.e. other cars, roadside infrastructure) communication
WVTA	Whole Vehicle Type Approval
WP29	Article 29 Data Protection Working Party

List of tables

Document history

Version	Date	Description
1.0	2011-09-13	First issue of deliverable
1.1	2011-09-19	Editorial corrections

1 Introduction

1.1 EVITA objectives

The objectives of the EVITA project are to design, to verify, and to prototype a modular, (cost-) efficient security solution for automotive on-board networks in order to protect data within such networks against compromise and, in doing so, to enable secure communication among cars and between cars and infrastructure. By focusing on the protection of the on-board network, EVITA complements other e-safety related projects that focus on the protection of inter-vehicular communication.

1.2 Scope of this deliverable

The scope of this document is to provide guidance in relation to legal issues encountered within the scope of automotive on-board networks. The main legal domains treated are privacy and liability since these legal issues appear to be the most problematic in the 18 **use cases** defined in Deliverable D2.1 of the EVITA project[1].

The 18 individual use cases can be grouped into a number of categories for the convenience of the legal analysis:

- **V-2-X:** use cases involving external wireless communication between vehicles and other vehicles or roadside infrastructure;
- **eToll:** toll transactions;
- **eCall:** emergency assistance calls;
- **nomadic devices:** use cases involving in-vehicle wireless communications links or temporary wired connection such as USB devices;
- **aftermarket:** installation of aftermarket modules or replacement of defective modules;
- **diagnosis:** including both diagnostic and software maintenance activities.

In the following paragraphs we take a closer look on each of these **six use case categories**.

1.3 Relevant use cases

1.3.1 V-2-X

V-2-X is based on the exchange of data between a vehicle (V) and its environment (X), which may include other vehicles as well as roadside infrastructure. Consequently the quality of V-2-X depends on the quality of the information exchanged between all actors involved. A first

[1] E. Kelling et al, "Specification and evaluation of e-security relevant use cases", Deliverable D2.1 of EVITA, 2009. http://www.evita-project.org

step is that this information should be trustworthy. This means that the information contained in the messages reflects the situation as it actually is on the roads.

With regard to traffic information, this could mainly entail that if a traffic jam is indicated at a certain location, there is effectively a traffic jam at that location. The presence of a non-indicated traffic jam at a certain location should not necessarily mean that the information is not trustworthy. Traffic jams can start suddenly and may not be immediately notified. But if a traffic jam is notified this traffic jam should effectively exist. What should be done if a traffic jam has ceased to exist only recently? How soon should the information be cleared from the system? One could say that as soon as notifications cease this should be interpreted as the end of the traffic jam. Legal requirements in this regard may be established as a result of Directive 2010/40/EU discussed in Chapter 2 of this deliverable.

Another element of trustworthiness is that the message should be authentic. Authenticity means that the message should come from the entity from which it is said to be originating[3].

From a product safety and product liability point of view it is further important that automatic vehicle responses are restricted to situations where an actual danger is present. Product safety rules state that a product is safe if it does not present any risk to users or presents only those risks that are considered acceptable. Motor vehicle accidents claimed around 35,000 lives in the EU in 2009[4], yet a motor vehicle is considered to be a safe product since motor vehicle accidents are considered system damage. Yet if, for example, the brakes could be activated erratically in some way through V-2-X messages, the vehicle would be considered unsafe. Automatic action such as braking or throttle release should take place only when the situation requires should automatic action such as braking or throttle release take place. The driver should however remain in control of his vehicle at all times. This is important since it is unclear how liability law would deal with autonomous vehicles circulating on the roads.

1.3.2 Road Tolling

Electronic road-toll collection is moving to the forefront. Given the flexibility of implementation, electronic toll collection is seen as a means to different ends[5]. In some situations it is used to combat congestion or to impose a certain mobility policy such as the LCC, in others the revenues are used to finance road-network maintenance and expansion. The increase of traffic and the sometimes difficult geographical situation means that the classic toll booths and toll plazas are not always suitable[6]. Electronic Toll Collection is a possible solution to these problems. Depending on the technology and system architecture it may be possible to achieve this without the need for extensive and expensive road-side infrastructure to implement the system.

[3] EVITA D2.3, section 2.1.2.3.

[4] "ETSC MEP Briefing: European Parliament Own Initiative Report on Road Safety", European Transport Safety Council, 4th March 2011

[5] Jaap-Henk Hoepman, "Follow that car! Over de mogelijke privacygevolgen van rekeningrijden en hoe die te vermijden", Privacy en Informatie 5(2008), 225

[6] Roger Clarke, "Person-Location and Person-Tracking: Technologies, Risks and Policy Implications", *Information Technology and People* 14 (2001): 206

One can distinguish between three general types of road tolling schemes[7].

- A first one is a zone-based system. In such a scheme a toll is due to enter a specific zone. Two examples are the LCC and Singapore's Electronic Road Pricing.
- A second one is a point-to-point system. Examples include the French Télépéage and the 407 Express Toll Route in Canada. In these systems the use of a particular stretch of road is charged. This is probably the best known example as well.
- A third system is a wide-area system also known as pay-as-you-drive. In such a system one is charged for the actual use of the roads within a certain territory.

This is also the main difference between the two other schemes. In a zone-based scheme, it does not really matter how long is spent in the zone or the distance travelled; the charge is simply for access to the controlled zone. In a point-to-point scheme, the charge is for access to a specific section of a road, but seldom for the full distance travelled on that road, again a fixed amount. A wide-reach system allows a more targeted policy by differentiation based on criteria such as distance travelled, time of day, type of road and vehicle type[8].

From a **privacy** point of view, the most problematic type of road tolling seems to be the wide-area system[9]. In zone-based and point-to-point systems anonymous payment schemes have already been implemented and the personal information collected is minimal. In France one pays at a toll booth, but no record is kept from the transaction. On the Canadian 407 an electronic system has been implemented that guarantees conditional anonymity[10]. This system uses a pre-paid account and as long as sufficient funds are available in the account linked to the On-Board Equipment (OBE), the user will not be identified. On the contrary, given the reach of a wide-area system, a track-log is required in order to enable accurate tolling. This track-log records every movement of the vehicle in the territory covered by the wide-area system. And this extensive coverage is a reason for concern[11]. In the other two types, the only personal information known, if any at all, is when a person passes a specific point. This information is not useless, but does not provide the level of knowledge that a detailed track log provides.

The possibility of detailed tracking and tracing begs two questions. The first is to what extent track and trace is tolerable at all. Is the toll operator authorised to monitor the users continuously or only to collect data at specific intervals? Another question relates to law

[7] International Working Group on Data Protection in Telecommunications. Report and Guidance on Road Pricing – Sofia Memorandum, http://www.datenschutz-berlin.de/attachments/596/Roadpricing_engl.pdf?1245751410

[8] Jaap-Henk Hoepman, "Follow that car! Over de mogelijke privacygevolgen van rekeningrijden en hoe die te vermijden", *Privacy en Informatie* 5(2008), 225

[9] International Working Group on Data Protection in Telecommunications. Report and Guidance on Road Pricing – Sofia Memorandum, http://www.datenschutz-berlin.de/attachments/596/Roadpricing_engl.pdf?1245751410

[10] Ann Cavoukian, *407 Express Toll Route: How you can travel the 407 anonymously,* Information and Privacy Commissioner/Ontario archive, http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=335

[11] Roger Clarke, "Person-Location and Person-Tracking: Technologies, Risks and Policy Implications", *Information Technology and People* 14 (2001): 206; International Working Group on Data Protection in Telecommunications. Report and Guidance on Road Pricing – Sofia Memorandum, http://www.datenschutz-berlin.de/attachments/596/Roadpricing_engl.pdf?1245751410; Paul Won-Bin Sung et al, *Impact of Electronic Road Toll Technology on Privacy*, Otago Polytechnic repository, http://bitweb.tekotago.ac.nz/staticdata/papers06/papers/265.pdf

enforcement access to these track logs, as these could provide information that proves potentially useful in a criminal investigation. This issue has two main aspects. The first is the accessibility of the existing data. Can the data stored in back-end servers or OBE be seized and searched in a criminal investigation? In the proposed system in the Netherlands, the government would not have any access to road tolling data unless the data would be required for a criminal procedure[12]. A second aspect is whether the government should have access to a "backdoor" to overcome safeguards built into the OBE. For instance, in the US, the FBI has already used stolen vehicle recovery features to eavesdrop on suspects[13]. This requirement would have an impact on the architecture of the system, because the system can only do what it is designed to do. A privacy-by-design approach of the OBE could inhibit real-time tracking and tracing[14]. When use is made of OBE the back-office only receives the total amount of toll due but none of the details used to aggregate the fee. These remain in the OBE under the control of the user of the vehicle. Furthermore, toll systems based on DSRC technology may not allow for continuous tracking unless an extensive network of road-side infrastructure is available.

A very important further requirement is **non-repudiation**. Next to protection of the private life of the user it may be the most crucial requirement. When the Netherlands were debating a nation-wide electronic road tolling system one of the most important aspects was reliability[15]. To this effect the Netherlands set forth that only approved equipment could be used and that this equipment could only be installed by certified entities. It also included a provision that one could not repudiate the toll amounts unless one had a certificate stating that one possessed defective OBE. This effectively means that the OBE is considered to be providing correct information unless one holds a certificate that this is not the case.

With regard to the **confidentiality and anonymity,** one can refer to the case of the 407 Express Toll Route. It offers an anonymous tolling option and this option would require that no personal data be transmitted outside the vehicle. Also important in this regard is that it should not be possible to follow a vehicle based on its communication with a back-office server. Today it is already possible to follow a person using the signals emitted by his mobile phone. This could also be applied to follow a vehicle by using the signals from on-board communication equipment. Some vehicles use a Bluetooth-link with a mobile phone to engage in external communication. This would facilitate following a user even more since only one device would have to be followed instead of several.

---

[12] Ernst-Jan Hamel. "Overheid belooft privacy bij kilometerheffing"in Webwereld Archive, http://webwereld.nl/nieuws/64314/overheid-belooft-privacy-bij-kilometerheffing.html (accessed 16 December 2009)

[13] Kevin Poulsen, "Courts limit in-car FBI spying", The Register. http://www.theregister.co.uk/2003/11/20/court_limits_incar_fbi_spying/ (accessed 16 December 2009);

International Working Group on Data Protection in Telecommunications. Report and Guidance on Road Pricing – Sofia Memorandum, http://www.datenschutz-berlin.de/attachments/596/Roadpricing_engl.pdf?1245751410(Accessed 15 December 2009); Lawrence Lessig, *Code V2.O.* (New York: Basic Books, 2006)

[15] Christophe Geuens , Els Kindt and Jos Dumortier, "Anders Betalen voor Mobiliteit : Is de privacy nog steeds gewaarborgd?", *Computerrecht* 2010/5, pp. 228-236

1.3.3 E-Call

One big issue for e-Call is the activation of e-Call[16]. Activation of e-Call from outside the vehicle in which it has been installed must be prevented in order to ensure that continuous tracking of the vehicle is not possible. Activation should only take place through the occurrence of a motor vehicle accident or via a panic button operated from inside the vehicle. Currently, activation through a motor vehicle accident is mostly achieved by linking the system to the crash sensors used for the airbags. If the airbags are deployed, then e-Call is activated. But this also means that e-Call should be activated every time the airbags are deployed and maybe even when, due to a malfunction, the airbags do not deploy despite being given the appropriate command. This is important from a product liability perspective. E-Call could be considered defective if it is not activated in situations when it should be activated. This means that in case of a motor vehicle accident fulfilling the preset parameters for alerting the emergency services the emergency services should be notified. This is also specified in the functional requirements of the Use Case. But at the same time, false or malicious e-Call messages have to be avoided.

e-Call presents privacy and personal data protection issues. As already mentioned above, e-Call should not become a tracking system. It should only be used for alerting the emergency services. It should not be put to other uses. Additionally, when the system is activated only authorized recipients should be sent the data.

1.3.4 Nomadic Devices

With regard to nomadic devices (ND) potential legal difficulties could stem from data protection rules and product liability. Since the idea is that there would be data exchange between the vehicle head unit (HU) and ND, the communication links as well as the access points of the communication have to be secured. Not only should the communication in itself be protected, but also the points where information leaves one device and enters the other have to be secured to prevent attackers from accessing the HU or ND through those points and to prevent amongst others theft of information or loss of control of the vehicle because of attackers.

This is important from a **data protection** point-of-view since data protection rules require that personal data be protected from illegitimate use with appropriate means. As we will further explain in more detail "appropriate means" entail that one should consider the nature of the personal data involved and the potential threats to that personal data. Based on this assessment one should implement the means that are most adequate in dealing with these issues. If this requirement is not met, the data controller can be held liable for failing to comply with the security safeguards as set out by data protection rules. In this context it is important to mention that data protection laws in the EU are based on Directive 95/46/EC, but are subject to implementation in national legislation, which may lead to disparities in implementation between the Member States. The Directive states that the Member States are responsible for imposing liability for damage caused by infringement of the national implementation

[16] Christophe Geuens and Jos Dumortier "Mandatory implementation for in-vehicle eCall: Privacy compatible?", Comput. Law and Secur. Rev., Vol 26, Issue 4, 2010, pp. 385-390

of Directive 95/46/EC. In addition to the provisions found in national implementations of Directive 95/46/EC, national rules on liability may also apply.

The issues with regard to **product liability** focus primarily on the secure integration of ND with the HU. This integration should not have a negative effect on the vehicle or its occupants. As mentioned previously, to consider a product as safe the impact of that product on other products must be taken into account. Therefore if the integration of ND with the HU comes with negative consequences for the HU or vehicle, issues with regard to product liability arise. And this comment could be extended to the communication channels. The communication channels should benefit from appropriate security because they should not provide an attacker with easy access to the ND, but more importantly the HU or, even worse, the vehicle in which the HU has been integrated. Not only should the content of the communication be protected but also the communication channel itself should benefit from appropriate security. The communication channel should not provide an easy point of access to attackers or other unauthorised entities.

1.3.5 Aftermarket

With regard to aftermarket equipment, similar comments as with regard to secure integration in the previous section can be made. It is important that the ECU, OBE or anything that is installed or replaced in the vehicle is properly integrated in the vehicle and therefore does not impede the proper operation of the vehicle.

Another aspect in this regard is to assure that only authorised products are installed in the vehicle. Installation of counterfeit products may be detrimental to the operation of the vehicle and should therefore be prevented. Furthermore, products that have been tampered with should also be prevented from being installed in the vehicle. These illegitimate products should not allow attackers to gain access to or acquire control over the vehicle.

This evidently raises the question with regard to the legal consequences if illegitimate products were to be installed in the vehicle and cause damage. It is important to point out that what is discussed in the previous paragraph is a malicious induction of failures in the vehicle. Two actors are likely to see their liability invoked. The first is the manufacturer of the vehicle whose product is affected by the tampered product. The second is the manufacturer of the tampered product.

With regard to product liability of the manufacturer of the tampered product one could say that the manufacturer is exempt if the failure was likely not present at the moment he manufactured the product[18].

1.3.6 Diagnosis

With regard to the diagnosis use cases the main legal issues are related to data protection and, as we will further discover in this report, in particular to the definition of the data controller(s) and the processor(s) in such a scenario. Take the example of a car repair shop processing data

[18] Art. 7 b), 85/374/EEC

in the context of a remote diagnosis system and therefore using a specialised service provider operating under a contract with the car manufacturer. Let us further imagine that the specialised service provider operating the remote diagnosis system uses the services (for example the data centre) of a cloud service provider. Who is (are) the controller(s) and the processor(s) in this constellation?

A further issue related to data protection is related to data access. While the service station is authorized to obtain knowledge of certain data, others are not. Therefore the communication interfaces should benefit from appropriate protection to prevent personal data from leaking through the interfaces[19]. Attackers should be prevented from obtaining knowledge of data through the use of the diagnostic interfaces as a point of access. It seems unlikely that it will be accepted that attackers can make use of the diagnostics process to tamper with the user's vehicle. This tampering could include modification or extraction of personal details or other data contained in the vehicle, or impeding its proper operation. This would be a serious threat to the general safety of the vehicle and its occupants.

1.3.7 Common Issues

A first common issue is eavesdropping. The possibility that outsiders obtain information regarding the communication taking place between a vehicle and authorised entities should be prevented. The possibility that outsiders obtain knowledge of information transferred inside the vehicle should also be prevented. This is mainly important with regard to the protection of personal data held in the vehicle and transferred inside the vehicle or communicated to authorised entities.

In relation to this first issue there is also the issue of secure communication. While this was mainly brought forward with regard to the diagnostics and nomadic device use case categories, this also matters for other use cases. Secure communication should be guaranteed both for wireless and hardwired communication. It would appear pointless to secure the wireless communication means of a vehicle if the hardwired connection is not protected. This has been demonstrated by researchers at the Universities of San Diego and Washington[20].

1.4 Dark-Side Scenarios

The possibility that security vulnerabilities of modern vehicle systems may be exploited by attackers has prompted several academic investigations in recent years. Examples of attacks on vehicle systems already implemented or simulated by researchers via wireless communications links are summarised in Table 1. One of the security studies listed in Table 1

[19] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Experimental Security Analysis of a Modern Automobile" in *Proceedings of IEEE Symposium on Security and Privacy ("Oakland") 2010*, IEEE Computer Society, May 2010 (also available at Autosec.org), p. 2

[20] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Experimental Security Analysis of a Modern Automobile" in *Proceedings of IEEE Symposium on Security and Privacy ("Oakland") 2010*, IEEE Computer Society, May 2010 (also available at Autosec.org)

addresses attacks on Tyre Pressure Monitoring Systems (TPMS). This is of particular interest as mandatory installation of TPMS is required for vehicles of category M_1 from 1st November 2012[21] under the EC WVTA legislation (see further Chapter 4.1.7.3).

A further case study in this general area was carried out by Volvo for the SIGYN project[22]. This project aims to create a system that provides remote firmware update and diagnostic facilities for vehicles. Various security and privacy issues related to ad hoc vehicular networks were investigated, and countermeasures that could help to mitigate these risks were suggested[23].

Table 1 Examples of published vehicle security investigations

Attack experiment	Potential attacker Objectives	Assets attacked	Vulnerabilities exploited
Wireless hack of Bluetooth/media player system installed in vehicle[24]	Theft of vehicle without forced entry Conduct malicious surveillance Sabotage safety critical systems in vehicle	Central locking GPS System Braking system	Bluetooth protocol and Bus connected to media player enable attackers to access ECU of vehicle.
Using relay technology to extend wireless range of keyless entry system[25]	Theft of vehicle without forced entry	Central locking Keyless engine ignition	Possibility of extending the wireless communication range of the keyless module tricks the keyless system into thinking that the keyless module required to open door or start vehicle is near or within vehicle.
Using wireless technology to disrupt signals sent from tyre pressure monitoring system (TPMS) sensors to on-board computers[26]	Stop vehicle Distract driver Conduct malicious surveillance	Vehicle ECU TPMS display messages TPMS wireless communications	Simple protocols and absence of security measures on TPMS communications enables attackers to spoof messages sent to ECU. Unique identifier on TPMS enables location tracking.
Simulation of attack on vehicle Engine Control Unit by inserting malicious code via Control Area Network (CAN)-Buses[27]	Denial of service/ Distract driver Sabotage safety critical systems in vehicle	Electric windows Electronic throttle control	The integrated network topology of the CAN Bus exposes electronic components of the vehicle to spoof messages and replay attacks.
Simulation of attack on ECU via FlexRay[28]	Sabotage safety critical systems in vehicle	Equipment facilitating firmware updates over air and remote diagnostics. Brakes/Airbags	FlexRay protocol open to external access enables hackers to use external networks such as the Internet to remotely access the vehicle diagnostic equipments

[21] Art 9(2), EC Regulation No. 661/2009

[22] K. Amirtahmasebi, S.R. Jalalinia, "Vehicular Networks – Security, Vulnerabilities and Countermeasures", MSc Thesis, Chalmers University of Technology, June 2010

[23] K. Bjelkstal, "Exchange of Diagnostic Information between Car and Centralized Functions", VINNOVA Information 2008-04l, ISSN 1650-3120, Vehicle-ICT Sweden, April 2008

[24] Erica Naone "Taking control of cars from afar", Technology Review, 14/03/2011, available online at: http://www.technologyreview.in/computing/35094/page1/

[25] A. Francillon, B. Danev, S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars", available online at: http://eprint.iacr.org/2010/332.pdf

[26] I. Rouf *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study", Proc. 19th USENIX Security Symposium, August 2010

[27] T.Hoppe and J. Dittmann, "Sniffing/replay attacks on CAN buses: a simulated attack on electric window lift classified using an adapted CERT Taxonomy", Proc. 2nd Workshop on Embedded System Security, October 2007

[28] D.K. Nilsson, U.E. Larson, F. Picasso and E. Jonsson, "A first simulation of attacks in the automotive network communications protocol FlexRay", Proc. Int. Workshop on CISIS, 2008

The dark-side scenarios of EVITA have been described in Annex B of Deliverable 2.3. An important opening remark in relation to the scenarios is that attackers are rather likely to be subject to criminal law as a result of their actions. This may have important consequences on how the law will deal with these attacks should they occur. For the purpose of the technical development these scenarios are part of a prior assessment to identify potential vulnerabilities in systems and determine what measures should be taken to protect in-vehicle networks. From a legal perspective they can also serve as help in determining responsibilities under law. With regard to these legal responsibilities, it is important to point out that not only the vehicle operator/owner may suffer the consequences of the attack, but also others such as the OEMs may suffer as a result of an attack. Consequently OEMs and their suppliers may be victims as much as the vehicle operator/owner. The range of stakeholders considered to be under threat includes vehicle users, other road users, OEMs and their suppliers, ITS operators and civil authorities. The potential threat agents considered in this work are similarly wide-ranging, including dishonest drivers, hackers, criminals and terrorists, dishonest organisations and rogue states.

Another important aspect is Annex C of Deliverable 2.3, which outlines a risk analysis related to the dark-side scenarios. The dark-side scenarios are not considered equally; each is associated with a number of hazards (described as "attack objectives" in Deliverable D2.3), for which relative severity is assessed based on both the type and the degree of harm that could result for the stakeholders. The type of harm is considered in terms of safety, privacy, financial and operational aspects, and the severity of each aspect is classified in one of five qualitative levels. The severity ratings are derived from automotive functional safety[31] and software development[32] standards. These approaches have been extended to consider other types of harm and the potential to affect many vehicles through an attack. The severity rating also reflects the potential for an attack to affect many vehicles, which is regarded as more severe than attacks that only impact on a few vehicles. Furthermore, each attack objective may be achieved via one or more "attack methods", for which the probability of a successful attack can be estimated. The potential for the driver to influence the situation also contributes to the probability estimate for safety-related attack objectives. The relative risk associated with the attack objectives is related to the perceived severity of these hazards, but moderated by the estimated probability of a successful attack. Thus, attacks with severe outcomes and high probability represent high risks, while attacks with low probability and minor outcomes represent low risks. Attacks with severe outcomes may be relatively low risk if the probability of success is low, while attacks with high probability of success may be relatively high even if the outcome is not at the higher end of the severity spectrum.

Intent is often relevant with regard to criminal prosecution. Many crimes require intent to be proven in order to obtain a conviction. It is not required for prosecution but in some cases there can be no conviction without intent. This is also important with regard to liability. If one is the victim of a criminal act one can act as plaintiff claiming damages ("*partie civile*"). In some jurisdictions it is impossible for a private person to sue directly for criminal acts. One can file charges with the public authorities, mostly the police, and then the public prosecutor

[31] ISO/CD 26262, "Road vehicles – Functional safety", ISO, draft, 2006 (9 parts)

[32] "MISRA Guidelines for safety analysis of vehicle based programmable systems", ISBN 978 0 9524156 5 7, MIRA, 2007

can launch a criminal investigation. Or the public authority decides to prosecute and the victim can then act as plaintiff claiming damages and join the procedure but in a passive role. The victim acting as plaintiff claiming damages is only a passive party but his presence as plaintiff allows him to claim damages if the suspect is convicted based on the charges. This prevents the victim from having to sue in civil court to obtain damages. If the suspect is not convicted the plaintiff will have to refer to civil court if he wishes to obtain damage. The outcome of the criminal trial should be of no influence on the outcome of the civil trial. But it should not be forgotten that the burden on the victim is much higher if he wishes to obtain damages from a civil trial, which requires active participation compared to the passive role he has in a criminal trial where the public prosecution is the main actor acting against the suspect.

1.5 Summary of privacy and liability issues

A summary of possible liability issues for the 18 use cases, grouped into the categories described above, is presented in Table 2. Similarly, a summary of possible personal/vehicle information that may be transmitted, which may suggest possible data protection issues, is presented in Table 3. The content of these tables is based on the "dark-side scenarios"[33] outlined in EVITA Deliverable D2.3.

[33] EVITA D2.3, Appendix B

Table 2 Summary of possible liability issues affecting EVITA use cases

Category	Use Case	Description	Possible Liability Issues
V2X	1	Active Brake	Collision due to system failing to operate Collision due to malicious remote operation of system Secondary collision or loss of control could be judged to be caused by incorrect operation Malicious transmission of false signals
	2	Local Danger Warning from Other Cars	Distraction of driver Driver disregards warnings (false/late messages reduce confidence)
	3	Local Danger Warning to Other Cars	See case 2 Manipulation of traffic flow (via false or delayed warning messages)
	4	Messages Lead to Safety Reaction	Secondary accidents
	5	(MyCar2Car) Local Danger Warning to Other Cars	See case 2 Manipulation of traffic flow (via false or delayed warning messages)
	6	(MyCar2Car) Traffic Information to Other Entities	See case 3 Manipulation of speed limits (by creating false illusion of traffic conditions)
	9	Remote Car Control	Theft of or from vehicle Personal injury caused by operation of windows or hood Driver distraction due to manipulation of in-car environment (temperature, sound levels, seat position) Injury to pets in car due to overheating
	10	Point of Interest	Distraction of driver due to "spamming" (unwanted information/advertising)
e-Toll	7	e-Tolling	Overcharging Underpayment Payment avoidance Disclosure of personal bank account data
e-Call	8	e-Call	Delays in rescue due to failure to operate correctly Charges for response to a false alerts Loss of service (due to overloading system with false calls)
Nomadic Devices	11	Install Applications	Interference with vehicle operation (through installation of malicious code)
	12	Secure Integration	Interference with vehicle operation (through installation of malicious code)
	13	Personalise the Car	Interference with vehicle operation (through installation of malicious code)
Aftermarket	14	Replacement of Engine ECU	Interference with vehicle operation (through installation of corrupt or malicious code)
	15	Installation of V-2-X Unit	Identity fraud (false vehicle status, vehicle identity, or user identity)
Diagnosis	16	Remote Diagnosis	Disclosure of personal data Interference with vehicle through installation of malicious code Unnecessary replacement of vehicle parts or equipment (due to falsified diagnostic reports)
	17	Remote Flashing	Interference with vehicle operation (through installation of malicious code) Insurance/warranty may be invalidated due to unauthorised modifications
	18	Flashing per OBD	Interference with vehicle operation (through installation of malicious code) Insurance/warranty may be invalidated due to unauthorised modifications

Table 3 Summary of possible data protection issues affecting EVITA use cases

Category	Use Case	Description	Possible Data Protection Issues
V2X	1	Active Brake	Vehicle identity Sequential past, present and predicted future position/time data
	2	Local Danger Warning from Other Cars	Received information only, but could perhaps be exploited by malicious users
	3	Traffic Information from Other Entities	Received information only, but could perhaps be exploited by malicious users
	4	Messages Lead to Safety Reaction	Vehicle identity and type classification Sequential past, present and predicted position/time data Description of hazard caused by e.g. emergency manoeuvre or breakdown
	5	(MyCar2Car) Local Danger Warning to Other Cars	Vehicle identity for authentication Present position/time data Description of hazard from on-board sensors
	6	(MyCar2Car) Traffic Information to Other Entities	Vehicle identity for authentication Present position/time data Description of traffic from on-board sensors
	9	Remote Car Control	Link between vehicle and driver mobile device Implication that car is unoccupied Information on car status
	10	Point of Interest	Vehicle identity Sequential past, present and predicted future position/time data Implication of driver's needs (e.g. looking for filling station implies low on fuel)
e-Toll	7	e-Tolling	Vehicle identity Toll contract identity Sequential past and present position/time data
e-Call	8	e-Call	Vehicle identity Sequential past and present position/time data Description (perhaps even identity) of driver, and possibly all other occupants Medical data on driver, and possibly all other occupants Data on crash
Nomadic Devices	11	Install Applications	Possibility to install malicious software that could enable "leakage" of personal data via mobile device
	12	Secure Integration	Possibility to install malicious software that could enable "leakage" of personal data stored in car or in notebook via the mobile device
	13	Personalise the Car	Link between vehicle and mobile device that could be used to identify user Personal information about the user
Aftermarket	14	Replacement of Engine ECU	Vehicle identity
	15	Installation of V-2-X Unit	Vehicle identity Payment contract identity
Diagnosis	16	Remote Diagnosis	Any data held on vehicle
	17	Remote Flashing	Possibility to install malicious software that could enable "leakage" of personal data
	18	Flashing per OBD	Possibility to install malicious software that could enable "leakage" of personal data

1.6 Document outline

The remainder of the report is structured as follows: Chapter 2 focuses on the European legal framework in relation to Intelligent Transport Systems (ITS). Chapter 3 discusses the legal framework for privacy and data protection. Chapter 4 outlines relevant liability law, including vehicle type approval and product safety. Chapter 5 provides conclusions.

2 ITS Legal Framework

2.1 Overview

The subject of this Chapter is the European legal framework in relation to Intelligent Transport Systems (ITS). ITS is usually defined as advanced applications that use Information and Communication Technologies (ICT), which are embedded in different transport modes for interaction between them. Generally speaking, the objective of the EVITA project is to make ITS more secure. Hence it needs to take account of the European legal framework that is currently under development in the area of ITS. At the time of writing this framework consists of the ITS Framework Directive 2010/40/EU and the specific legal provisions on electronic road tolling in Directive 2004/52/EC and Commission Decision 2009/750/EC. The first section of this Chapter will deal with the framework directive. The second section will describe the legal framework for electronic road tolling.

2.2 ITS Framework Directive 2010/40/EU

2.2.1 Introduction

On the 6th of August 2010 Directive 2010/40/EU was published in the Official Journal of the European Union. This Directive is entitled: Directive 2010/40/EU of the European Parliament and the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for the interface with other modes of transport[34]. As is clear from the name, the Directive is a *framework Directive* for the deployment of ITS in Europe. ITS, for the purposes of the Directive, refers to the application of information and communication technologies in the field of road transport and its interfaces with other modes of transport[35]. The Directive distinguishes between ITS applications and services. An ITS application is an operational instrument for the use of ITS[36]. An ITS service is defined as the provision of an ITS application through a well-defined organisational and operational framework with the aim of contributing to user safety, efficiency, comfort and/or to facilitate or support transport and travel operations[37]. One example of such a service is OnStar[38], developed by General Motors (GM). GM provides an on-board unit in its vehicles through which a range of services controlled by a service centre can be provided, such as remote door-unlock, routing or emergency assistance requests. The OnStar-unit itself could be considered as a "platform" in the 2010/40/EU sense.[39]

[34] *O.J.* 06.08.2010, L 207
[35] Art. 4(1) 2010/40/EU
[36] Art. 4(3) 2010/40/EU
[37] Art. 4(4) 2010/40/EU
[38] http://www.onstar.com
[39] Defined as: "an on-board or off-board unit enabling the deployment, provision, exploitation and integration of ITS applications and services".

For a number of years the Commission has been promoting the adoption of a pan-European in-vehicle emergency call system that would bring rapid assistance to accidents involving vehicles. The essential function of the proposed "e-Call" system[40] is that, in the event of an accident, the eCall device in the car will transmit an emergency message that automatically alerts the nearest emergency service to the occurrence and location of the accident. Other information that may be provided as part of the message could include the medical history of the driver and the likely severity of the accident. Although an eCall message could be triggered manually, the intention is that the car will send the message automatically in the case of a severe accident. The life-saving features of eCall are the automatic transmission of the call for assistance and provision of detailed information concerning the location of the accident site. Consequently, the proposed eCall system should achieve a drastic reduction in the time taken to rescue and treat the casualties, thereby enhancing the survival of road accident victims. Such a system would also constitute a "platform" in the 2010/40/EU sense.

2.2.2 Coordinated and coherent deployment

2.2.2.1 Standards and Specifications

According to the European Commission the current national initiatives in the area of ITS are fragmented and uncoordinated and lack the means to provide geographic continuity throughout the Union[41]. To redress the situation a European Directive is necessary[42]. This Directive is meant to support a coherent and coordinated deployment of ITS throughout Europe. To achieve this coherent and coordinated deployment the Commission relies on standards[43] and specifications[44]. A standard is defined as follows:

> *A technical specification approved by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory and which is one of the following:*
> - *International standard: a standard adopted by an international standardisation organisation and made available to the public;*
> - *European standard: a standard adopted by a European standardisation body and made available to the public;*
> - *National standard: a standard adopted by a national standardisation body and made available to the public.*

Compliance with a standard is voluntary. In this respect it differs from a specification, which is defined as follows:

[40] COM (2005) 431, "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: The 2nd eSafety Communication – Bringing eCall to Citizens", 14/9/2005

[41] Recital 6 2010/40/EU

[42] Recital 6 2010/40/EU

[43] Standard as defined in Article 1(6) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations

[44] A binding measure laying down provisions containing requirements, procedures or any other relevant rules

A binding measure laying down provisions containing requirements, procedures or any other relevant rules.

Unlike a standard a specification is binding. There is no choice as to whether to apply it or not, while one can choose whether or not to apply a (voluntary) standard. Another important difference between standards and specifications is who issues them. Standards have to come from a recognized standardisation body such as CEN or CENELEC or a comparable national organisation. Specifications are issued by the European Commission. The objective is to adopt these specifications between 2010 and 2017 to address the compatibility, interoperability and continuity of ITS solutions across the EU. The first priorities will be traffic and travel information, the eCall emergency system and intelligent truck parking.

To further enhance the coherent deployment coordination should take place with other existing committees dealing with related domains such as the European Electronic Toll Service (EETS) committee and INSPIRE on geographic data exchange[45]. This prevents conflicts and disparities with existing Union regulations and initiatives in related domains.

2.2.2.2 Delegated acts

2.2.2.2.1 Competent Body

Specifications require authority to impose generally binding rules. Therefore the European Commission has – for a restricted period of time[46] - been authorised to issue *delegated acts* in relation to specifications[47]. This means that the Commission has the authority to set out binding rules to ensure compatibility, interoperability and continuity for the deployment and operational use of ITS. To support the Commission on these delegated acts two committees have been foreseen in 2010/40/EU[48]. In the first instance the Commission will be assisted by the European ITS Committee as part of the so-called *comitology* procedure foreseen in Directive 2010/40/EU. Additionally the Commission should establish a European ITS Advisory Group[49]. This Advisory Group should consist of all relevant stakeholders such as industry, consumer organisations and other relevant fora. The purpose of this Group is to assist on technical and business issues with regard to the use and deployment of ITS in the Union. This should reconcile the interests of both the Union and the public in the development and deployment of ITS.

[45] Recital 22 2010/40/EU

[46] The power to adopt the delegated acts referred to in Article 7 has been conferred on the Commission for a period ending on 27 August 2017.

[47] Art. 7 2010/40/EU

[48] Art. 15 2010/40/EU

[49] Art. 16 2010/40/EU ; the ITS Advisory Group has been set up by the Commission Decision of 4 May 2011, published in the *Official Journal (O.J.)* C135 of 5 May 2011. It is composed of 25 members and chaired by a representative of the European Commission.

2.2.2.2.2 Objection and Revocation

The delegated acts are, however, not an autonomous competence of the Commission. The Council and the European Parliament can *object* to a delegated act and thus exercise control over delegated acts. Thereto the Commission is required to notify a delegated act as soon as it has been adopted. As of the date of notification the European Parliament and the Council have two months to object to the delegated act, a period extendable by another two months on the initiative of either the Council or the European Parliament. After expiration of this period, and if neither the European Parliament nor the Council express objections, the delegated act may be published in the Official Journal[50]. If either one objects, the delegated act shall not enter into force[51]. The body expressing the objection is also required to state the reasons for this objection. Consequently a delegated act only enters into force two months after adoption if both the Council and the European Parliament notify the Commission they do not wish to object to the delegated act.

The authority to adopt delegated acts can also be *revoked or restricted* by the Council or the European Parliament. The body initiating the procedure of revocation notifies the other bodies within a reasonable period of time prior to making the final decision. Additionally, the body also notifies which competences it wishes to see revoked or restricted and the related arguments. It would appear as if this provision intends to include some form of prior consultation between the Commission, the Council and the European Parliament to discuss the issue. The Commission has a right to be heard before its powers are revoked. If a decision to revoke delegation is taken the decision enters into force immediately or at the date specified in the decision. However the revocation does not affect delegated acts that have already entered into force. It only affects the future, not the past. While the Commission is given a quite broad competence it is reasonable to conclude that effective methods for supervision of delegated acts exist. But the decision on the use of these methods rests entirely with the Council or the European Parliament. Consequently the effective impact of this supervision remains yet to be seen.

2.2.2.2.3 Criticism with regard to data protection

The European Data Protection Supervisor (EDPS) is of the opinion that while in principle there is no objection against delegated acts, they cannot be used if they would touch upon the protection of privacy and personal data of individuals[52]. The EDPS refers to art. 8.2 ECHR which states that the right to privacy of an individual can only be restricted by law and when necessary in a democratic society. A law requires the intervention of a representative body which the Commission is not because it is not established based on general elections. There-

[50] Art. 14.2, 2010/40/EU
[51] Art. 14.3, 2010/40/EU
[52] Opinion of 22 July 2009 on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, *OJ* 25.02.2010, C 47, nr. 23-25

fore delegated acts cannot be used in matters relating to privacy and data protection. Such matters require the involvement of the European Parliament.

As was described in the previous section, Directive 2010/40/EU incorporates possibilities to limit the use of delegated acts. But there is no requirement for supervision in relation to delegated acts. Therefore it is unclear how the European Parliament and the Council will use their competence in this matter and thus whether there will be an effective oversight of the use by the Commission of the power to issue delegated acts.

2.3 Union Rules on Electronic Road Tolling

Electronic Road tolling already benefits from a dedicated legal framework. This framework consists of Directive 2004/52/EC[53] and a Commission Decision 2009/750/EC[54] detailing the provisions of the Directive. The concept underlying the legal framework is that users subscribe to a service offered by a service provider and that as a result they gain access to toll roads in the Union without having to conclude contracts with the different road operators. The service provider acts as a link between the user and the road operators.

2.3.1 Directive 2004/52/EC

2.3.1.1 Scope

The scope of Directive 2004/52/EC is to ensure interoperability of electronic road tolling systems in the Union. Directive 2004/52/EC does not intend to impose electronic road tolling. The only goal is to make sure that *when* electronic toll schemes are introduced it does not require the road user to obtain several toll units to circulate on the Union road network. The Directive applies to *electronic collection* of all types of road fees on the entire Community road network[55]. Electronic collection at bridges, tunnels and ferries is targeted as well. Three situations fall outside the scope of this Directive[56].

The first one is, evidently, a road tolling system for which no electronic means of collection exists. This corresponds to the scope of 2004/52/EC which covers interoperability of *electronic* toll systems.

The second is electronic road tolling systems that do not need the installation of on-board equipment. The London Congestion Charge (LCC) is such an example because it functions using Automatic Number Plate Recognition cameras installed on gantries spanning the road. These register the license plate of the vehicle and this registration serves as the basis for tolling. This exemption appears reasonable since the issues regarding interoperability concern

[53] Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community, *O.J.* 30/04/2004, L 166, p. 124-143

[54] Commission Decision 2009/750/EC of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements (notified under document C(2009) 7547), *OJ* 13.10.2009, L 268, p. 11–29

[55] Art. 1, 2004/52/EC, contrary to further in the deliverable, we make no distinction between material and geographic scope

[56] Art. 1.2., 2004/52/EC; Opinion of the Committee of the Regions, *OJ* C 73, position 4.4 and recommendation 3

electronic toll systems requiring on-board equipment, because it is the on-board equipment that puts the burden on the user. The user is responsible for obtaining the equipment and ensuring its proper operation. It is also this on-board equipment that lacks harmonization and requires users to contract with various road operators if one wishes to benefit from the advantages presented by electronic road tolling. Additionally it should be pointed out that some electronic toll schemes are mandatory, such as the German Toll-Collect for trucks. While the use of on-board equipment is not required, the majority of trucks on German roads use it for reasons of convenience[57]. And if one circulates on roads subject to different mandatory toll schemes with proprietary on-board equipment this increases the burden on the road user.

Finally, small - strictly local - road toll systems, for which compliance costs engendered by the Directive would be disproportionate to the benefits, are also exempted from the scope. It is however still unclear what toll systems would be covered by this exemption or what criteria determine the strictly local character.

2.3.1.2 Interoperability

The primary goal of the Directive is to guarantee interoperability of road tolling systems at the contractual, technical and procedural level[58]. This shall be done and supervised by a European Electronic Toll Service (EETS) that has to be set up according to the rules of the Directive[59]. Commission Decision 2009/750/EC describes this in more detail and will be discussed in section 2.3.2 below. This service should encompass all roads in the Community on which road usage fees are collected electronically taking into account the exemptions described in section 2.3.1.1 of this deliverable. EETS only has authority over the method of toll collection: the modalities of the toll levied by the Member States remain under the authority of the Member State and more specifically the Toll Charger[60]. This is discussed in section 2.3.2.2.2 below. The features of the European service are based on the items enumerated in the Annex to the Directive and deal with the technical procedural and legal issues of EETS[61]. Most of these issues are addressed by Decision 2009/750/EC, which is discussed in section 2.3.2 below.

On the technical side, interoperability is guaranteed by restricting the choice of technology to three possibilities or a combination thereof[62]:

1. satellite positioning (GPS, Galileo, Glonass…),
2. mobile communications using the GSM-GPRS standard (reference GSM TS 03.60/23.060),
3. 5.8 GHz microwave technology (often referred to as DSRC).

Dedicated short-range communications (DSRC) are one-way or two-way short- to medium-range wireless communication channels and a corresponding set of protocols and

[57] Toll Collect, *Mobilität fur Morgen, Chancen fur Verkehr, Wirtshaft und Umwelt,* Unternehmenbrochure, website Toll Collect Presse-section
[58] Recital 13, 2004/52/EC
[59] Art. 3-4, 2004/52/EC
[60] Art. 3.2., 2004/52/EC
[61] Art. 4.1., 2004/52/EC
[62] Art. 2.1., 2004/52/EC

standards specifically designed for automotive use. The United States Federal Communications Commission (FCC) allocated 75MHz of spectrum in the 5.9 GHz band for DSRC to be used by Intelligent Transportation Systems ITS in the US. In Europe the European Telecommunications Standards Institute (ETSI) has allocated 30 MHz of spectrum in the 5.9 GHz band for ITS. The decision to use these frequencies is due to the spectral environment and propagation characteristics, which are suited for vehicular environments. These frequencies can offer high data rate communications over distances up to 1 km with low weather dependence. The main use in Europe and Japan is currently in electronic toll collection.

In Directive 2004/52/EC a preference for a combination of satellite positioning and GSM/GPRS technology is expressed[63]. Because of its greater flexibility and versatility this combination should allow for the best fulfilment of the requirements of the new road tolling policy of the Community and the Member States. This technology should also facilitate the implementation of other technologies in the OBE, on condition that this does not constitute an additional burden on them or cause discrimination between these additional services[64]. This is primarily aimed at a combination with the digital *tachograph*[65] or eCall capabilities. It could, however, be expanded to other technologies such as routing or other applications that could be helpful when using a motorized means of transport.

Throughout the adoption process of the Directive, there have been dissenting opinions within the EU regarding the restriction on technological choice. The Committee of the Regions was of the opinion that the choice of technology should not be restricted too much since this could disadvantage other, possibly cheaper and more efficient, technologies[66]. Reference was made to the London Congestion Charge (LCC), which uses cameras and license plate recognition. The main problem with a system such as LCC is that it requires a considerable investment in roadside infrastructure, and that it may not be practicable to cover the road network of a Member State. The main argument against systems similar to LCC and in favour of GSM/GPS is that the latter does not require considerable investment in infrastructure. The GPS signal is readily available to anyone with a GPS receiver and GSM/GPRS networks are operational in all Member States and already cover almost the full territory of the Union. The announcement of a Public Regulated Service for Galileo providing encrypted positioning signals to counter spoofing and other potential security issues should increase the reliability of satellite positioning[67]. However, the Committee is of the opinion that the preferred option of combined GPS-GSM technology has yet to prove its value. Furthermore, the Committee considers that interoperability can be achieved through other methods than restricting the choice of technology. Therefore they recommended that Recital 8 of the Com-

[63] Recital 8, art. 2.3. 2004/52/EC; Council Common Position of 22 March 2004, *OJ* C 95 E, Recital 8

[64] Art. 2.4, Recital 11 2004/52/EC; Council Common Position of 22 March 2004, *OJ* C 95 E, Recital 8; Council Resolution of 17 June 1997, *OJ* C 194, II-3

[65] A *tachograph* is a device fitted to a vehicle that automatically records its speed and distance, together with the driver's activity selected from a choice of modes. The drive mode is activated automatically when the vehicle is in motion, and modern tachograph heads usually default to the other work mode upon coming to rest. The rest and availability modes can be manually selected by the driver whilst stationary. The EEC Regulation 3821/85 from December 20, 1985 made tachographs mandatory throughout the Union as of September 29, 1986.

[66] Opinion of the Committee of the Regions, *OJ* C 73, position 5

[67] European Commission, DG Enterprise and Industry, "Galileo: Secure Satellite Navigation for emergency and security services", 08/10/2010, DG Website Newsroom: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?item_id=4606 (accessed 08/08/2011)

mission proposal for the Directive be taken out[68]. The Commission did not agree with this and maintained the recital. Their main reason for disregarding this request is that current systems using Dedicated Short-Range Communication (DSRC) 5.8 GHz microwave technology are not interoperable because of a lack of standardization[69]. The Commission is also of the opinion that DSRC will not meet the requirements because of its age; in 2008 the technology already dated back 30 years. In addition, a non-negligible disadvantage of DSRC is that there is a need for extensive infrastructure and this requires considerable investment. Moreover, these costs increase with the area to be supervised and could therefore be prohibitive and consequently prevent the introduction of electronic toll schemes. Furthermore, the Commission feared that new experiments using DSRC would endanger interoperability. Consequently, the Commission retained its preference for a GPS-GSM/GPRS based technology, despite significant advances in DSRC technology in recent times[70].

2.3.2 Commission Decision 2009/750/EC

2.3.2.1 Introduction

The EETS is further defined in Commission Decision 2009/750/EC. The goal of the EETS is to allow citizens of the Community to adhere to a single service provider for access to all toll domains and the associated electronic tolling. The service provider is the *EETS provider* ("Provider"). A *toll domain* is an area where a toll is levied according to a certain toll regime subject to conditions of the EETS. The *toll regime* is the set of rules, including enforcement, governing the collection of toll on the toll roads. The entity responsible for the toll regime is the *toll charger*. The Toll Charger is a private or public organization which levies tolls for the circulation of vehicles in an EETS domain. This Toll Charger can be a separate entity, but it can also be part of an organization that acts as a Provider. However, if the entity takes up both roles there must be separate profit and loss accounts and separate balance sheets for each activity to allow an accurate cost-benefit analysis per activity. There may also be no cross-subsidies between the two activities of Provider and Toll Charger. This means that each activity must be responsible for its own resources, and that resources cannot be transferred from one entity to another to support the other entity's activity.

The decision also foresees the possibility of pilot toll systems. This should allow the development of new systems. But the Commission must give its approval to the pilot before Member States can grant authorisation. This authorisation shall initially be limited to 3 years. Providers are not required to take part in these pilots but are allowed to.

---

[68] Recital 8, 2004/52/EC: "*In particular, owing to their great flexibility and versatility, application of the new satellite positioning (GNSS) and mobile communications (GSM/GPRS) technologies to electronic toll systems may serve to meet the requirements of the new road-charging policies planned at Community and Member State level. (…)"*

[69] Proposal for a Directive of the European Parliament and of the Council on the widespread introduction and interoperability of electronic road toll systems in the Community /* COM/2003/0132 final - COD 2003/0081 */, Chapter II.7

[70] Communication from the Commission to the European Parliament pursuant to the second subparagraph of Article 251 (2) of the EC Treaty concerning the common position of the Council on the adoption of a Directive of the European Parliament and of the Council on the interoperability of electronic road toll systems in the Community, /* COM/2004/0222 final - COD 2003/0081 */, nr. 3

2.3.2.2 Actors of EETS and their duties

2.3.2.2.1 EETS Providers

2.3.2.2.1.1 Eligibility Requirements

The decision outlines different rights and obligations of the EETS Providers. They must conclude EETS contracts covering all EETS domains within 24 months after registration as Provider in a Member State. To receive this registration they must meet the criteria set out in the Commission Decision[71]:

> *(a) Hold EN ISO 9001 certification or equivalent;*
>
> *(b) Demonstrate having the technical equipment and the EC declaration or certificate attesting the compliance of the interoperability constituents as laid down in Annex IV(1) to the present Decision;*
>
> *(c) Demonstrate competence in the provision of electronic tolling services or in relevant domains;*
>
> *(d) Have appropriate financial standing;*
>
> *(e) Maintain a global risk management plan, which is audited at least every 2 years;*
>
> *(f) Be of good repute.*

Some of these criteria are relatively easy to demonstrate such as holding an EN ISO 9001 certificate. The requirements 'appropriate financial standing' and 'good repute' are on the contrary unclear. Clarification could be provided by application guidelines that have yet to be published. Providers must inform Users of the coverage of their toll domains and of any changes thereto. This can be done by posting the list on a website. Every year Providers must declare the extent of their EETS domains coverage to the Member State of registration.

The Providers also have a duty to cooperate with the Toll Chargers regarding enforcement efforts. The principle of EETS is that there is minimal direct contact between the Toll Charger and the User. The Provider operates as a "go-between" and, unlike the Toll Charger, holds detailed information on the User. This includes information that is required for enforcement. Consequently, the cooperation of the Provider is indispensable to the Toll Charger to enforce his toll policy.

2.3.2.2.1.2 On-board Equipment

2.3.2.2.1.2.1 Provision

Providers must provide the users with *On-Board Equipment* (OBE) which complies with the relevant technical requirements. The Provider has to prove compliance of the OBE. It is, however, not specified how this equipment must be provided. This leaves room for structures such as sale, lease and tied selling.

[71] Art. 3, 2004/52/EC

2.3.2.2.1.2.2 Operation

In addition, the Provider must also monitor the performance of their service level. Consequently they must continuously monitor the operation of their service to ensure correct operation. Correspondingly they must also provide audited processes that provide appropriate measures to be taken when performance problems or integrity breaches are detected. This means that Providers have to assess possible issues in advance and draft scenarios on how to deal with these issues in case they present themselves. This is comparable to the work on "Dark-Side Scenarios" outlined in deliverable D2.3 of the EVITA-project[72]. The Providers must also monitor the operational status of the OBE of the User. This means that they are allowed to check whether the OBE is switched on when it should be and whether it functions correctly. However this requirement does not allow the Provider to read or download the tolling data inside the OBE. In case the OBE is found not to be operational or malfunctioning, it must be put on a list of invalidated equipment, taking into account Community rules on data protection. This list of invalidated equipment has to be distributed to all Toll Chargers to which the Provider is connected through agreement. This transmission releases the Provider from liability for tolls charged to the equipment listed as invalidated and notified as such to the Toll Charger. This will be discussed further in section 2.3.2.2.2.3 of this deliverable.

2.3.2.2.1.2.3 OBE Set-up

Providers are responsible for the fixed vehicle classification parameters stored in the OBE or the Provider's information system. Additionally Providers are also responsible for the correct personalization of the OBE using the personal data as provided by the EETS User. Furthermore, variable parameters that have to be introduced by in-vehicle intervention shall be configurable by the User through an appropriate Human-Machine Interface (HMI). This HMI shall remain the same regardless of the toll domain the User circulates in. An existing example of such a variable parameter is the number of axles of the trailer that a truck is pulling. This parameter is currently used in Germany by Toll-Collect. This could imply that the OBE notifies the User of the required parameters and allows for an easy input of this data by the User.

2.3.2.2.1.3 User invoice

The Provider is responsible for invoicing. The invoicing of individual users shall clearly separate the service charges of the EETS Provider and the tolls incurred. With regard to tolls the invoice should specify at least the time and location where the tolls were incurred and the user-relevant composition of specific tolls. This last aspect refers to parameters of regimes such as the German *LKW-Maut*, where the number of axles determines the toll amount or the LCC where different charges exist for different groups such as residents or commuters. The User can however ask for different specifications to be mentioned in his invoice. The elements mentioned in the Decision are only the standard requirements.

EETS Providers must inform Users as quickly as possible of any situations regarding non-declaration of tolls and offer a possibility of rectifying the situation before taking enforcement

[72] A. Ruddle *et al.*, "Security requirement for automotive on-board networks based on dark side scenarios", Deliverable D2.3 of EVITA, 2009

action. This duty of notification follows from the requirement that the provider must monitor the operational status of the User's OBE.

2.3.2.2.2 Toll Chargers

2.3.2.2.2.1 Ensure interoperability

Primarily Toll Chargers must take action to ensure compliance with technical and procedural EETS interoperability conditions set forth by Directive 2004/52/EC and Decision 2009/750/EC. In case problems arise, the Toll Charger shall assess the problem with the stakeholders involved, and take remedial action to ensure that interoperability is maintained. Evidently, the Toll Charger is only responsible for solving problems that fall within his area of responsibility. He must make sure that his operation is compliant with the interoperability requirements. Furthermore, he must accept all certified equipment from Toll Chargers he has contracted with. But if the issue preventing interoperability lies for example with the OBE, the Provider will be responsible for solving the issue since he is responsible for providing the OBE and for ensuring its compliance.

2.3.2.2.2.2 Domain Statement

Toll Chargers must develop and maintain a *domain statement* setting out the general conditions for Providers for accessing their toll domains. The domain statement could be viewed as the terms and conditions for Providers to contract with the Toll Charger. This statement must include at least the toll transaction policy, procedures and service level agreement, invoicing policy, payment policy and commercial conditions. These commercial conditions should be agreed upon through bilateral negotiations between Toll Charger and Provider and should also include service level requirements.

The Toll Chargers shall accept, on a non-discriminatory basis, any Provider requesting to provide toll services on the domain(s) under the Toll Chargers responsibility. Non-discriminatory refers to the fact that all applicants must be subject to similar conditions unless there are reasons for awarding different conditions to specific Providers. This corresponds to the realization of the Common Market in the EU where all actors should benefit from a level playing field regardless of their nationality. Acceptance shall be governed by compliance to the domain statement with the objective to complete negotiations within 24 months after the Provider has been registered in a Member State. If an agreement cannot be reached the matter may be conferred upon a conciliation body responsible for the relevant toll domain. The conciliation body will be discussed later.

2.3.2.2.2.3 OBE

Toll Chargers shall accept any operational OBE from Providers they have contractual relationships with and which have been certified according to the rules set out for conformity to specifications and suitability for use and interoperability of constituents[73]. Toll Chargers do not have to accept OBE that appears on the list of invalidated equipment. Correspondingly, Providers are not liable for tolls relating to users using invalidated OBE notified to the Toll

[73] Annex IV 2009/750/EC

Charger. If a Toll Charger knows that a specific OBE has been invalidated the Toll Charger is responsible for obtaining the tolls from that User and not the Provider.

Toll Chargers shall keep on their website a list of all Providers with whom they have a contract and whose OBE is accepted as a consequence. A parallel requirement can be found for Service Providers who must notify of the toll domains that they can provide access to. A Toll Charger may require a Provider's collaboration in order to perform unannounced and detailed toll system tests involving vehicles either circulating or having recently circulated on the Toll Charger's toll domain. This has been discussed above under the Provider's obligations. The number of vehicles submitted to such tests over a year shall be commensurate with the yearly average traffic or traffic projections of the Provider on the Toll Charger's domain(s).

For an EETS dysfunction that is attributable to the Toll Charger, the Toll Charger shall provide for a degraded mode of service enabling vehicles to circulate safely with a minimum of delay and without being considered as toll evaders.

2.3.2.2.2.4 Toll Context data

There are also rules relating to *toll context data* (TCD). TCD means the information defined by the responsible Toll Charger that is necessary to establish the toll due for circulating in a vehicle on a particular toll domain and conclude the toll transaction. Changes to TCD must be notified by the Toll Chargers to the Member State(s) in which their toll domains are located, relating to amongst others definition of the toll domain, nature of toll and levy principles, vehicles liable to toll, vehicle classification parameters and toll declarations required.

The toll shall be determined by the Toll Charger according to - amongst others - vehicle classification. Vehicle classification in turn shall be determined according to the parameters described in Decision 2009/750/EC. The set of vehicle classification parameters to be supported by EETS shall not restrict the choice of tariff schemes by the Toll Chargers. EETS shall have the flexibility to allow the set of classification parameters to evolve according to foreseeable future needs. What can be used as vehicle classification parameters is also strictly defined by the decision:

(a) any measurable vehicle parameter that can be unambiguously measured by its road side equipment;

(b) any vehicle parameter that is supported by standard EN15509 and ETSI ES 200674-1 and its related Technical Reports for protocol implementation;

(c) the vehicle parameters which are mandatory in vehicle registration documents and as standardised in CEN ISO/TS24534.

(d) the variable vehicle classification parameters currently used in toll systems, e.g. number of axles (including lifted axles), presence of a trailer…;

(e) the following environmental parameters;

- the vehicle's emission class, i.e. its environmental category in accordance to Directive 88/77/EEC and Directive 2006/38/EC ;
- a harmonised CO2 related parameter, e.g. the harmonised community code V.7 in vehicles registration documents.

When circulating in a toll domain, the vehicle OBE shall be able to communicate its vehicle classification parameters and OBE status information to the toll-declaration monitoring equipment of the toll charger. New vehicle classifications could also be introduced. These require a notification to the Commission, to be carried out by the Member State of registration of the Toll Charger, who shall refer the matter to the Electronic Toll Committee that delivers its opinion within six months. A new tariff scheme based on a tariff already in use in at least one EETS toll domain shall be supported by Providers as of the date of its entry into force. This means that Providers must make all necessary technical and operational arrangements so their Users can access the toll domains concerned, regardless of whether their users circulate on those domains.

2.3.2.2.3 EETS User

2.3.2.2.3.1 Choice of Provider

The rights and obligations of EETS Users are also defined in the Decision. The User is free to choose his Provider. When entering into a contract the User shall be informed about the processing of their personal data and the rights stemming from applicable legislation on the protection of personal data. The User must ensure that the user and vehicle data provided to the EETS provider are correct. Previously it has been mentioned that the Provider is responsible for personalizing the OBE. Consequently the Provider cannot be held responsible for erroneous data in the OBE when the error lies with the User.

2.3.2.2.3.2 OBE

The User must also ensure that the on-board equipment is operational whilst the vehicle is circulating in an EETS domain. Therefore Users shall operate their OBE in accordance with EETS provider's instructions; in particular as these apply to the declaration of variable vehicle parameters. For this declaration an intelligible HMI must be foreseen, yet the responsibility for providing the parameters lies entirely with the User. The Provider can in principle not be held responsible for erroneous data input by the User.

2.3.2.2.3.3 Toll Payments

The User is obviously responsible for paying the tolls he owes as notified to him by the invoices sent by his Provider. But instead of paying them to the Toll Charger who gives him access to his toll domain, as is currently the case in France for example with the toll plazas installed on motorways, the User pays the Provider. The Provider acts as a relay between Toll Charger and User. The Provider notifies the User of the amount of the tolls that he owes. The User pays the Provider who then transfers the money to the Toll Charger. Payment of toll fees by a user to his Provider shall be deemed as fulfilling the User's obligation to pay towards the relevant Toll Charger. This appears logical since the User only has a contract with the EETS Provider. That contract gives the User the possibility to circulate freely on all EETS domains covered by his EETS Provider without having to conclude a contract with every toll operator of every toll domain he circulates on. This is in keeping with the goal of the single service set forth by Directive 2004/52/EC.

2.3.2.2.4 Conciliation Body

The decision also instates a Conciliation Body which should be established in every Member State[74]. This body should facilitate mediation between Toll Chargers with a toll domain located within the territory of the Member State and Providers who have contracts or are in contractual negotiations with those Toll Chargers. This means that it can be called upon both prior to concluding the contract and for disputes arising in execution of a contract between a Toll Charger and a Provider. The body shall be especially empowered to verify whether the contractual conditions imposed by a Toll Charger on different Providers are non-discriminatory and a fair reflection of the costs and risks of the parties to the contract. This non-discriminatory aspect has already been highlighted when discussing the domain statements in section 2.3.2.2.2.2 of this deliverable.

A Member State shall take the necessary measures to ensure that the organisation and legal structure of its Conciliation body are independent from the commercial interests of Toll Chargers and Providers. The request to intervene should come from a Toll Charger or a Provider for any dispute relating to their contractual relations or negotiations. The body must state within one month following the receipt of a request whether it has the necessary documents in its possession. The Member State shall empower the body to request all relevant information from Toll Chargers, Providers and any third parties active in the provision of EETS within that Member State. The body shall issue its opinion no later than six months after receiving the request for intervention. It is unclear what the actual power of this opinion is. It would appear that it is not binding, which would conform to the status of the Conciliation body as a mediator between parties. His duty would be more reconciling the differing views of the actors in the dispute rather than deciding who is right and who is wrong. In this regard it is important to stress the independence requirement mentioned earlier in this section.

2.3.2.2.5 Supervisory Bodies

In each Member State a body or bodies should be entitled to carry out or supervise the procedure for the assessment of the conformity to specifications or suitability for use of interoperability constituents. It or they shall be notified to the Commission and the other Member States, along with their identification numbers obtained from the Commission. The Commission shall publish the list of bodies, their identification numbers and field of competence in the Official Journal. The Commission shall keep this list updated. The bodies shall comply with the following list of minimum criteria:

a) The body shall be accredited according to the EN 45000 series of standards.
b) The body and the staff responsible for the checks must carry out the checks with the greatest possible professional integrity and the greatest possible technical competence and must be free of any pressure and incentive, in particular of a financial type, which could affect their judgement or the results of their inspection, in particular from persons or groups of persons affected by the results of the checks.

[74] Art. 10, 2009/750/EC

c) The body, its Director and the staff responsible for carrying out or supervising the checks may not become involved, either directly or as authorised representatives, in the design, manufacture, construction, marketing or maintenance of the interoperability constituents or in their use. This does not exclude the possibility of an exchange of technical information between the manufacturer or constructor and that body.
d) The body must possess or have access to the means required to perform adequately the technical and administrative tasks linked with the checks.
e) The staff responsible for the checks must possess:
   - proper technical and vocational training
   - a satisfactory knowledge of the requirements relating to the checks that they carry out and sufficient practice in those checks
   - the ability to draw up the certificates, records and reports which constitute the formal record of the inspections conducted
f) The independence of the staff responsible for the checks must be guaranteed. No official must be remunerated either on the basis of the number of checks performed or of the results of those checks.
g) The body must take out civil liability insurance unless that liability is covered by the State under national law or unless the checks are carried out directly by that Member State.
h) The staff of the body is bound by professional secrecy with regard to everything they learn in the performance of their duties (with the exception of the competent administrative authorities in the State where they perform those activities) in pursuance of Directive 2004/52/EC and this Decision or any provision of national law implementing the Directive.

If the supervisory body no longer meets these criteria, the Member State shall immediately withdraw the approval and notify the Commission and the other Member States of this decision. The Commission of other Member States can also challenge the competence of the notified body by referring the matter to the Electronic Toll Committee who shall deliver an opinion within 3 months after receiving the request. The Commission shall inform the concerned Member State of the measures required to uphold the status of the notified body.

These notified bodies shall be included in a Coordination Group set up as a working group of the Electronic Toll Committee. The Coordination Group shall compile and maintain a comprehensive list of standards, technical specifications and normative documents against which EETS interoperability constituents' conformity to specifications and suitability for use can be assessed. The Coordination Group shall serve as a forum for discussing any problems that may arise in relation to the conformity to specifications and suitability for use assessment procedures and for proposing solutions to these problems.

2.3.2.2.6 Public electronic register

All Member States must keep a public electronic register for the following:[75]

(a) The EETS domains within their territory, including information relating to:

[75] Art. 19, 2009/750/EC

– *the corresponding Toll Chargers,*

– *the tolling technologies employed,*

– *the Toll Context Data,*

– *the EETS domain statement,*

– *the EETS Providers having EETS contracts with the Toll Chargers active in their area of competence.*

(b) The EETS Providers to whom it has granted registration according to Article 3.

Modifications to Toll Chargers registers shall be entered immediately after adoption, where necessary indicating the date of entry into force. In case a Toll Charger intends to introduce new vehicle classification parameters, the Member State where the Toll Charger is registered shall inform the Commission and the other Member States. The Commission shall refer the matter to the Electronic Toll Committee and deliver its opinion within six months, in accordance with the procedure referred to in Article 5(2) of Directive 2004/52/EC. Where a new tariff scheme is based on vehicle classification parameters already in use in at least one EETS domain, Providers shall support the new tariff scheme as of the date of its entry into force.

These registers have to be available within 9 months after the date of entry into force of decision 2009/750/EC. The decision entered into force on 14 October 2009. At the end of each calendar year, the authorities in charge of the registers on EETS domains and Providers shall communicate the registers to their counterparts in other Member States and to the Commission.

2.3.2.3 EETS Service

2.3.2.3.1 Introduction

2009/750/EC describes a series of general and specific requirements. The specific requirements are divided into single continuous service, security and privacy requirements, an extensive part on infrastructure requirements, and another on management and operational requirements.

2.3.2.3.2 General requirements

The general requirements can be summed up as follows. Devices intended to be handled by the Users must be designed to comply with product safety regulations. The design of the EETS must be such as to enable the system to continue its mission in case of malfunction or failure of components, possibly in a degraded mode, with a minimum delay for EETS Users. The OBE must also fulfil the rules on Electro-Magnetic Compatibility with installations, equipment or private networks with which they might interfere. When interfacing within the framework of EETS, the technical characteristics of the Provider's equipment and the Toll Charger's equipment must be interoperable.

2.3.2.3.3 Single Continuous service

EETS stands for a single continuous service.[76] This means first of all that once the vehicle classification parameters have been stored and/or declared then no further in-vehicle human intervention is required during a journey unless there is a modification to the vehicle's characteristics.

Secondly, it means that human interaction with a particular piece of OBE shall remain the same whatever the EETS domain. This means that the User shall have the same interface for all toll domains.

2.3.2.3.4 Security Requirements

EETS shall provide the means to protect stakeholders against fraud or abuse. EETS is also responsible for security features relative to the protection of data stored, handled and transferred between stakeholders in the EETS environment. The security features shall protect the interests of EETS stakeholders from harm or damage caused by lack of availability, confidentiality, integrity, authentication, non-repudiation and access protection of sensitive user data appropriate to a European multi-user environment. To this aspect of security the EVITA consortium could offer a valuable contribution.

2.3.2.3.5 Interoperability requirements

2.3.2.3.5.1 Infrastructure

2.3.2.3.5.1.1 Common Communication Protocols

Common communication protocols shall be implemented between Toll Chargers and Provider's equipment. EETS shall provide means for Toll Chargers to easily and unambiguously detect whether a vehicle circulating in their toll domain and allegedly using EETS is actually equipped with validated and properly functioning OBE providing truthful information. The OBE shall provide the means for Toll Chargers to identify the responsible Provider. Additionally, the OBE shall regularly monitor this feature, invalidate itself if an irregularity is detected and, where possible, inform the Provider of the anomaly. This means that the OBE has to be designed with diagnostic facilities.

For technologies based on microwave technologies specific standards have to be supported. The OBE of EETS providers must support EN15509 and ETS ES 200674-1 and its related technical reports for protocol implementation. For the fixed and mobile roadside equipment of Toll Chargers the relevant standard is EN15509.

2.3.2.3.5.1.2 Global Navigation Satellite systems

For toll systems based on Global Navigation Satellite Systems (GNSS) EETS Providers shall monitor the availability of navigation and positioning satellite localisation data. Providers shall inform Toll Chargers of the difficulties they may experience in establishing toll declara-

[76] Art. 12, 2009/750/EC

tion data related to the reception of satellite signals. In this regard reference should be made to the phenomenon of the "urban canyon". Urban canyon is the term used to describe the effect of streets cutting through dense blocks of tall buildings, resulting in an urban environment that is similar to a natural canyon. Urban canyons have an impact on a variety of local conditions, including temperature, wind speed, air quality and radio reception (particularly for GPS signals). GNSS normally require line of sight between satellite and receiver to fix the location of the receiver. In built-up areas such as cities this line of sight may be hindered because of the presence of buildings. If the location of the OBE is unknown the OBE cannot collect the required data for the tolling scheme. Toll Chargers shall use the information received to identify problem areas and, where necessary, provide augmentation localisation signals such as EGNOS[77] (the European Geostationary Navigation Overlay Service), in agreement with Providers. This is very important with regard to non-repudiation of toll declarations. If GPS-based location information is used for toll calculation, an inaccurate GPS-signal is likely to lead to inaccurate toll calculations. The EGNOS system consists of three geostationary satellites and a network of ground stations, and supplements the GPS, GLONASS and Galileo systems by reporting on the reliability of positioning data and providing corrections to improve the accuracy of location information.

2.3.2.3.5.1.3 Fitment of OBE

The fitment of the OBE should comply with prescriptions in Directives 90/630/EEC[78] (forward vision) and 2000/4/EC[79] (interior fittings). Analysing this is, however, out of scope for this deliverable and will not be discussed any further.

2.3.2.3.5.1.4 Interfaces between Providers and toll chargers

There are two categories of interfaces between EETS Providers and Toll Chargers. Electronic interfaces between the EETS Provider's OBE and the Toll Charger's fixed or mobile equipment are the first category. The second category includes the interfaces between the respective back-offices.

The first category shall at least enable DSRC charging transactions, real-time compliance checking and localisation augmentation, where applicable. This last element refers to systems using GNSS and the associated mandatory assessments mentioned in section 2.3.2.3.5.1.2 of this deliverable. These three capabilities must all be present in the OBE. The Toll Charger on the contrary can choose to implement all capabilities or implement just one capability in his roadside equipment. In the aforementioned section 2.3.2.3.5.1.2 of this deliverable it is noted that the Toll Charger is only required to provide location augmentation in areas where GNSS signal reception is problematic. Correspondingly, he is not required to implement such a capability in areas where no such problems exist.

---

[77] ESA website: http://www.esa.int/esaNA/egnos.html

[78] Commission Directive 90/630/EEC of 30 October 1990 adapting to technical progress Council Directive 77/649/EEC on the approximation of the laws of the Member States relating to the field of vision of motor vehicle drivers, *O.J.* 6.12.1990, L 341, p. 20–29

[79] Directive 2000/4/EC of the European Parliament and of the Council of 28 February 2000 amending Council Directive 74/60/EEC on the approximation of the laws of the Member States relating to the interior fittings of motor vehicles (interior parts of the passenger compartment other than the interior rear-view mirrors, layout of controls, the roof or sliding roof, the backrest and rear part of the seats), *O.J.* 8.4.2000, L 87, p. 22–31

For the interactions between the respective back-offices there is a list of interfaces that have to be implemented by the EETS Provider and the Toll Charger. The interfaces are the following:

- *Exchange of toll declaration data between EETS Providers and Toll Chargers, specifically:*
- *Submission and validation of claims for toll payment based on DSRC charging transactions;*
- *Submission and validation of GNSS toll declarations.*
- *Invoicing or settlement;*
- *Exchange of information to support exception handling:*
- *In the DSRC charging process;*
- *In the GNSS charging process.*
- *Exchange of EETS blacklists;*
- *Exchange of trust objects;*
- *Sending of Toll Context Data from Toll Chargers to EETS Providers.*

The Toll Charger can, however, choose between DSRC and GNSS to decide which charging scheme he wishes to support, while the Provider has to foresee all possibilities. Previously in this deliverable it has been mentioned that the Providers are subject to the domain statement of the Toll Charger and have to support the TCD set forth by the Toll Charger. This under the caveat that the Provider is not discriminated against. These interface requirements are an example in practice of that general requirement imposed on the Provider.

2.3.2.3.5.2 Interoperability constituents

Interoperability constituents bearing the 'CE'-marking shall be considered by Member States as complying with the relevant essential requirements. For conformity assessment to specifications or the suitability for use of interoperability constituents (or both) the manufacturer of the constituents to be used in EETS provision, or his authorised representative, shall choose among the procedures laid down in Decision 768/2008/EC[80].

Interoperability constituents can bear 'CE'-marking if they are covered by 'EC' declarations of conformity to specifications or suitability for use or both. The content of the 'EC' declarations is also strictly defined:

- the name and address of the manufacturer, EETS Provider or the authorised representative established within the Community (give trade name and full address, in the case of the authorised representative, also give the trade name of the manufacturer or constructor);
- description of interoperability constituents (make, type, version, etc.);
- description of the procedure followed in order to declare conformity to specifications or suitability for use;
- all the relevant requirements met by the interoperability constituents and, in particular, their conditions of use;

[80] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, *O.J.* 13.08.2008, L218, p 82-128

- where applicable, name and address of the Toll Charger(s)or notified body(ies) involved in the procedure followed in respect of conformity to specifications or suitability for use assessment;
- where appropriate, reference to the technical specifications;
- identification of the signatory empowered to enter into commitments on behalf of the manufacturer or of the manufacturer's authorised representative established within the Community.

Directive 2009/750/EC holds a safeguard clause in relation to interoperability constituents[81]. Member States are not allowed to refuse interoperability constituents to be placed in the market bearing the 'CE' logo or declaration of conformity. However the Member States are allowed to take necessary steps when there is reason to believe that interoperability constituents bearing a CE marking and placed on the market are unlikely to meet the essential requirements. They can prohibit their use, restrict their field of application or withdraw them from the market. The Member States must forthwith inform the Commission of the measures taken and give reasons for its decision. The Member State must state in particular whether the failure to conform is due to incorrect application, or inadequacy, of technical specifications. Following that notification the Commission shall consult the parties as quickly as possible. When the Commission finds the measure to be justified, she shall inform the Member State concerned as well as the other Member States. If the Commission finds the measure unjustified the Commission shall also notify the manufacturer, or its authorized representative established within the Community.

Any decision concerning the assessment of conformity to specifications or suitability for use of interoperability constituents, and any decision taken pursuant to the release clause in Directive 2009/750/EC shall set out in detail the reasons on which it is based[82]. It shall be notified along with remedies available under the laws in force in the Member State concerned, and of the time limits allowed for the exercise of such remedies.

These interoperability constituents should utilise open standards. In this regard it is useful to refer to 2010/40/EU discussed in section 2.1 of this Chapter. To ensure coherent and coordinated deployment of ITS in the EU, ITS services and applications should be based on open standards. This requirement is also found in the legal framework on electronic road tolling. It might be useful to point out that the framework on electronic road tolling predates 2010/40/EU. But as already mentioned, coordination between the ITS Committee and the EETS Committee must take place to prevent conflicts and this recurring requirement could be seen as a first step.

2.3.2.3.6 Operation and management requirements

The operation and management requirements deal with data protection and contingency. Several of these have already been detailed in previous sections.

[81] Art. 15, 2009/750/EC
[82] Art. 16, 2009/750/EC

EETS shall fulfil the requirements of data protection legislation, in particular 95/46/EC and 2002/58/EC. The privacy aspects of ITS will however be discussed in the following Chapters, notably in Chapter 3 on the legal framework with regard to privacy and data protection.

Toll Chargers and EETS Providers shall determine contingency plans in order to avoid important traffic flow disruptions in case of EETS unavailability. This thus requires a joint effort and not unilateral measures. This has already been discussed in previous sections and will therefore not be discussed further here.

Toll Chargers should inform drivers, where applicable, through roadside signage or other means, possibly even the OBE, of the requirement to pay a toll or charge for circulating a vehicle in a toll domain and in particular when they enter and leave a toll domain. The detail of the TCD (Toll Context Data) required for the toll domain (see section 2.3.2.2.2.4) should be commensurate with the toll regime requirements in view to guarantee equality of treatment between EETS Users in relation to tolls and charges. Fair and indiscriminate pricing is one of the basic principles of EETS.[84]

[84] For more details on the implementation of electronic fee collection (EFC) interoperability and EETS see the "Guide for the application of the Directive on the interoperability of electronic road toll systems, published by the European Commission and published on the website of the DG for Mobility and Transport, http://ec.europa.eu/transport/publications/doc/2011-eets-european-electronic-toll-service_en.pdf

3 Legal Framework for Privacy and Data Protection

"Despite the many potential benefits of Intelligent Transport Systems, the associated increase in vehicle/infrastructure electronics and communications raises security and privacy issues which, if left unaddressed, could jeopardise the wider deployment of ITS. For example, location-based services may — in combining location information and personal data — have possible implications for personal privacy. There may also be security vulnerabilities in electronics and communications systems. ITS technologies must ensure the integrity, confidentiality and secure handling of data, including personal and financial details, and show that citizens' rights are fully protected".[85] A second legal cornerstone to be taken into account in the EVITA project is therefore the European legal framework for privacy and personal data protection.

European Union law and its application have always been inspired by the fundamental rights contained in international instruments, as repeatedly recognized by the Court of Justice of the European Union (the 'Court of Justice' or 'ECJ').[86] The fundamental rights as laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR' or the 'Convention') have in particular been a key source of inspiration for the general principles of EU law. Fundamental rights contained in international treaties, such as the rights of the Convention take in many countries precedence over national law. Another and most important element to note is the incorporation of fundamental rights in Union law and the accession of the Union to the Convention since the 1st of December 2009. We will hereunder first discuss these relevant fundamental rights in the ECHR and in the Charter of Fundamental Rights of the European Union and continue with an exploration of the concepts and their application in the framework of the European legal framework relating to personal data protection (Directive 95/46/EC) in order to single out elements which are important for the context of the EVITA project.

3.1 Art. 8 European Convention of Human Rights

The right to respect for one's private and family life[87] is listed as one of the human rights and fundamental freedoms in the European Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR' or the 'Convention') concluded in 1950 in the framework of the Council of Europe ('CoE') in Article 8.

[85] Quote from the "Action plan and legal framework for the deployment of intelligent transport systems (ITS) in Europe" (2011), available from http://ec.europa.eu/transport/publications/index_en.htm

86 See ECJ, C-222/84, *Johnston v. Chief Constable of the Royal Ulster Constabulary*, 15.5.1986, §18 ; For the inspiration of the data protection legislation by the fundamental rights, see ECJ, Joint Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk*, 20.05.2003, §68: 'It should also be noted that the provisions of Directive 95/46/EC, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy must necessarily be interpreted in the light of fundamental rights, which, according to settled case law, form an integral part of the general principles of law whose observance the Court ensures'. The latter case was the first decision of the Court of Justice on Directive 95/46/EC.

[87] For purposes of this research, the right to respect for family life is not further analysed, as the focus will remain on the right to respect for (individual) private life.

Article 8 of the Convention reads as follows:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The formulation of this Article is general and the right to respect for private (and family) right is not precisely defined. The scope and effect of Article 8 however has been discussed in many cases before the European Court of Human Rights in Strasbourg (the 'Court' or the 'ECtHR').[88] The Court has repeated at various occasions that the notion of one's private life is not susceptible to an exhaustive analysis or definition but *a broad term*.[89] The notion of one's private life has to be determined *from case to case*, depending on facts and circumstances. Individuals can lodge an appeal if they have personally and directly been victim of a violation of the rights and guarantees set out in the Convention and this violation has been committed by one of the States. Condition is that all remedies in the State concerned have been used, in particular that the claim has been filed, including appeal, with the appropriate national courts.

To summarize: there is no doubt that the introduction of ITS in the Member States needs to fulfil the requirements of Article 8 ECHR. This means in particular that every individual EU citizen can potentially invoke this Article if he or she estimates that the introduction of a specific ITS (eCall, road toll system, etc.) violates his/her privacy rights, for example, because the processing of personal information by the system goes further than what is necessary in a democratic society.

A relevant issue is whether individuals can invoke the fundamental right, not only in their relation with the national authorities (e.g., the government), but also in their relation with other individuals. This issue has been subject of divergent views and debate amongst many legal scholars and is also referred to as the issue of the "*Drittwirkung*", the concept being originally basically developed in Germany.[90] First of all, varying views on the concept itself

---

[88] The European Court of Human Rights was set up in 1959 by the Council of Europe together with a European Commission of Human Rights ('Commission') to decide upon claims for alleged violations of the European Convention on Human Rights of 1950. The Commission had a 'filtering role' in relation with the petitions filed : as individuals did not have direct access to the Court, they had to apply to the Commission, which, if it found the case well-founded, would launch the case in the Court on the individual's behalf (see Section II of the Convention before Protocol N° 11). Protocol N° 11 to the Convention (signed on 11 May 1994) entering into force on 1 November 1998 abolished the Commission and established the permanent European Court of Human Rights as single and permanent court. The Court has its seat in Strasbourg. The decisions of the Court are published in the Reports of Judgments and Decisions, the Court's official series and are also electronically available via the HUDOC Portal of the Court available at http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/ , which provides free online access to the case-law.

[89] For legal authors who have analyzed the concept for Europe and under the Convention, see, e.g., R. Beddart, *Human rights and Europe,* Cambridge, Cambridge University Press, 1993, p.p. 114; A. Clapham, *Human rights in the private* sphere, Oxford, Clarendon Press, 1993, 385 p.; D. Harris, M. Boyle and C. Warbrick, *Law of the European Convention on Human Rights,* London, Butterworths, 1995, 753 p.

[90] On the concept of 'Drittwirkung' in Germany, see also F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Brussels/Paris, Bruylant, 1990, pp. 674–683 ; A. Clapham, 'The 'Drittwirkung' of the Convention', R. Macdonald, F. Matscher and H. Petzold, *The European System for the Protection of Human Rights,* Dordrecht, Martinus Nijhoff, 1993, p. 206.

can be distinguished. According to some, *Drittwirkung* means that the provisions concerning the human rights *apply* to legal relations between private parties. According to others, *Drittwirkung* means that individuals can *enforce* these rights against other individuals.[91] An individual, according to this view, cannot lodge a complaint before the Court against another individual or private party. He or she could only indirectly bring a complaint of violation by a private party, when a Contracting State could be held responsible for such violation (for example, because a national judgement conflicts with the Convention or because the State failed to enact regulation). The Court itself did never pronounce an opinion as to whether the guarantees of the Convention should be extended to relations between private parties *inter se* or not.[92]

The authoritative legal scholars who have reviewed the matter in more detail, come to the conclusion that, although *Drittwirkung* 'does not imperatively ensue from the Convention', 'nothing in the Convention prevents the States from conferring *Drittwirkung* upon rights and freedoms (…) within their national legal systems insofar as they lend themselves to it'.[93] The values encapsulated in Article 8 ECHR are not confined to only disputes between individuals and public authorities. *How* these fundamental rights have direct effect may therefore differ from State to State.[94]

The issue of the *Drittwirkung* should not be confused with the *effect* given by national systems to the provisions of the Convention. In some countries, Article 8 ECHR has been qualified as one of the provisions of 'public order' in Europe which have a direct effect ('*directe werking*'/'*effect direct*') upon the national legislation.[95] As a result, Article 8 ECHR supersedes in these countries the domestic legislation which is contrary to it and the national regulation will be reviewed and interpreted in conformity with Article 8 ECHR (*i.e.*, in conformity with its meaning and interpretation and the conditions for limitations to the fundamental right)[96] while Article 8 ECHR can be invoked before the national courts. In some other countries, however, the national courts are more hesitant to recognize the constitutional value of fundamental rights.

---

[91] P. van Dijk, F. van Hoof, A. van Rijn and L. Zwaak (eds.), *Theory and Practice of the European Convention on Human Rights*, Antwerp, Intersentia, 2006, p. 29 ('van Dijk, van Hoof, van Rijn and Zwaak (eds.), Theory and Practice of the European Convention 2006'.

[92] See van Dijk, van Hoof, van Rijn and Zwaak (eds.), *Theory and Practice of the European Convention*, 2006, p. 29 and further references to the *Verein gegen Tierfabriken* case .

[93] See on this particular issue, J. Velu, *Le droit au respect de la vie privée*, Namur, Presses Universitaires de Namur, 1974, pp. 49-50; see also, for views by common law specialists, M. Hurt, 'The "horizontal effect" of the Human rights Act : moving beyond the public-private distinction', in J. Jowell and J. Cooper (eds.), *Understanding Human Rights Principles*, Oxfort and Portland, Oregon, Hart, 2001, pp. 161-177 and G. Phillipson, 'Transforming Breach of Confidence ? Towards a Common Law Right of Privacy under the Human Rights Act', 66 MLR, 2003, (726), pp. 726-728.

[94] Some States accept direct effect, while other States not so easily (see also *below*). See also van Dijk, van Hoof, van Rijn and Zwaak (eds.), Theory and Practice of the European Convention 2006, pp. 26-27.

[95] The Supreme Court in Belgium has acknowledged explicitly in 1971 precedence of international treaty rules which have direct effect. See Cass., 27 May 1971, *Pas.* 1971, I, pp. 886-920.

[96] See also E. Kindt, E. Lievens, E. Kosta e.a., 'Chapter 2. Constitutional rights and new technologies in Belgium', in R. Leenes, B.-J. Koops, P. De Hert (eds.), *Constitutional Rights and New Technologies. A Comparative Study*, The Hague, Asser, 2008, (11), 19-20.

3.2 Charter of Fundamental Rights of the European Union

A new and most important step in the affirmation of the importance of the fundamental rights for the EU has been the adoption of the 'EU Charter of Fundamental Rights' ('EU Charter').[97] The EU Charter sets out a whole range of civil, political and social rights enjoyed by the EU's citizens. It states in *Article 7* that 'everyone has the right to respect for his or her private and family life, home and communications' and codifies in *Article 8* a fundamental right to protection of personal data.

The fundamental rights proclaimed in the EU Charter were, with a number of amendments[98], *incorporated* in EU law as *primary law with full legal value* by the Treaty of Lisbon (Article 6 (1) of the TEU).[99] The Treaty of Lisbon also amends two core treaties of the EU, i.e. the Treaty on European Union ('TEU') (sometimes also referred to as the 'Maastricht Treaty') and the Treaty establishing the European Community ('TEC')[100] being presently renamed as the Treaty on the Functioning of the European Union ('TFEU'). The Treaty of Lisbon was signed on 13 December 2007 and took after the ratification by all Member States effect on the 1st of December 2009.[101]

Nowadays every citizen of a Member State can consequently challenge actions of EU institutions or of Member States that infringe fundamental rights. Such claims can be brought before the national courts that could make a reference for a preliminary ruling to the Court of Justice (ECJ).[102] The Court has jurisdiction to review the legality of such acts. The ECJ is further competent for the interpretation and the application of the TEU and the TEC.[103] Article 6 (1) of the TEU states that the fundamental rights of the EU Charter shall have the same legal value as the Treaties and the ECJ will review the application of the fundamental rights in areas of its competence.

Insofar the fundamental rights of the EU Charter correspond to the rights of the ECHR, the meaning and the scope of the EU Charter fundamental rights shall be the same as of the rights in the Convention. Article 52 (3) of the EU Charter states explicitly that rights contained in the Charter which correspond to rights guaranteed by the ECHR, shall be interpreted in the same way.[104] The right to respect for privacy is such fundamental right which is guaranteed

---

[97] Charter of Fundamental Rights of the European Union, *O.J.* C 364, 18.12.2000, pp. 1 – 22.

[98] The EU Charter was slightly adapted at Strasbourg on 12 December 2007.

[99] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13 December 2007, *O.J.* C 306, 17.12.2007, pp. 1- 229; see also the consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (previously named Treaty establishing the European Communicty), *O.J.* C 115, 9.05.2008, in particular Article 6 (1) of the (revised) Treaty on European Union, p. 19, available at http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2008:115:SOM:en: HTML; in an intermediate step, the EU Charter was first inserted in the Treaty Establishing a Constitution for Europe (*O.J.* C 310, 16.12.2004, pp.1 – 474. Because of ratification problems, this was not carried through.

[100] This was previously named the Treaty establishing the European Economic Community (EEC Treaty) of 1957, often referred to as the Treaty of Rome.

[101] The United Kingdom and Poland, for example, negotiated some restrictions regarding the appliation of the EU Charter. See Protocol etc. *O.J.* C 306, 17.12.2007, pp. 156- 157.

[102] However, according to Article 46 previous TEU, the Court has no jurisdiction with regard to the common foreign and security policy of the EU (Title V) and limited jurisdiction with regard to the police and judicial cooperation in criminal matters (Title VI). The Court has also no jurisdiction over 'any measure or decision [concerning the controls on persons when crossing internal borders] relating to the maintenance of law and order and the safeguarding of internal security' (Article 68 of the previous version of the TEC Treaty).

[103] See Article 19 TEU. This is also a reference that the 'rule of law' shall be observed.

[104] Article 52 (3) of the EU Charter states that 'the meaning and scope of those rights shall be the same'. About the relationship between the EU Charter and the ECHR, see for example, F. Tulkens, 'Towards a Greater

by both the EU Charter and the ECHR.[105] At the same time, it is stated that Union law[106] may provide more extensive protection.

Many rights as stated in the Convention are taken over by the Charter. This can be explained by the initial intention of the Charter to replace European treaties and the human rights set forth therein, including the Convention. This process did not go through[107] but both texts remained. As a result, the wording and even some rights differ in the two texts. For example, the fundamental right to data protection is unique in the EU Charter and not expressly stated in the Convention.[108] This means that it remains a challenge to reconcile the meaning and the application of both texts.

The competence of the ECJ to review also the application of the fundamental rights may lead to potential conflicts with decisions of the European Court of Human Rights in Strasbourg (the 'European Court of Human Rights' or 'ECtHR') which was established with an express human rights jurisdiction.[109] These potential conflicts between decisions of the Court of Justice and the European Court of Human Rights in the enforcement of the respect for fundamental rights and the interpretation and application of the texts, will in principle be overcome by the fact that the revised Treaty on European Union provides for the accession of the European Union to the Convention (revised Article 6 (2) TEU). It means that all acts of the European Union institutions, including of the Court of Justice, is subject to the judicial review by the European Court of Human Rights for their compatibility with the fundamental rights contained in the Convention.[110]

3.3 European Union Data Protection Framework

3.3.1 Art. 16 Treaty on the Functioning of the European Union

Since the Lisbon Treaty, an express provision is inserted in the Treaty on the Functioning of the European Union or TFEU which states that the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, *shall lay down* the rules relating to the free movement of *personal data and the protection of individuals* with regard to the processing of such data by Union institutions, bodies, offices and agencies, and by the Member States *when carrying out activities which fall within the scope of Union law* (Article 16B TEC).

For this reason, the Commission launched a consultation in 2009 on the legal framework for the (new) fundamental right to protection of personal data, as a first step to the establishment of a comprehensive legal framework for data protection fit to cope with the changes

---

Normative Coherence in Europe: The Implications of the Draft Charter of Fundamental Rights of the European Union' (2000) 21 *HRLJ* 329

[105] See, however, about how the ECJ connects other rights of the Charter, in particular the right to data protection (which is not mentioned in the ECHR) with rights known from the ECHR

[106] With 'Union law', reference is in fact made to the EU Charter.

[107] The ratification of the Treaty to the Charter was stopped in 2005.

[108] The fundamental right to data protection as applied by the European Court of Human Rights is deduced and based on Article 8 of the Convention.

[109] See K. Lenaerts and E. de Smijter, 'The Charter and the Role of the European Courts', *MJ* 2001, (90), p. 92 ('Lenaerts and de Smijter, The Charter and the Role of the Courts, 2001')..

[110] See Lenaerts and de Smijter, The Charter and the Role of the Courts, 2001, pp.100-101.

since the Lisbon Treaty. At the time of writing this report the outcome of this process is still uncertain.[111] On 4 November 2010 the Commission adopted a strategic Communication on a comprehensive strategy on data protection in the European Union highlighting its main ideas and key objectives on how to revise the current rules on data protection.[112] In this document the Commission explicitly mentions the challenges related to ITS.[113] For the time being however, the applicable legal framework to be taken into account by the EVITA project remains the one established by the Directives 95/46/EC and 2002/58/EC.

3.3.2 Directive 95/46/EC on protection of personal data

Directive 95/46/EC[114] (the 'Data Protection Directive' or 'Directive 95/46/EC') is the basis for the data protection legislation of all the European Union countries.[115] The Directive 2002/58/EC[116] (the 'eCommunications Privacy Directive' or 'Directive 2002/58/EC'), as amended, is of importance as well, more in particular for data protection in the domain of publicly available electronic communications services.

3.3.2.1 Concepts

In this section the most fundamental concepts of data protection law are discussed and linked to the domain of ITS. Crucial concepts are "personal data", "controller" and "processor".

[111] See further: http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

[112] http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[113] See page 3 of COM(2010)609

[114] 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, *O.J.* L 281, 23.11.1995, pp. 31- 50, also available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (part 1) and http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf (part 2).

[115] It should be noted that in some EU countries, data protection rights principles and legislation already existed long before these Directives. See, for example, the data protection legislation enacted in France in 1978. Other examples of 'early' data protection legislation are the legislation in the German state of Hesse (Germany) (1970, being the worldwide first 'modern' data protection legislation), Sweden (1973) and federal data protection legislation in Germany (1977). Such legislation was later on adapted where needed to implement the Directive. For an overview of the implementation of the Directive in the 27 Member States, see European Commission, *Status of implementation of Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data,* available at http://ec.europa.eu/justice_home/fsj/privacy/law/ implementation_en.htm

[116] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O. J.* L 201, 31.07.2002, pp. 37-47. Article 3 §1 states: 'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community'. Directive 2002/58/EC replaced the Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, *O. J.* L 24, 30.01.1998, pp. 1-8 and was amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (*O. J.* L 337, 18.12.2009, pp. 11-36) introducing *inter alia* the obligation to notify personal data breach (see Article 2).

3.3.2.1.1 Personal Data

Personal data is any information that relates to an identified or identifiable natural person[117]. It is evident that this definition can lead to various interpretations. Therefore the Article 29 Data Protection Working Party has issued an opinion regarding the concept of personal data[118].

The Article 29 Working Party explains in its opinion the notions of a person that is 'identified' and of a person that is 'identifiable'. The Working Party understands identified in general terms. It considers a person as identified if that person is distinguished within a group of persons from all the other members of the group.[119] Directly identified or identifiable is in practice when a person is referred to by a name. Indirectly refers to a situation where additional pieces of information are necessary.

The most common way to identify an individual is by name. In that case, a person may be identified directly by a name. The circumstances of the case will determine whether the identifier, in this case the name, is sufficient to achieve direct identification.[120] According to the definition the person needs to be 'identified or identifiable'. A person is identified within a group of persons if he is distinguished from others in that group. Identifiable is a person who has not yet been identified, but who could be. A person can be directly or indirectly identifiable.

Direct Identification mostly refers to identification through the name, the most common identifier, although this will not always be sufficient if for example the surname is quite common. Direct identification refers to the situation where a person has already been identified contrary to the situation of indirect identification where it is possible to identify a person but identification has not yet taken place.

Indirect identification comes from a unique combination, small or large, of identifiers; specific to a person's physical, physiological, mental, cultural or social identity. These identifiers may not even include the name; it is sufficient that the person can be distinguished from others in the same group.

Directive 95/46/EC says that we must take into account all means likely reasonably to be used to identify a person by the controller or a third party[121]. The Article 29 Working Party gave in its Opinion a clarification on this aspect. For assessing 'all the means likely reasonably to be used to identify a person', as it is worded in Recital 26 of the Directive 95/46/EC, the Article 29 Working Party stated that "all relevant factors shall be taken into account, including not only the cost of conducting identification, but also the intended purpose, the way the processing is structured, the advantages expected by the controller and the interests at stake of the data subjects, as well as the risks of organisational (breaches of confidentiality duties) and technical dysfunctions". [122]

---

[117] Art. 2(a), 95/46/EC

[118] Opinion 4/2007 on the concept of personal data, WP 136, Art. 29 Working Party website

[119] In fact, 'identified' and 'identifiable' are understood by the Article 29 Data Protection Working Party as to whether there are sufficient identifiers to single out a particular person.

[120] WP 29 Opinion 4/2007, p. 13. In the opinion, the Article 29 Data Protection Working Party gives the example that a name may not be sufficient to identify a person from the whole of a country's population, while this may well be possible for a pupil in a class.

[121] Recital 26, 95/46/EC

[122] *Ibid.*, p. 15.

To know which means are likely reasonably to be used, not only the means available to the controller but also those *available 'to any other person'* shall be taken into consideration. This other person does not need to have a particular relationship with the controller. A typical example is the website provider who processes the IP-number of website visitors (for example to determine their geographic location) but is unable to identify the website visitor. The provider processes nevertheless personal data because the website visitor is identifiable, not by the provider (the data controller) in this case, but by the ISP from which the website visitor got the IP-number to connect to the Internet.

The rule compels to take a maximum number of factors into account. It is a dynamic test; we must look not only at the state of the art of technology available to identify the person but also possible developments that take place during the duration of the processing. So the longer the data are stored, the more likely a person is to be identifiable because of the increased possibilities likely to be offered by technological developments. One must also look at the controller's purpose. In some cases a processing operation only makes sense if the data subject can be identified. That processing operation should always be considered processing of personal data. In those cases the possibility that the legislation be circumvented through statements contradictory to the goal must be prevented. Therefore we must look at the actual facts of the processing and disregard its form. A similar approach is described below in relation to the determination of controller. Another factor is the value of the data compared to the cost of identification. We must also look at the technical and organizational measures put in place by the controller to prevent identification. If these measures make it impossible to identify the person using reasonable means, a data subject may not be identifiable and the data regarded as anonymous.

The final building block of the concept of "personal data" is that the information must relate to a *"natural person",* meaning a human being. Legal persons do not fall within the scope of Directive 95/46/EC. In the ITS context this can be relevant because vehicles are often owned by companies or other organisations. Transfer of data originating from one of those vehicles will not necessarily contain information relating to natural persons. However as soon as the data *can* lead to a conclusion about, for example, the current location of a driver whose identity can be revealed using reasonable means (for example by the employer of the vehicle driver), we are again under the scope of Directive 95/46/EC.

In the context of communications between vehicles or between vehicles and infrastructures there will typically be processing of personal data in all applications where it is necessary to identify the vehicle and where such identification provides information about a natural person (for example the owner or the driver of the vehicle). Typical examples of examples needing some kind of vehicle identification are automatic emergency calls, electronic fee collection systems charging road vehicles, remote diagnosis systems, etc. In most of these cases the identification of the vehicle can potentially lead to information about the owner or the driver (for example the location of the person concerned or simply the information that person X is the owner of car Y or Z). On the other hand one can imagine e.g. remote diagnosis systems collecting data about identified cars owned by a company, without any natural person being involved in the whole process. In such cases the data processing falls evidently outside the scope of Directive 95/46/EC since no personal data are being processed.

On the other hand one can imagine many applications where vehicle identification is not necessary, for example in some cases where vehicles simply receive information originating

from traffic management or navigation systems. As soon as, however, a vehicle needs to connect to the network and receives an IP-address, personal data are possibly being processed. The crucial question will therefore always be: does the application allow identifying the natural person owning or driving the vehicle?

3.3.2.1.2 Controller

The following question to answer is: who will be accountable for processing the personal data. In the terminology of Directive 95/46/EC this (natural or legal person, or any other entity) is called "the controller".

The controller is the person deciding the goals and means of a particular data processing operation. In the Data Protection Directive the controller is defined as:

> *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.*

This definition has been the source of debate for numerous years, and the WP29 has issued an opinion clarifying this concept as well.[123] Controller is a functional concept to allocate responsibilities where the factual influence lies. The facts take precedence over form in this determination. Following are the main elements as the WP29 has identified them.

'Natural or legal person, public authority, agency or any other body' defines who can be controller. Basically there is no restriction on who can be controller; it does not even require a physical person. A legal body does require a physical person as a contact point, but the controller needs not to be a physical person.

'Determines' refers to a legal (explicit) or implicit competence. A party is somehow given the competence to process data. An explicit competence can be when a person is specifically appointed controller but this is a rare occasion. More frequent is the situation where a task is imposed to collect or process certain personal data. An implicit competence is not laid down in law nor is it the consequence of an imposed duty. One example is labour relations where the employer processes certain data in relation to his employees in order to fulfil his duties with regard to his employees and the government.

This determination can be done *alone or jointly with others*. This is important with regard to the allocation of the responsibilities of the controller. If multiple parties are involved as controller in a single data processing operation this could have different consequences. First of all there could be *joint control*. This would mean that each party is equally responsible for all aspects of the data processing operation. This is mainly important with regard to liability for damages that could result from the data processing operation. This should not have any effect on the data subject's rights granted by Directive 95/46/EC. Another possible situation is that of *distributed joint control*. In that case each party is responsible for a specific part of the data processing operation. This situation may occur in a V-2-X environment because often many different parties are involved. The key, however, is that the determination of goal and

[123] Art. 29 Working Party Opinion 1/2010 on the concept of "controller" and "processor", adopted 16 February 2010 (WP 169)

means of data processing is done jointly with others. If each party involved autonomously decides on his processing there is no joint determination and thus no joint control. There are only different controllers executing non-related processing operations on personal data. In this latter case we might have a situation of transfer of personal data to third parties.

The *'purpose'* is the reason for processing personal data and the *'means'* refer to how the actual processing is organised and executed. The WP29 also explains this as the "why" and "how" of data processing. The power to determine has several aspects. First of all there is the level of influence a party has in deciding means and purposes. Secondly the level of detail in which a party can organise a processing plays a role. A final and related aspect is the margin of appreciation a person leaves to the individuals processing data on his behalf. If he leaves them no margin of appreciation, he is deemed a controller. At first sight the opinion does not appear to make matters easier. But the reason for this relative complexity is that the concept of 'controller' is a factual one. As an abstract concept it would be subject to abuse and evasion. By trying to look at who actually *is* the controller, rather than who is *presented* as controller, the protection offered by Directive 95/46/EC should be maximised[124]. The allocation of the duty of controller also limits the competence of other actors involved in the data processing.[125].

3.3.2.1.3 Processor

A processor is anybody that processes data on behalf of the controller. He is a subcontractor of the controller so to say, charged with executing the data processing operation as a whole or in part.

Very often it is difficult to distinguish between controllers and processors. Take the example of a car repair shop processing data in the context of a remote diagnosis system and therefore using a specialised service provider operating under a contract with the car manufacturer. Let us further imagine that the specialised service provider operating the remote diagnosis system uses the services (for example the data centre) of a cloud service provider. Who is (are) the controller(s) and the processor(s) in this constellation? Who determines the purposes and means of the personal data processing?

The problem is that the qualification of an entity as either a controller or a processor has significant implications. These implications are situated at mainly three levels: the allocation of responsibility and risk, the determination of applicable law, and compliance with the substantive provisions of the Directive.[126] Given these implications, it is essential to be able to determine which role an entity has assumed towards a particular processing operation.

The distribution of responsibility and liability among controllers and processors results from a combination of several provisions. As far as the controller's obligations are concerned, the allocation of responsibility is in first instance the result of article 6(2) of the Directive.

[124] C. Kuner, *European Data Protection law*, Oxford University Press, Oxford, 2007, nr. 2.27

[125] Art. 29 Working Party Opinion 1/2010 on the concept of "controller" and "processor", adopted 16 February 2010 (WP 169), p.15

[126] See for a comprehensive analysis B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", to be published in Computer and Security Law Report, 2011.

This provision stipulates unambiguously that it shall be the controller who must ensure that the principles of data protection (as contained in article 6(1)) are complied with. In addition, the Directive specifies a wide range of additional obligations (accommodation of data subject rights, maintaining an appropriate level of security, etc.) which shall be incumbent upon the controller. Finally, article 23 of the Directive explicitly confirms that the liability for damages caused by non-compliant behaviour shall be borne by the controller, unless he can prove that he is not responsible for the event giving rise to the damage suffered.[127] As far as the processor's obligations are concerned, the Directive is far more succinct. In fact, it articulates obligations addressed directly towards the processor only in a limited number of instances.[128] Be that as it may, the processor shall in principle be obligated to observe all relevant aspects of data protection law by means of contract with the controller (see article 17(3)).[129] In addition, article 16 explicitly provides that the processor may only process personal data pursuant to the instructions of the controller.

The qualification of an actor as either a controller or a processor is also an essential element in determining which law(s) applies (apply) to a processing operation or set of processing operations.[130] Article 4 (1) sets forth the various instances in which a Member State must apply the national laws it has adopted when implementing the Directive. Each of these instances hinges, to a greater or lesser extent, upon the location in which the controller is established.[131] However, the qualification of an actor as a processor can also be determinative in deciding which law to apply to a particular processing operation. Article 17 (3) provides that the scope of the security obligations (which shall be incumbent upon the processor by virtue of the contract which is to be concluded among controllers and processors) shall be determined by the national law of the Member State where the processor is established.[132] As a result, both concepts are pivotal in determining the scope of data protection legislation, not only by reason of the type of entity concerned but also when determining the applicability of national provisions.

Although the qualification of an actor as a processor or a (co)controller is consequently crucial, it will in particular in the context of examples as the one mentioned above related to a remote diagnosis system not be easy to establish. In the view of the WP29 each party taking in charge an *essential contribution* to the data processing chain should be considered as a (co)controller. Specifically, joint control shall arise whenever '*different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterise a controller*'.[133]

---

[127] See also Opinion 1/2010, *l.c.*, 4.

[128] See also J. Alhadeff and B. Van Alsenoy (eds.), 'D6.2 Contractual Framework', *l.c.*, second iteration, 31; T. Olsen and T. Mahler, 'Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II', *Computer, Law & Security Review* 2007, Vol. 23, n° 5, 418.

[129] See also Opinion 1/2010, *l.c.*, 26.

[130] See Opinion 1/2010, *l.c.*, 5.

[131] For more information see Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law', WP179, 16 December 2010.

[132] The rationale behind this provision is to ensure uniform requirements within one Member State with regard to security measures. Due to the fact that security requirements can diverge considerably among Member States, this may have practical implications. (see Opinion 8/2010, *l.c.*, 25)

[133] Opinion 1/2010, *l.c.*, 19. In order to ascertain whether an entity's 'determination of means' gives rise to a qualification of (co-)controller, the Working Party has stated that the entity's influence must extend to 'those

From a practical point of view it will be necessary to determine explicitly, taking into account the respective roles of the every actor involved in the V2V or V2I communication, which party or parties will be considered as the controller(s) vis-à-vis the data subject.

3.3.2.1.4 Applicable National Law

The applicable national law defines the geographical scope of the implementing legislation enacted by EU Member States. It defines when Member State rules are applicable to the processing of personal data.

When the controller has an establishment in a Member State, the national law of the Member State of establishment applies to the processing operation. This raises a question with regard to the concept of establishment. In principle an "establishment" is a permanent presence on the territory of a Member State[134]. The form of this presence is not important; what is important is whether there is effective and real exercise of activity on the territory of that Member State. This presence can be a branch, but it can also just be an employee present in the Member State[135]. Much will depend on the law of the concerned Member State. If there is effective and real exercise of activity, then there is an establishment in a Member State and the national rules of that Member State must be applied.

With regard to road tolling it should be pointed out that a Service Provider and a Toll Charger are required to have an establishment in a Member State of the Union. This makes electronic road tolling subject to Directive 95/46/EC by virtue of this provision. If Directive 2004/52/EC is to serve as an example of future ITS legislation it would seem reasonable to assume that organizational requirements will include the mandatory presence of an establishment of the organizing entity on the territory of a Member State.

When the controller is not established in an EU Member State uses equipment located in the territory of a Member State, the law of that Member State applies unless the equipment is only used for transit[136]. This begs the question as to what is meant by "equipment". This is not clear. One seems to assume that it is not required that the equipment be operated or owned by the controller. What matters is that the equipment used is part of the "why" and "how" of the data processing decided by the controller[137].

We assume that providers operating V2V or V2X communications services, without being established in the European Union, will not be very frequent. Practically speaking the data protection law applicable to an ITS will be the law of the EU Member State where the controller is established. If there is only one controller and if this controller is established in an EU Member State, the solution is simple: the applicable law will be the law of that Member State. If the controller is established in more than one Member State the applicable law will be determined by the purpose of the processing operations: the applicable law will be the law

---

essential elements which are traditionally and inherently reserved to the determination of the controller' (*Ibid*, 14).

[134] Preamble 18, Dir. 95/46/EC

[135] C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 2.51

[136] A. Kuczerawy, "Facebook and its EU users - applicability of the EU data protection law to US based SNS", in M. Bezzi et al. (Eds.): *Privacy and Identity*, IFIP AICT 320, pp. 75–85 (Springer)

[137] *See* C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 3.27

of the Member State where the establishment is located in the context of whose activities the processing activities are being carried out.

More complex legal situations will occur where ITS processes are composed of various services (network, data hosting, web services, etc.) provided by (co)controllers established in different Member States. The question which national data protection law(s) are applicable to these situations can only be tackled on a case-by-case basis.

3.3.2.2 Lawful processing

3.3.2.2.1 Data quality

Compliance with requirements regarding data quality rests with the controller(s).

3.3.2.2.1.1 Fair and lawful

Only if one of the six grounds mentioned in Article 7 of Directive 95/46/EC applies to a certain processing is that processing legitimate and can one proceed with it. The list of six grounds will be discussed in section 3.3.2.2.2 below. This requirement has been further stressed by the EDPS in relation to ITS services and applications.[138] They require a legitimate ground and that ground cannot be the operation of the service or application. This would amount to stating that one needs the data because one needs the data. In the case of e-Call applications the legitimate ground would most probably be the protection of a vital interest of the data subject. Other services will be offered via a contract and in this case the execution of that contract also will be the legitimate ground for data processing. But a legitimate ground can only be one of the grounds listed imposed by law to legitimise a data processing operation. We will come back to this later in this Chapter.

"Fair" refers to the requirement of providing information to the data subject that the controller has to abide by. Therefore "transparent" may be a more appropriate term than fair. This will be explained in more detail in section 3.3.2.2.4 below.

3.3.2.2.1.2 Specified, explicit and legitimate purpose

Article 6 of the Directive requires a specified, explicit and legitimate purpose pursuant to which personal data will be collected. Personal data cannot be processed further in a way that is incompatible with that purpose. This principle is also referred to as the "purpose limitation" principle[139]. This purpose limitation is very important but also sometimes difficult to interpret. It is not that easy to determine which goals are compatible or incompatible. In the case of direct marketing, for example, a goal is sometimes considered "compatible" if a company

[138] Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, (2010/C 47/02), published in the Official Journal of 25 February 2010 but also on the EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

[139] C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 2.89

contacts its customers in relation to similar products or services to those which the company has provided them with previously[140].

3.3.2.2.1.3 Adequate, relevant and not excessive

When personal data are required they should only be processed insofar as necessary for the performance of ITS applications and services[141]. The "not-excessive" part of this provision refers to the data minimization principle: process as little data as you can. The guiding principle is "select before you collect"[142]. The EDPS stresses that this principle should be implemented both in relation to organizational as well as technical aspects of ITS applications and services. Instead of collecting everything and then filtering out the data required and either disposing of or securely storing the rest, these systems should be designed in such a way that they only collect the information they need[143]. The importance of this principle is that the mere existence of personal data entails a risk to the data subject. This has been clearly demonstrated by the European Court of Human Rights (ECtHR), for instance in the *Rotaru* decision[144].

In relation to ITS, the EDPS also found added risks in the requirement of interoperability where excessive personal data are collected. This interoperability could entail the interconnection of different databases making it easier that data subjects be subject to data mining and profiling. These technologies aim at cross-referencing data from different sources to compile an individual's profile. The problem is that this profile is only based on the data available and not on reality[145]. Additionally the quality of the criteria used for data mining or profiling may be questionable. The result could be that the profile compiled by the computer is inaccurate or even false. Several examples exist where people have been put on black-lists because their name resembles that of a wanted person or they are supposed to meet certain criteria that would label them as possible terrorists.

3.3.2.2.1.4 Accurate and up-to-date

The data processed must be accurate and up-to-date. Correspondingly, the controller must take all reasonable steps to ensure that inaccurate or out-dated data are rectified or erased. A well-known example that illustrates how companies may comply with that requirement is

---

[140] C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 2.89, 5.196

[141] Art. 10.3, 2010/40/EU

[142] B. Jacobs, "Select before you collect", *Mens en Maatschappij* 2005, 1006

[143] J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," In *19th USENIX Security Symposium 2010*, Usenix, 26 pages, 2010.; C. Troncoso, G. Danezis, E. Kosta & B. Preneel, *PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance*, In Workshop on Privacy in the Electronic Society 2007, Proceedings of the 2007 ACM workshop on Privacy in electronic society table of contents Alexandria, Virginia, USA SESSION: Privacy preserving services and human factors table of contents, p. 99 - 107, 2007

[144] Rotaru v. Romania, *ECtHR* 2000, application no. 28341/95. This case concerned a person on whom a file was kept by the Romanian secret service. This file concerned a name-sake, yet Mr. Rotaru suffered the inconveniences of the fact that the file existed. The Romanian secret service acknowledged after a trial that the file did not concern the person but refused to destroy the file and only made mention of the fact in the file. The ECtHR did not agree with this course of action and decided that the mere existence of the file and the possibility of mistaken identity was an infringement on the right for the protection of Mr. Rotaru's private life.

[145] B. Jacobs, "Select before you collect", *Mens en Maatschappij* 2005, 1006

when their web portals offer customers access to their personal profile so that they can correct and modify their personal data where necessary.

3.3.2.2.1.5 Anonymisation

Compliance requires that data should not be kept in an identifiable form for longer than needed for the purposes for which the data were collected and further processed. In this regard reference can be made to the requirement of anonymisation contained in Directive 2010/40/EU.

This also concerns the duration of data retention. Data retention refers to the time span a controller can keep personal data that has been collected. As mentioned earlier, the existence of data is a risk in itself: the longer the data is kept the more the risks grow, especially with regard to the security measures implemented. A security measure that was considered adequate last year may be out-dated today. Another issue is that the amount of data available only keeps growing. As a consequence, the longer data is stored, the more data becomes available about a person, and, as a result, the more accurate his or her profile may become. But this is not only to the detriment of the data subject since, sometimes, the more data that is available, the more difficult it may become to filter out the required data[146].

3.3.2.2.2 Grounds for legitimate processing

As discussed earlier, a data processing operation needs a legitimate purpose. In addition to that goal, *at least one of the six grounds* for legitimate processing listed in Article 7 of the Directive and discussed in this section must be present to justify the data processing operations.

3.3.2.2.2.1 Unambiguous consent

The first of the six possible grounds justifying the processing of personal data is the unambiguous consent of the data subject. Consent with regard to the data subject is defined as "any freely given specific and informed indication" of the data subject's wishes. Note that the definition mentions the word indication instead of other possibilities such as expression. If one were to look up "indication" in the Merriam Webster dictionary one would find that the "indicate" means "to point out or point to". It gives a general direction but not absolute certainty and should be considered on a combination of elements[147]. Related thereto "unambiguous" consent must be distinguished from "explicit" consent. Unambiguous consent means that the data subject can reasonably be assumed to have consented to the data processing operation whereas explicit consent means that the data subject must have expressed his consent to the data processing operation.

Unambiguous consent thus leaves room for an assumption of consent while in the case of explicit consent there can be no room for an assumption. In that regard the importance of the use of "indication" shines through, given the earlier cited definition.

[146] *See, e.g.*, B. Jacobs, "Select before you collect", *Mens en Maatschappij* 2005, 1006
[147] C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 2.17

Another important aspect is that consent must be freely given[148]. The data subject must have a choice in fact of whether or not to consent to the processing of personal data. If there exists a dependent relationship between controller and data subject, such as an employment relation, consent cannot be freely given[149]. This is the reason why the Art. 29 Working Party is of the opinion that consent can only exceptionally be used in employment relations. Consent should only be used if the data subject has the choice to withdraw his consent. From this one could conclude that a "free consent" requires two elements: first of all the free choice to give consent, and secondly the free choice to withdraw consent. If one or both elements are missing, consent should not be relied upon as a legitimate basis for data processing.

The Article 29 Working Party has recently (July 2011) responded to a request from the EU Commission and has published an opinion on the definition of consent.[150] The Opinion provides a thorough analysis of the concept of consent as currently used in the Data Protection Directive and in the e-Communications Privacy Directive. Drawing on the experience of the members of the Article 29 Working Party, the Opinion provides numerous examples of valid and invalid consent, focusing on its key elements such as the meaning of "indication", "freely given", "specific", "unambiguous", "explicit", "informed" etc. The Opinion further clarifies some aspects related to the notion of consent. For example, the timing as to when consent must be obtained, how the right to object differs from consent, etc.

3.3.2.2.2.2 Contract with the data subject

Processing of personal data is also allowed when it is required for establishing a contract with the data subject or when it is required in the execution of a contract involving the data subject. This can be explained by a simple example. If a person buys a car, the vendor needs the buyer's identification data in order to fill out the contract form.

3.3.2.2.2.3 Compliance with the data controller's legal obligation

A legal obligation for the data controller is the third ground which can justify processing of personal data. With regard to this ground for legitimate data processing it is important to point out that it should concern a mandatory legal obligation. This means that the controller does not have a choice whether or not to apply the law. Should he have this choice, the controller could not appeal to that legal ground. Again, if a person buys a car, the vendor will most probably need to process the car's registration documents because the law requires him to do so.

3.3.2.2.2.4 Protect the data subject's vital interest

Here the example of "e-Call" (emergency call) may be used. When the e-Call unit sends out an emergency message, that message contains certain personal data. Data are only sent in case of emergency, i.e. a car crash. The goal of e-Call is to mitigate the consequences of a car crash to the occupant of the vehicle involved. This accident mitigation is a data processing aimed at protecting the data subject's vital interest, more precisely his life or physical integrity.

---

[148] Art. 29 Working Party Opinion 8/2001 on the processing of personal data in the employment context, 13 September 2001, p 23

[149] C. KUNER, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 2.16

[150] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

3.3.2.2.2.5 Necessary for the performance task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed

This fifth ground is gaining importance given the current trend of governments outsourcing certain of their activities to private companies[151]. In the context of a car sale civil servants the administration in charge of delivering the license plates will need to process identification data relating to the physical person who buys the car or to the physical person who represents the company buying the car.

3.3.2.2.2.6 Necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

The last ground involves a balance of interest between the interests of the controller and the fundamental rights and freedoms of the data subject. The issue with this ground is that it tends to be applied differently depending on the Member State involved. As an example of this legal ground the WP29 (in its Opinion on the definition of "consent") refers to client management services by a car vendor (e.g. to have the car serviced in different affiliate companies within the EU).[152]

3.3.2.2.3 Grounds for legitimate processing of sensitive personal data

Sensitive personal data includes data relating to racial or ethnic origin, religious beliefs, sexuality and trade union membership and personal data concerning health. According to Article 8 of the Directive 95/46/EC the processing of these special categories of personal data is prohibited unless the law explicitly provides an exemption. One important exemption is the *explicit* consent of the data subject.

Processing of sensitive personal data in the context of automotive on-board networks will most probably not very often occur. Nevertheless, it is important to point out that data collected in the operation of ITS may lead to the occasional processing of sensitive personal data. Extensive sets of location data may reveal a person's religious beliefs if cross-referenced with a map. If a person is recurrently found to be travelling to or close to the location of a mosque, one could conclude the data subject is Muslim. A similar solution could be drawn if the person is found to be travelling frequently to the vicinity of labour union locales.

3.3.2.2.4 Information to the data subject

If the personal data are obtained from the data subject, the data controller must provide the data subject, at the moment of collecting the data, with the specific information he is required to provide pursuant to applicable national law[153]. The controller must, however, not provide this information if the data subject is already in possession of the required information.

[151] C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 5.28

[152] WP29, Opinion 15/2011 on the definition of consent, p. 8

[153] Article 10, Directive 95/46/EC. This information may include the controller's identity; the purposes of the processing for which the data are intended; any further information such as the recipients or categories of reci-

In the context of ITS personal data are often automatically collected, without the data subject being aware of this collection. Moreover the data subject will, in many cases, not have sufficient information and knowledge to fully understand the purposes and means of the data processing. Nevertheless it is extremely important to provide to the data subject sufficient information, explaining as clearly as possible, which data are collected for which purposes, how long these data will be stored and who will have access to them.

If the data have not been obtained from the data subject notification to the data subject must be done at the moment of recording of the data or disclosure to a third party. Here, as in the previous hypothesis, no notification is required if the data subject has already been notified. In this case there are three additional exemptions for the controller. The controller is not required to notify the data subject if he proves that notification is impossible. If the notification would require a disproportionate effort from the controller, he is exempt as well. Finally, the controller is also exempt if the recording or disclosure of personal data is laid down in law.

3.3.2.2.5 Data subject's access rights

Member States are responsible for guaranteeing the data subject's access rights. The practical implementation of the rights guaranteed by 95/46/EC will thus depend on the implementation in national law of 95/46/EC.

The data subject is entitled to receive, at reasonable intervals without constraint and without excessive delay or expense, confirmation as to whether or not his personal data are being processed by the controller. This confirmation should state the purpose of the processing, the categories of personal data that are being processed and the recipients or categories of recipients to whom the data are disclosed. The personal data that are being processed must be communicated to the data subject in an intelligible form and the source of the personal data should also be communicated. If the data processing involves automated decision making the controller must inform the data subject of the logic involved in the data processing. This is not mandatory for other forms of data processing.

In addition to notification, the data subject is also entitled to rectification, erasure or blocking of any personal data not complying with data protection rules. It is also a general principle for data processing operations that personal data must be kept accurate and up-to-date. It is, however, not mentioned how this should be achieved by the controller. One possible option would be a web portal allowing the users to check and modify their personal details and modify their privacy settings. Any of the pre-cited operations must be notified to third parties to whom the data are disclosed. This notification is not required if it would require a disproportionate effort from the controller or if it would simply be impossible for the controller to accomplish.

---

pients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the existence of the right of access to and the right to rectify the data concerning the data subject in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

3.3.2.2.6 Restrictions on data subject's rights

95/46/EC holds several possibilities for restrictions on the rights of the data subject:

- National security, defence or public security,
- Prevention, investigation, detection, and prosecution of criminal offences or breaches of ethics of regulated professions,
- Important economic or financial interests of the country,
- Monitoring, inspection of regulatory function connected with the exercise of official authority,
- Protection of the data subject or rights of freedoms of others.

This is a limitative list of grounds for restricting the access of data subjects to their personal data. These restrictions can only be imposed by the Member States and must be necessary to safeguard the ground invoked. These exemptions should be offset against the exemptions to the scope of 95/46/EC such as "processing in the course of a purely personal or household activity". The latter exempt the processing entirely from applicability of 95/46/EC, while the exemptions in this section only restrict the rights of the data subject, but do not affect other provisions of 95/46/EC. The latter remain applicable.

3.3.2.2.7 Other data subject's rights

In some cases the data subject has the right to object to the processing of his personal data. The most important case is direct marketing. Any person can object to the processing of personal data relating to him/her for this purpose.

Member States must also grant their citizens the right not to be subject to automated decisions producing legal effects or having a significant effect on the data subject. The automated decision is further specified as a decision solely based on automated processing of data intended to evaluate certain personal aspects relating to the data subject such as creditworthiness or performance at work. In essence this provision sets forth rules relating to automated profiling of data subjects. The legal effects mentioned would be effects that alter a person's rights or duties. The significant effects are less easy to determine[154].

There are two situations when automated decisions are allowed. The first situation is where automated processing is required for entering into or the performance of a contract to which the data subject is party. This requires that either the contract request has been lodged by the data subject and has been satisfied or that suitable measures to safeguard his personal interests are present. Such suitable safeguards could be arrangements for the data subject to present his point of view. Previously, when discussing the grounds for legitimate processing of personal data, it has been mentioned that one of these grounds is the performance of a contract to which the data subject is party.

[154] L. Bygrave, "Automated Profiling. Minding the Machine: article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law and Security Report* 2001, Vol. 17 nr. 1, p.19

A second situation is where the automated decision has been authorized by law. This does require that the law contains measures to protect the data subject's interests.

3.3.2.2.8 Confidentiality and security

Directive 95/46/EC only contains very general "high-level" provisions with regard to the confidentiality and security requirements imposed on the controller of personal data processing. Article 16 of the Directive stipulates that any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17 further states that the controller should implement "*appropriate* technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing."

What is meant by "appropriate" depends on the circumstances. Art. 17 only mentions that "having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

The controller finally must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures (by concluding a binding contract with the processor about these items).

3.3.2.2.9 Notification to Data Protection Authority

Prior to the start of a data processing operation, the controller, or his representative, must file a notification with the National Data Protection Authority. This is a key compliance requirement for the controller and non-compliance could result in penalties being imposed[155]. The issue with notification is that notification requirements and exemptions differ greatly among Member States[156]. Therefore, it will first of all be important to determine the applicable national law according to the criteria set out in section 3.3.2.1.4 of this deliverable. When the applicable national law has been determined, the criteria set forth by that national law have to be observed. If the law of several Member States is applicable, the criteria of each of the Member States have to be complied with. Given that national laws may differ considerably, this could lead to notification being required in one Member State while in another Member State an exemption to the notification requirements may apply and there is thus effectively no requirement of notification.

[155] C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 5.42
[156] C. Kuner, *European Data Protection Law*, 2007, Oxford University Press, Oxford, 5.39

3.3.2.3 Judicial Remedies, Liabilities and sanctions

3.3.2.3.1 Remedies

95/46/EC requires Member States to foresee remedies for data subjects. These remedies should allow data subjects to take action against data processing operations.

3.3.2.3.1.1 Administrative remedies

A first type of remedies is administrative remedies. These remedies should allow data subjects to amongst others rectify personal data, obtain erasure or blocking of certain data.

3.3.2.3.1.2 Judicial remedy

The rights granted to the data subject by applicable national law should also foresee judicial safeguards for the data subject. This means that the Data Subject should have access to the judiciary power when he is prejudiced by a data processing operation. Administrative remedies are therefore a necessary remedy but not sufficient. This is in line with ECtHR case-law in relation to the right to a fair trial[157]. It is acceptable that an administrative court different from the judiciary power deals with a matter for as long as an appeal to a judiciary power is possible. It is also a general principle that the public must have access to the judiciary power to seek protection of their fundamental rights and freedoms. And the right to data protection follows from art. 8 ECHR and is as such a fundamental right that must be subject to protection by the judiciary power. The Directive allows for a margin of appreciation for the Members States when implementing the Directive with regard to the rights that are granted to the data subjects. They can award more rights than are mentioned in the Directive, or in some cases the Directive offers a possibility that Member States can decide not to implement.

3.3.2.3.2 Liability

95/46/EC requires the Member States to make the necessary arrangements to enable data subjects to recover damages suffered by illegitimate data processing operations. 95/46/EC does not mention how this should be done and consequently leaves this to the discretion of Member States.

If the controller can prove that he is in no way responsible for the damage suffered by the controller, he can be exempt from liability. In this assessment it is important to keep in mind the responsibilities of the controller already described in previous sections. Consequently, one could assume that an exemption will only be possible if the controller has scrupulously complied with all obligations imposed on him and that despite this compliance the data subject still suffered damage. The preamble to the Directive mentions fault on behalf of the data subject or *force majeure* as grounds for exemption[158].

[157] Art. 6, ECHR
[158] Preamble 55, 95/46/EC

3.3.2.3.3 Sanctions

Member States must foresee sanctions for infringement of the rules of data processing implemented in national law according to 95/46/EC. These sanctions should act as an incentive to increase compliance with data protection rules. These sanctions should be part of a larger set of measures implemented by the Member States to ensure correct implementation of 95/46/EC by the Member States. The specific mentioning of sanctions stresses the importance attached to them by the EU.

3.3.2.4 Transfer to third countries

Directive 95/46/EC holds stringent rules on the transfer of personal data to third countries (countries outside the EU). This transfer is only allowed to third countries that provide an adequate standard of protection of personal data. The countries that have been found to provide adequate protection are very few. The list is published on the website of the European Commission[159]. There are certain initiatives to facilitate transfer to third countries such as the US Safe Harbour Program.

The provisions with regard to the transfer of personal data to third countries are probably not very relevant in the context of ITS. Directive 2004/52/EC on electronic road tolling requires that Service Provider and Toll Charger should have an establishment in the EU. Consequently personal data processing in relation to electronic road tolling will be subject to the rules of the Member State where the Service Provider or Toll Charger has its establishment. What is considered as an establishment under 95/46/EC has been discussed in the aforementioned section of this report.

3.3.3 ITS Framework Directive 2010/40/EU

The ITS Framework Directive holds specific provisions on the processing of personal data in its Article 10. These provisions are the subject of this section. This Article doesn't actually create new legal obligations but essentially refers to the existing legal framework in the area of privacy and personal data protection. Together with the Opinion of the EDPS[160] it provides however a few interesting guidelines on how to apply privacy and data protection rules to the ITS context.

3.3.3.1 Compliance with the existing data protection legal framework

The ITS Directive holds one specific Article in relation to privacy and data protection[161]. A first section of that Article is one commonly used in directives when personal data are addressed[162]. The processing of personal data should be carried out in accordance with Union

[159] http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm

[160] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:047:0006:0015:EN:PDF

[161] Art. 10 1-4, 2010/40/EU

[162] A similar one is used in art. 2.7 of Directive 2004/52/EC on electronic road tolling

rules protecting the fundamental rights and freedoms of individuals, in particular Directive 95/46/EC on the protection of personal data and Directive 2002/58/EC on the protection of data in electronic communications. Since the introduction of the Lisbon Treaty the protection of personal data has gained more importance within the EU as well. Art. 16 TFEU refers to data protection and has general application in EU matters. It has, however, no influence on existing rules. All rules enacted prior to the entry into force of the TFEU are not affected[163]. The legal framework has been discussed in the previous sections of Chapter 3 and consequently reference is made to those sections.

3.3.3.2 Data minimization

When personal data are required they should only be processed insofar as is necessary for the performance of ITS applications and services[164]. This provision refers to the data minimization principle: process as little data as you can. The guiding principle is: "select before you collect"[165]. The European Data Protection Supervisor (EDPS) stresses that this principle should be implemented both in relation to organisational as well as technical aspects of ITS applications and services. Instead of collecting everything and then filtering out the data required and disposing of or securely storing the rest, these systems should be designed in such a way that they only collect the information they need[166].

3.3.3.3 Interoperability

In relation to ITS the EDPS also finds added risk in the requirement of interoperability. This interoperability could entail the interconnection of different databases making data subjects susceptible to data mining and profiling. These technologies aim at cross-referencing data from different sources to build an individual's profile. The problem is that this profile is only based on the data available and not on reality. Additionally, the quality of the criteria used for data mining or profiling may be questionable. The result could be that the profile compiled by the computer is inaccurate or even false. Several examples exist where people have been put on black lists because their name resembles that of a wanted criminal or they are supposed to meet certain criteria that would label them as possible terrorists. The EDPS has also criticized this provision of Directive 2010/40/EU for lacking force. This criticism stems from the fact that the Directive does not contain a list of ITS services and applications. Yet it can be countered by the fact that it is a framework directive, hence not meant to be exhaustive or settle every issue. Detailed regulation of services and applications will happen through separate

[163] H. Hijmans, A. Scirocco, Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?, *Common Market Law Review* 2009, p. 1515

[164] Art. 10.3, 2010/40/EU

[165] B. Jacobs, "Select before you collect", *Mens en Maatschappij* 2005, 1006

[166] J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," In *19th USENIX Security Symposium 2010*, Usenix, 26 pages, 2010.; C. Troncoso, G. Danezis, E. Kosta & B. Preneel, *PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance*, In Workshop on Privacy in the Electronic Society 2007, in Proceedings of the 2007 ACM workshop on Privacy in Electronic Society, Alexandria, Virginia, USA (Session: Privacy preserving services and human factors), pp. 99-107, 2007

directives comparable to Directive 2004/52/EC on electronic road tolling[167], which predates the ITS Directive, or through specifications and standards.

3.3.3.4 Consent

A third provision stresses the importance of observing the rules on consent where applicable. This should especially be done when sensitive personal data are involved. In this regard an e-Call system (see section 2.2.1), which also transmits or connects to a person's medical records, could be given as an example where additional caution should be practiced. The implementation of this requirement will depend on the scope of the ITS application or service. In the case of e-Call there may not be a need for the User to consent to data processing[168]. And some applications will be exclusively consent-based since that is one of the most plausible legitimate grounds to process personal data, apart from the necessity to protect the vital interests of the data subject[169]. With regard to consent, it is important to note that obtaining consent from the User should not be considered a blank cheque to process personal data without any limitations. Every processing of personal data is subject to the general principles that any data processing has to comply with, and specifically the principles of purpose limitation and data minimization of the general Data Protection Directive (95/46/EC). These cannot be overruled by a data subject's consent.

3.3.3.5 Protect against misuse

A fourth provision imposes on Member States the duty to protect personal data against misuse including unlawful access, alteration or loss. The means of choice for the Member States to achieve this requirement is the enactment of specific laws[170]. Many countries have laws punishing illegal interception of electronic communications and the like. It would appear that, where existing national rules are inadequate for dealing with issues related to ITS, these rules should be amended or complemented.

[167] Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community (Text with EEA relevance), *OJ* 30.4.2004, L 166, pp. 124-143

[168] C. Geuens, J. Dumortier, "Mandatory implementation for in-vehicle eCall: Privacy compatible?", *Computer Law & Security Review* July 2010, pp. 385-390, ISSN 0267-3649, DOI: 10.1016/j.clsr.2010.03.009

[169] Art. 7(d), Directive 95/46/EC.

[170] R. Queck, A. De Streel, L. Hou, J. Jost & E. Kosta, *The EU Regulatory Framework Applicable to Electronic Communications*, in L. Garzaniti & M. O'Regan, "Telecommunications, Broadcasting and the Internet". EU Competition Law & Regulation, 3rd ed., Thomson Sweet & Maxwell, I-402

3.3.4 Directive 2002/58/EC on the protection of personal data in electronic communications

The last building block of the European legal framework in the domain of privacy and personal data protection is Directive 2002/58/EC.[171] This Directive (further addressed as "the Communications Privacy Directive") adds some important provisions with regard to security and privacy protection in the electronic communications sector. It contains legal rules with regard to widely debated issues such as network security, unsolicited messages (spam), spyware and cookies, traffic data retention for law enforcement purposes or location based services.

3.3.4.1 Scope and definitions of the Communications Privacy Directive

The provisions of the Communications Privacy Directive apply to the processing of personal data in connection with the provision of "publicly available electronic communications services" within the European Union (article 3.1. of the Communications Privacy Directive).

The concept of "electronic communications services" is defined in article 2(c) of the Framework Directive[172] as a "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting".

In order to fall under the scope of the Communications Privacy Directive, electronic communications services should thus constitute an economic activity ("for remuneration"). However, such remuneration must not necessarily consist of a payment made by the beneficiary of the service. Services which are offered for free and which are financed by third parties (e.g. through sponsoring) are therefore also covered by the Communications Privacy Directive.

The definition of "electronic communication" stems from the Framework Directive as well, and is incorporated by reference in the Communications Privacy Directive. An electronic communication is defined as the "conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed" (article 1 (a) of the Framework Directive).

In an increasingly converging environment, the distinction between private communications and broadcasting becomes more and more difficult to maintain. As a matter of fact, the above mentioned definition of "electronic communication" stemming from the Framework Directive could very well include television and radio broadcasting services to the public at large. Therefore, the Communications Privacy Directive not only refers to the definition of "electronic communication" but also defines the term "communication" as "any information

[171] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Official Journal* of July 31, 2002)

[172] Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF

exchanged or conveyed between a finite[173] number of parties by means of a publicly available electronic communications service". Such communication "does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network", except however "to the extent that the information can be related to the identifiable subscriber or user receiving the information" (article 2 (d) of the Communications Privacy Directive).

The latter exception was clearly inserted in the Directive in order to include certain broadcasting services such as video-on-demand and digital radio (recital 18 of the Directive).

The European regulatory framework for electronic communications services can be juxtaposed to (i) the regulatory framework on information society services and (ii) the one on broadcasting. Whereas broadcasting services and information society services are mainly content-related, electronic communications services are oriented towards the conveyance of signals.

Broadcasting constitutes a point-to-multipoint service. Information society services and electronic communications services however, both constitute point-to-point services. This similarity can make it difficult to determine which rules apply to a given service which can qualify both as an information society service and as an electronic communications service.

For instance, video-on-demand or digital radio services seem to be rather content-related and therefore subject to the rules on information society services. However, as discussed above, the European legislator has chosen to create an exemption to the general carve-out on broadcasting services in order to include such broadcasting services in the regulatory framework of electronic communications services, whenever the individual user or subscriber can be identified.

In light of the ITS context, due care shall be taken in assessing whether a given service falls under the scope of the Communications Privacy Directive. There are two main communication infrastructures covered by the EVITA project: Car-to-Car ("C2C") and Car-to-Infrastructure ("Car2X").[174] EVITA is mainly concerned in addressing communications that take place within the car and communications between the car and the outside world (handled by a "Communications Unit"). In-vehicle communications that take place thanks to in-vehicle wired interfaces are not covered by the e-Communications Privacy Directive since no processing of personal data occurs in connection with the provision of publicly available electronic communications services. However, where in-vehicle communications use a wireless interface, or where communications are sent outside the vehicle to other vehicles or infrastructure elements (roadside units, toll booths, etc.) – which happens with some of the use cases – the e-Communications Privacy Directive applies whenever the transmission can qualify as a processing of personal data made in connection with the provision of publicly available electronic communications services.

Let us take a few examples that aim at applying the current legal framework of the e-Communications Privacy Directive to a few use cases:

1) In Use Case 1 ("Active Brake")[175], a car receives a message that indicates that it is in immediate danger of collision with an object. If there is no timely reaction from the car

[173] Emphasis added.

[174] *See* D2.1, p. 3 and its Figure 1.

[175] *See* D2.1, p. 13.

driver, the car will automatically initiate an emergency braking mechanism to limit or avoid the impact. There are two instances in the flow of communications going on between the cars involved[176] that could be considered as potentially falling under the scope of "publicly available electronic communications services": a) the car-2-X message[177] sent from the Communications Unit ("CU") of the "Car" to the CU of "MyCar"; and b) the emergency braking message from the CU of "Car" to the outside world.[178] Were it *not* the case, communications a) and b) would then be excluded from the scope of the e-Communications Privacy Directive. However, they would still have to comply with the general data protection legal framework Directive 95/46/EC.

2) In Use Case 2 ("Local Danger Warning")[179], a driver is warned in critical situations in which he may have overseen an obstacle, or in order to "extend his view" to help him anticipate dangers. Two types of communications are involved ("Cooperative Awareness Messages", or "CAM's", and "Decentralised Environmental Notifications", or "DEN's). CAM's enable vehicles to share information with each other by broadcasting or geocasting data to all surrounding vehicles or to vehicles within a geographic region, respectively.[180] DEN's enable vehicles to exchange information about events and road conditions (traffic jam, glaze, black ice, etc.) for a certain time and within a certain area by using *geocasting* or broadcasting mechanisms to send messages to surrounding vehicles or vehicles in a geographic region.[181]

To summarize: In the context of EVITA, automotive on-board units ("OBU's") do not fall within the scope of the revised Directive 2002/58/EC unless they are used as part of the provision of "publicly available electronic communications services in public communications networks (...), including public communications networks supporting data collection and identification devices".[182] In the terminology of the European legislation most of the services addressed by EVITA will be "information society services". Nevertheless some provisions of the Communications Privacy Directive will without any doubt be applicable when using automotive on-board networks.

3.3.4.2 Provisions relating to security

The Communications Privacy Directive imposes on the providers of publicly available electronic communications services (hereinafter referred to as "providers of services") a number of obligations relating to security. The Communications Privacy Directive states that the provider must take appropriate technical and organizational measures to safeguard security of its

[176] *See* Figure 7, D2.1, p. 15.

[177] Step No. 4 on Table 1, D2.1, p.16.

[178] Step No. 14 on Table 1, D2.1, p. 16.

[179] *See* D2.1, p. 18.

[180] Car 2 Car Communication Consortium, Manifesto: Overview of the C2C-CC System (version 1.1), 28 Aug. 2007, p. 39, http://www.car-to-car.org/index.php?id=31&L=jqnnjvkailnwrpd .

[181] *See* Car 2 Car Communication Consortium, Manifesto: Overview of the C2C-CC System (version 1.1), 28 Aug. 2007, pp. 44-49, http://www.car-to-car.org/index.php?id=31&L=jqnnjvkailnwrpd .

[182] Article 3, revised Dir. 2002/58/EC by Dir. 2009/136/EC.

services. If necessary this should be done in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk present".

It should be noted that a provider of services, aside from a duty to implement appropriate safety measures, also has a duty of information towards its customers: in case of a particular risk of a breach of security of the network, a service provider must inform its subscribers thereof, even when such risk is beyond the provider's responsibility. In the latter case, the service provider must also inform its customers of any possible remedies, including an indication of the costs which are likely to be involved (article 4.2). Such measures can, for example, consist of specific software or encryption technologies (recital 20).

The provision of information about security risks should be free of charge, but the service provider is entitled to charge the nominal costs attached to provisioning such information, e.g. the cost of the download by a user of an e-mail message containing a security warning (recital 20). Finally, the requirement to inform subscribers of particular security risks does not discharge a service provider from its obligation to take, at its own costs, appropriate and immediate measures to remedy any new and unforeseen security risks and restore the normal security level of the service (recital 20).

Since 2009, the European Union has introduced (through Directive 2009/136/EC that reviews Directive 2002/58/EC) a mandatory data breach notification regime for the telecommunications sector. Pursuant to this Directive, telecommunications and Internet service providers are required to report certain data breaches to their national regulator and affected individuals. At the time of writing, this mandatory security breach notification still needs to be further implemented in the national laws of the Member States.

3.3.4.3 Provisions relating to cookies and spyware

The Communications Privacy Directive contains protective rules relating to the confidentiality of communications and regulates specifically the storing of information and the gaining of access to information that is already stored in the terminal equipment of users and subscribers.[183] In practice, these rules apply to a broad range of situations and they are most probably applicable to automotive on-board units as well. For instance they apply to cookies, which can be a legitimate and even useful tool for the analysis of the effectiveness of an internet website or for the verification of the identity of a user carrying out an online transaction[184], or even to spyware and viruses, which actually constitute an unwarranted intrusion into the private sphere of the users[185].

The 2002 ePrivacy Directive allowed the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a user (or a subscriber) only on the condition that the latter was provided with clear and comprehen-

[183] Article 5(3) ePrivacy Directive.
[184] Recital 25 2002 ePrivacy Directive
[185] Recital 66 Citizens' Rights Directive. The 2002 ePrivacy Directive also made explicit reference to "[s]o-called spyware, web bugs, hidden identifiers and other similar devices" (Recital 24).

sive information and was offered the *right to refuse* such processing.[186] This provision was amended in the frame of the review of the electronic communications legal framework[187].

The new regime introduced a new requirement: the *consent* of the subscriber or the user for the storing of information or the gaining access to information that is already stored in their terminal equipment. In this way, the new provision introduced a stricter regime with regard to the installation and use of cookies, spyware and similar technologies. The introduction of a requirement for consent has sparked a debate with regard to the implementation of this provision, especially as regards the practical impact it may have on the currently used practices relating to cookies.

3.3.4.4 Provisions relating to the processing, storage and retention of traffic and location data

As mentioned above, the Communications Privacy Directive aims at regulating the conveyance of signals rather than the regulation of content. It is therefore not surprising that the Directive contains a number of rules relating to the processing and storage of traffic data and location data. The concept of "traffic data" is defined as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof" (article 2 (b) of the Communications Privacy Directive).

The concept of "location data" is defined as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service" (article 2 (c) of the Communications Privacy Directive).

Article 6.1 of the Communications Privacy Directive provides that both providers of a public communications network (hereinafter referred to as "network operators") and providers of a publicly available electronic communications service who have processed and stored traffic data relating to subscribers and users, must erase or make anonymous such traffic data when it is no longer needed for the purpose of the transmission of the communication. For purposes of billing and interconnection payments, traffic data processing is permissible up to the end of the period during which the bill may be lawfully challenged or payment pursued (article 6.2). In the latter case, the subscriber or user concerned must be informed of the types of traffic data which are processed and of the duration of such processing (article 6.4).

There is an important exception to the ban on traffic data processing and storage mentioned above. However, this exception is subject to a threefold condition. The provider of a publicly available electronic communications service is entitled to process traffic data (i) upon prior consent by the user or subscriber, (ii) for the purpose of marketing his services or for the provision of value added services, and only (iii) to the extent and for the duration necessary for such services or marketing. The consent given by the user or subscriber can be withdrawn at any time (article 6.3). Prior to obtaining consent, the user or subscriber must be informed of the types of traffic data which are processed and of the duration of such processing (article

[186] The old Article 5(3) of the 2002 ePrivacy Directive stated that "Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller […]."

[187] The ePrivacy Directive was amended by the Citizens' Rights Directive.

6.4). It should be noted that this exception is only open to the provider of electronic communications services, and not to the operator of a network.

The Communications Privacy Directive sets forth that only authorized personnel is entitled to process traffic data. The processing of traffic data must be restricted to such persons acting under the authority of network operators and service providers who are "handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service". The processing must be restricted to what is necessary for the purposes of such activities (article 6.5).

Location data other than traffic data which relates to a user or a subscriber of a network or service can only be processed when

(i) such data is made anonymous or
(ii) the user or subscriber has given his consent to such processing for the purposes and for the duration of the provision of a value added service. In the latter case, the user or subscriber must be informed prior to consent of the type of location data which will be processed and of whether the data will be transmitted to a third party with a view to providing value added services (article 9.1).

In cases where consent of the user or subscriber has been obtained, the network operator or service provider must provide for the possibility for the user or subscriber, by simple means and free of charge, to refuse the processing of his/her location data for a given connection to a network or for a given transmission of a communication (article 9.2).

Furthermore, users or subscribers who have given their prior consent to the processing of location data can withdraw such consent at any time (article 9.1).

In parallel to the rules regarding the processing of traffic data, location data can only be processed by persons acting under a network operator's or service provider's authority, or under the authority of a third party providing a value added service. In the latter case, the processing must be restricted to what is necessary for the purposes of providing the value added service. However, unlike the rules on traffic data processing, it is not required that the persons acting under the operator's, provider's or third party's authority only perform certain specific tasks (article 9.3).

3.3.5 Intermediate conclusions on privacy and data protection aspects

The EVITA project aims to develop suitable architectures for secure automotive on-board networks, complementing other projects that focus on protecting communications between vehicles and between vehicles and infrastructure entities. Part of the project is also to provide an analysis of the legal issues related to communications between vehicles and between vehicles and infrastructure entities. The most relevant legal issues appear to exist in the domains of privacy and liability. These are also the legal issues identified in the European ITS Action Plan (Action 5).

Chapter 3 of this report has been dedicated to the legal issues in the domain of privacy and personal data protection. Following are the main conclusions of this Chapter:

As automotive on-board networks incorporate data-gathering and compiling systems into the transportation infrastructure, new privacy implications stemming from the potential misallocation or abuse of collected data are being created.

Therefore Directive 2010/40/EU rightly states in its Recitals 12 and 13 that "the deployment and use of ITS applications and services processing should be carried out in accordance with Union law"

In the previous pages we have tried to further develop what accordance with Union law in this area means and how the two aforementioned directives should be applied in the context of automotive on-board networks.

The EVITA project focuses on a series of general use case categories in order to cover most of the several objectives specifically related to the security of an on-board IT system:

- communication between cars (e.g. local danger warning),
- communication between car and infrastructure (e.g. eCall),
- integration of mobile devices (e.g., CE devices or smart-phones),
- aftermarket applications (e.g. feature activation), and
- workshop and diagnosis processes (e.g. software updates or remote diagnosis

In many, if not all of these cases, data relating to identified or identifiable natural persons will be processed. In most cases this data subject will be the owner and/or the driver of the vehicle. As a consequence the principles with regard to the protection of the fundamental right to respect for the individual's privacy and in particular the provisions promulgated by the European data protection directive will apply. This means, for example, that the controller will have to respect the proportionality and legality rules as explained in this chapter. It further means that, if the use of the on-board network is not regulated by specific legislation (as for example- possibly – for use cases such as eCall or road toll pricing), the introduction of the service will not be possible without the informed consent of the data subject.

At the design stage of each specific service it will be necessary to establish how the data subject can best be informed and how his/her consent can be collected. This will not be simple in all cases because designers will certainly need to solve specific practical questions such as how to include occasional drivers, etc. A particularly difficult problem in this context is the attribution of the roles of controller and processor or, in other words, how to fit these traditional concepts of Directive 95/46/EC in complex ITS processes involving multiple actors.

Since communications between vehicles and between vehicles and infrastructures will occur on publicly available networks, Directive 2002/58/EC comes into play as well. Questions such as the applicability of the mandatory security breach notification to users and public authorities, or how to implement the requirement to collect the prior consent of the user before storing information and gaining of access to information that is already stored in the on-board equipment, can only be solved in the context of every specific use case.

Providing a series of building blocks to enhance the privacy and the protection of personal data in the context of automotive on-board networks, EVITA is essentially a contribution to what is generally called "privacy by design".

4 Liability

ITS applications can lead to complex liability issues. In the ITS Action Plan the European Commission even states that these issues have notably hampered the market introduction of intelligent integrated safety systems, with legal questions regarding product/manufacturer liability and driver responsibility. In the case of automotive on-board networks not only car manufacturers and drivers are involved but a series of other actors can be held liable if damage occurs.

Liability rules impact on the functioning of every market. When entering into legal relationships, people place faith in the rule of law, trusting in the idea that if anything goes wrong 'someone will be liable' for the damage caused to their property as a result of the other party's misconduct. In other words, if the rules agreed between the parties or established by laws and regulations are not followed, the statutory law enforcement instruments and mechanisms will be executed to ensure justice and balance in society. Therefore, the presence of a clear regime for attaching liability promotes trust for the market players.

It should be emphasized, however, that liability regimes are deeply rooted in the national legal traditions of every single jurisdiction. Some European legal instruments – some of which we will deal with in this Chapter – contain provisions about liabilities but these provisions are subsequently integrated in the national liability regimes of every Member State and adapted to the terminology and the logic of the national jurisdiction.

There are nevertheless a few essential principles that are applied everywhere. One of these principles is that liability – defined as the duty to compensate the damage caused – can be determined by contract or by law. In the first case, parties agree among them who will be liable for which damage and under which conditions. This principle underpins the so-called "disclaimers". In the terms and conditions agreed on at the moment of a car sale, a car manufacturer, for example, can state that he will not be liable for damages caused by the wrong manipulation of a device by the car driver. Or a software vendor can mention in an end user license agreement that the he will not be liable for damages caused by the malfunctioning of his product. Or, vice versa, a customer can negotiate a service level agreement with a service provider or a network operator and agree that damages will be compensated if agreed service levels are not realised.

On the other hand, many laws prevent parties to freely establish their mutual liabilities in a contract. And more importantly: damages often occur between people who have never met before and/or never concluded a contract with respect to their liabilities.

Laws often prevent parties to freely contract about their liabilities in order to minimize the risks for consumers. One example is so-called "product liability". Because this concept is quite relevant in the context of this Chapter, we will develop it more into detail in the following pages.

Probably the most frequent situation is, however, the one in which damage leads to liability questions between people who never concluded a contract about this topic. This is what, in certain jurisdictions, is called "tort liability" or "liability for negligence". Generally speaking

this situation is regulated by law. For example the (national) law can stipulate that, if damage is caused by the negligence of a person, the negligent person shall compensate the damage.

The rule just mentioned will probably be the basic rule for tort liability in almost every jurisdiction but its interpretation and its application in concrete circumstances will differ. Over years and centuries legal courts in the national jurisdictions have developed their own jurisprudence about how to apply this basic rule. What is meant by "damage"? Which kind of damage will be taken into account? How to provide evidence of the damage? What is meant by "negligence"? Who should provide the proof that someone has been negligent? Which kind of causal relationship should there be between the negligence and the damage occurred? Etc. Answers to these questions are provided by the jurisprudence of the national courts but often also by other sector-specific or general legal rules. For example, in the previous Chapter, we have referred to Article 23 of the European data protection Directive 95/46/EC in which it is stipulated that "*any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered*" and further that "*the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage*".

In the following pages we will give an overview of some of the most relevant European legal instruments which have to be taken into account for determining liabilities for damages occurring in the automotive sector. The first series of these legal instruments deal with vehicle type approval. In case of a road accident presumably caused by a dysfunction of the vehicle or some of its parts, liability will evidently be influenced by an answer to the question whether the vehicle has been correctly built.

4.1 Vehicle Type Approval

4.1.1 Introduction

The importance and impact of vehicles on society are such that road vehicles have long been subject to specific certification and approval systems. In Europe there are two approval systems relating to vehicles:

- a system based on United Nations Economic Commission for Europe (UNECE) Regulations is used for type approval of automotive components and systems;
- EC Whole Vehicle Type Approval (WVTA), which is based on EC directives and provides for type approval of whole vehicles, vehicle systems and components. [189]

Although EC WVTA initially only applied to passenger cars (from 29th April 2009), the timetable for enforcement covers all new road vehicles and trailers by 29th October 2014[190]. In addition, Directive 2007/46/EC also covers national schemes for small series vehicles (limited

[189] Directive 2007/46/EC of The European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, *O.J.* 9/10/2007, L 263

[190] Annex XIX, 2007/46/EC

production) and individual approvals. The UNECE Regulations are part of the EC WVTA in the same way as the separate directives or regulations[191].

4.1.2 Goal

The goal of EC WVTA is to prevent trade barriers whilst at the same time ensuring the safety performance and restricting the environmental impact of vehicles and their subsystems and components in accordance with relevant regulations. If a production intent prototype passes the tests and the production arrangements also pass inspection, then other vehicles, sub-systems or components *of the same type* are approved for production and sale within Europe. Thus, the need to test every single one, or even to undertake more limited testing to obtain approval in every single country, is avoided. This significantly reduces certification costs and lead time, resulting in benefits for the manufacturer, importer and consumer.

4.1.3 Scope

The scope of Directive 2007/46/EC includes "*vehicles designed and constructed in one or more stages for use on the road, and of systems, components and separate technical units designed and constructed for such vehicles*", as well as "*parts and equipment intended for vehicles covered by this Directive*".[192]

Specified exclusions to 2007/46/EC include:

- agricultural or forestry tractors, which are subject to a specific framework directive[193];
- quadricycles, which are subject to a specific framework directive for two- and three-wheeled motor vehicles[194];
- tracked vehicles.

Furthermore, approval under 2007/46/EC is optional for the following classes of vehicles:

- vehicles intended exclusively for racing on roads;
- prototypes used on the road under the responsibility of a manufacturer to perform a specific test programme provided that they have been specifically designed and constructed for this purpose.

Those vehicles that are within the scope of 2007/46/EC are described in terms of a number of different categories[195]. For example, category M encompasses "*vehicles with at least four wheels designed and constructed for the carriage of passengers*", and those vehicles with "*no*

[191] Art. 34 2007/46/EC

[192] Art. 2 2007/46/EC

[193] Directive 2003/37/EC of the European Parliament and of the Council of 26 May 2003 on type-approval of agricultural or forestry tractors, their trailers and interchangeable towed machinery, together with their systems, components and separate technical units, *O.J.* 9/7/2003, L 171. Directive as last amended by Council Directive 2006/96/EC, O.J. 20/12/2006, L 363, p. 81

[194] Directive 2002/24/EC of the European Parliament and of the Council of 18 March 2002 relating to the type-approval of two or three-wheel motor vehicles, *O.J.* 9/5/2002, L 124. Directive as last amended by Council Directive 2006/96/EC, O.J. 20/12/2006, L 363, p. 81

[195] Annex II.A, 2007/46/EC

more than eight seats in addition to the driver's seat" (e.g. passenger cars) fall into the sub-category denoted M_1. Further sub-categories of passenger vehicles (category M) encompass those with more than eight passenger seats (i.e. busses and coaches), including M_2 (with mass less than 5 tonnes) and M_3 (with mass greater than 5 tonnes). Other vehicle categories defined in 2007/46/EC include vehicles designed and constructed for the carriage of goods (category N, again with three sub-categories), trailers and semi-trailers (category O, which has four sub-categories), and off-road vehicles (category G).

4.1.4 Requirements

Type approval is a formal process that in general requires third party testing by a recognised Technical Service and approval by a Type Approval Body. Each framework directive specifies the range of aspects of the vehicles that must be approved to separate technical directives. In addition to testing, type approval includes a Conformity of Production (COP) element[196]. COP requirements are based around established quality systems principles and, in general, certification to ISO 9001[197] may be an acceptable basis. An approval issued by one Authority will be accepted in all the Member States.

The requirements for WVTA focus on the key safety and environmental issues which have been recognised over the years.

The specific type approval requirements vary between the various categories of vehicle defined in 2007/46/EC, as specified in the tables of Annex IV Part 1 of this Directive, reflecting the differing operational roles of these vehicle categories.

Each Member State is required to appoint an Approval Authority to issue the approvals, and a Technical Service to carry out the testing to the Directives and Regulations. Organisations designated as Technical Services must demonstrate the necessary skills and competences in the relevant fields, and are subject to assessment of their capabilities at least every three years[198]. The Technical Service may fall into one or more of the following four categories, depending on their field of competence:

- **Category A:** technical services which carry out in their own facilities the tests referred to in this Directive and in the regulatory acts listed in 2007/46/EC Annex IV.
- **Category B:** technical services which supervise the tests referred to in this Directive and in the regulatory acts listed in 2007/46/EC Annex IV, performed in the manufacturer's facilities or in the facilities of a third party.
- **Category C:** technical services which assess and monitor on a regular basis the manufacturer's procedures for controlling conformity of production.
- **Category D:** technical services which supervise or perform tests or inspections in the framework of the surveillance of conformity of production.

[196] Art 12, 2007/46/EC
[197] ISO 9001:2008, "Quality management systems — Requirements"
[198] Art. 41, 2007/46/EC

In fact, an Approval Authority may itself act as a Technical Service for any one or more of these roles[199].

4.1.5 Process

The main steps involved in the WVTA process are:

- application by the vehicle or component manufacturer;
- testing by a technical service;
- granting of the approval by an Approval Authority;
- Conformity of Production established by the manufacturer in agreement with the Approval Authority;
- Certificate of Conformity by the manufacturer for the end-user.

There are multiple methods available for type approval. For whole vehicles, manufacturers may select one of the following[200]:

- **Step-by-step Type Approval:** a vehicle approval procedure consisting in the step-by-step collection of the whole set of EC type-approval certificates for the systems, components and separate technical units relating to the vehicle, and which leads, at the final stage, to the approval of the whole vehicle.
- **Single-step Type Approval:** a procedure consisting in the approval of a vehicle as a whole by means of a single operation.
- **Mixed Type Approval:** a step-by-step Type Approval procedure for which one or more system approvals are achieved during the final stage of the approval of the whole vehicle, without it being necessary to issue the EC Type Approval certificates for those systems.
- **Multi-stage Type Approval:** the procedure whereby one or more Member States certify that, depending on the state of completion, an incomplete or completed type of vehicle satisfies the relevant administrative provisions and technical requirements of this Directive.

The multi-stage type-approval may be used for complete vehicles that are converted or modified by another manufacturer[201].

4.1.6 Recall of vehicles[202]

If one or more systems, components or separate technical units fitted to a vehicle (whether or not duly approved in accordance with Directive 2007/46/EC) presents a serious risk to road safety, public health or environmental protection, a manufacturer who has been granted an EC

[199] Art. 41.5, 2007/46/EC
[200] Art. 6, 2007/46/EC
[201] Art. 9.2, 2007/46/EC
[202] Art. 32, 2007/46/EC

vehicle type-approval is obliged, in application of the provisions of a regulatory act or of the General Product Safety Directive (see Section 4.3 for further detail), to undertake to:

- recall the affected vehicles already sold, registered or put into service;
- immediately inform the Approval Authority that granted the vehicle approval;
- propose to the Approval Authority a set of appropriate remedies to neutralise the risk.

The Approval Authority is required to communicate the proposed measures to the authorities of the other Member States without delay. The competent authorities are then required to ensure that the measures are effectively implemented in their respective territories. If the measures are considered to be insufficient by the authorities concerned, or have not been implemented quickly enough, they are then required inform the approval authority that granted the EC vehicle type-approval without delay. The Approval Authority is then required to inform the manufacturer.

If the Approval Authority which granted the EC type-approval is itself not satisfied with the measures of the manufacturer, it is required to undertake all necessary protective measures, including the withdrawal of the EC vehicle type-approval where the manufacturer does not propose and implement effective corrective measures. In case of withdrawal of the EC vehicle type-approval, the concerned Approval Authority must notify (by registered letter or equivalent electronic means) the following organisations within 20 working days:

- the manufacturer;
- the approval authorities of the other Member States;
- the Commission.

These provisions also apply to vehicle parts that are not subject to any requirement under a regulatory act[203].

4.1.7 Recent developments of relevance to EVITA

4.1.7.1 Policy objectives

Directions for future automotive policy were investigated by the CARS 21 High Level Group, which brought together the main stakeholders (including member states, industry, non-governmental organizations and MEPs) in 2005 with the aim of examining the main policy areas impacting on the European automotive industry and making recommendations for future public policy and regulatory framework. The review conducted by CARS 21[204] concluded that the current type-approval system was effective, that it should be maintained, and that most of the legislation was necessary and useful in the interest of protecting health, safety, consumers and the environment. Nonetheless, a total of 38 EC Directives were identified that could be repealed and replaced with corresponding international UNECE regulations. In

[203] Art. 32.4 2007/46/EC

[204] COM (2007) 22, Communication from the Commission to the European Parliament and Council: A Competitive Automotive Regulatory Framework for the 21st Century - Commission's position on the CARS 21 High Level Group Final Report, 7/2/2007

addition, a series of measures to be considered in the area of road safety were also identified, and intelligent vehicles and roads were listed amongst the core research priorities.

Specific aims that were identified by the CARS 21 High Level Group which are of relevance to the EVITA project include the following:

- To investigate the costs, benefits and feasibility of introducing "emergency braking systems" (EBS) in vehicles (particularly heavy-duty vehicles).
- Proposals to make the inclusion of "electronic stability control" (ESC) mandatory, starting with heavy-duty vehicles and followed by passenger cars and light-duty vehicles.
- To continue efforts to promote the development, deployment and use of active in-vehicle safety systems and vehicle-infrastructure co-operative systems in the framework of the i2010 Intelligent Car Initiative[205].
- To adopt the 3rd eSafety Communication[206], which brings to the attention of the European Parliament and Council further measures aiming at full deployment of eCall starting from 2010.
- To encourage and support the conditioning of Community financing in the road sector to projects which follow best practice in road safety.
- Call on the Member States to further improve the enforcement of bans on drunk driving, enforcement of speed limits, enforcement of motor-cycle helmet use and to promote and enforce seat-belt use.

The pursuit of these aims has already resulted in amendments to Directive 2007/46/EC, and more can be expected in the future. In particular, a requirement for Brake Assist Systems (BAS) was introduced in EC Regulation 78/2009[207] in order to enhance the protection of pedestrians and other vulnerable road users. Furthermore, Annex V of EC Regulation 78/2009 also amends Directive 2007/46/EC to include the requirements of EC Regulation 78/2009 as an additional type approval topic under the heading "Pedestrian Protection".

4.1.7.2 Brake Assist Systems

In order to support the implementation of EC Regulation 78/2009, specifications and test methods for BAS are described in EC Regulation 631/2009[208]. The latter describes three slightly different categories of BAS, which are defined as follows:

[205] COM (2006) 59, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: On the Intelligent Car Initiative – Raising Awareness of ICT for Smarter, Safer and Cleaner Vehicles, 15/2/2006

[206] COM (2006) 723, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Bringing eCall back on track – Action Plan, 23/11/2006

[207] Commission Regulation (EC) No 78/2009 of the European Parliament and of the Council of 14 January 2009 on the type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users, amending Directive 2007/46/EC and repealing Directives 2003/102/EC and 2005/66/EC, *O.J.*, 4/2/2009, L35, pp. 1-31

[208] Commission Regulation (EC) No. 631/2009 of 22 July 2009 laying down detailed rules for the implementation of Annex I to Regulation (EC) No 78/2009 of the European Parliament and of the Council on the

- **Category A:** detects an emergency braking condition based on the brake pedal force applied by the driver;
- **Category B:** detects an emergency braking condition based on the brake pedal speed applied by the driver;
- **Category C:** detects an emergency braking condition based on multiple criteria, one of which shall be the rate at which the brake pedal is applied.

The required performance characteristic for BAS of Category A is that when an emergency condition has been sensed by a relatively high pedal force, the additional pedal force to cause full cycling of the ABS (Anti-lock Braking System) shall be reduced compared to the pedal force required without the BAS in operation. For categories B and C, when an emergency condition has been sensed, at least by a very fast application of the brake pedal, the BAS shall raise the pressure to deliver the maximum achievable braking rate or to cause full cycling of the ABS.

All three BAS categories require the driver to be involved in the braking action, and only unusual brake pedal demand can activate BAS operation for categories A and B. Although the description of Category C offers the opportunity to include inputs from other sources, it would appear that activation of Category C BAS functions must be instigated by driver activity (since the driver is still required to be making an unusual brake pedal demand). Thus, the driver remains the initiator of the braking action, although the nature of his brake pedal demand (and possibly other information sources, for BAS of Category C) may result in the braking system providing different performance characteristics than those that result under less extreme conditions of brake pedal demand.

The provisions of EC Regulation 78/2009 include requirements for all new vehicles of class M_1 (i.e. vehicles designed to carry no more than 8 passengers), as well as N_1 vehicles (i.e. goods vehicles up to 3,5 tonnes) that are derived from M_1 vehicles, to provide BAS functionality from 24th November 2009.

4.1.7.3 Advanced Vehicle Systems

Article 19 of EC Regulation 661/2009[209] lists the 38 EU directives identified by the CARS 21 High Level Group for repeal and replacement by corresponding international UNECE regulations (with effect from 1st November 2014), while Annex III of this regulation describes amendments to Directive 2007/46/EC to include the requirements of EC Regulation 661/2009 as an additional type approval topic under the heading "General Safety".

Among the motivations for EC Regulation 661/2009 it is noted that:

type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users, amending Directive 2007/46/EC and repealing Directives 2003/102/EC and 2005/66/EC, *O.J.*, 25/7/2009, L 195, pp. 1-60

[209] Commission Regulation (EC) No. 661/2009 of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor, O.J., 31/7/2009, L 200, pp. 1-24

- *"Technical progress in the area of advanced vehicle safety systems offers new possibilities for casualty reduction. In order to minimise the number of casualties, it is necessary to introduce some of the relevant new technologies."*
- "*The timetable for the introduction of specific new requirements for the type-approval of vehicles should take into account the technical feasibility of those requirements. In general, the requirements should initially apply only to new types of vehicle. Existing types of vehicle should be allowed an additional time period to comply with the requirements. Furthermore, mandatory installation of tyre pressure monitoring systems should initially apply only to passenger cars. Mandatory installation of other advanced safety features should initially apply only to heavy goods vehicles."*

The new requirements of EC Regulation 661/2009 include provisions for a number of such new technologies. In particular, Article 10 (concerning "advanced vehicle systems" (AVS)) requires vehicles in the categories M_2, M_3, N_2 and N_3 (i.e. busses capable of carrying more than 8 passengers, and goods vehicles exceeding 3,5 tonnes) should be equipped with an "advanced emergency braking system" (AEBS) and a "lane departure warning system" (LDWS). Furthermore, Article 12 requires vehicles of a wide range of vehicle classes, including the more numerous M_1 and N_1 types, to be equipped with "electronic stability control" (ESC). The requirement for "tyre pressure monitoring systems" (TPMS), initially for vehicles of category M_1, is set out in Article 9 of EC Regulation 661/2009. It should be noted, however, that the feasibility of attacking vehicle systems by exploiting security vulnerabilities in the wireless communications of a TPMS has already been reported[210].

Such developments are not unique to the EU. Installation of TPMS[211] has been mandated by the USA's National Highway Traffic Safety Administration (NHTSA) for all new light motor vehicles since September 2007. A requirement for ESC systems[212] has also been issued by the NHTSA, to be implemented from 2012 for a number of vehicle classes including passenger cars and busses. Similar measures have already been announced for Australia, Canada and Korea, and ESC regulation is under consideration in Japan[213].

Compliance with the requirements of Article 12 of EC Regulation 661/2009 (concerning ESC) is required for M_1 and N_1 vehicles from 1st November 2011. The schedule for introducing ESC in other vehicle classes (which is set out in Annex V of EC Regulation 661/2009) is variable, ranging from 1st November 2011 to 11th July 2016. Detailed rules concerning the specific procedures, tests and technical requirements for type-approval of systems relating to Article 10 (i.e. AEBS and LDWS) are required to be adopted by 31st December 2011, and installation of these systems is to be mandatory for new vehicles in classes M_2, N_2, M_3 and N_3 from 1st November 2015[214]. Compliance with the requirements of Article 10 of EC Regulation

[210] I. Rouf *et al*, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study", *Proceedings of 19th USENIX Security Symposium*, August 2010

[211] U.S. Department Of Transportation, National Highway Traffic Safety Administration, Federal Motor Vehicle Safety Standard FMVSS No. 138, 49 CFR, Parts 571 & 585: Tire Pressure Monitoring Systems

[212] U.S. Department Of Transportation, National Highway Traffic Safety Administration, Federal Motor Vehicle Safety Standard FMVSS No. 126, 49 CFR, Parts 571 & 585: Electronic Stability Control Systems

[213] Bosch Corporation (Japan), "Electronic Stability Control ESC on the rise in Japan", Press Release, September 2010, available online at: http://www.bosch.co.jp/en/press/rbjp-1009-02.asp

[214] Art 13.13, EC Regulation No. 661/2009

661/2009 regarding TPMS for category M_1 vehicles[215] (i.e. passenger cars) is required in Europe from 1st November 2012.

The advanced vehicle systems that are specifically mentioned in EC Regulation 661/2009 are defined as follows:

- **"Advanced emergency braking system" (AEBS):** a system which can automatically detect an emergency situation and activate the vehicle braking system to decelerate the vehicle with the purpose of avoiding or mitigating a collision;
- **"Electronic stability control" (ESC):** an electronic control function which improves the dynamic stability of the vehicle;
- **"Lane departure warning system" (LDWS):** a system to warn the driver of unintentional drift of the vehicle out of its travel lane.

The implication of these descriptions is that, unlike the BAS described in EC Regulation 631/2009, the driver is not necessarily involved in initiating the actions of the AEBS or of the ESC. Technical requirements and test methods for ESC systems to be used in lighter vehicles (such as classes M_1 and N_1) are already described in Annex 9 of UNECE Regulation No. 13-H (introduced in Amendment 2 to Revision 1 of Regulation No. 13-H[216]). However, security against malicious interference is not included in these specifications. Regulations relating to AEBS and LDW systems are still under development by UNECE[217].

A report commissioned by the EC on the subject of automated emergency braking systems[218] identifies three categories of such systems:

- **"Collision avoidance systems" (CAS)**: sensors detect a potential collision and take action to avoid it entirely, taking control away from the driver.
- **"Collision mitigation braking systems" (CMBS)**: sensors detect a potential collision but take no immediate action to avoid it until it becomes unavoidable, at which point automatic braking is applied (independent of driver action) in order to reduce the speed, and hence the severity, of the inevitable collision. Such systems may also trigger additional actions, such as pre-optimisation of occupant restraints.
- **"Forward collision warning" (FCW)**: sensors detect a potential collision and take action to warn the driver. Such systems could also be used to optimize occupant restraints.

Systems providing forward collision warning functions have been available on some EU vehicles since 1999. However, only the "collision avoidance" and "collision mitigation braking systems" outlined above correspond to the concept of AEBS as defined in EC Regulation 661/2009. Nonetheless, "forward collision warning" may perhaps be a necessary adjunct to "collision avoidance" in order to avoid contravening other legal requirements concerning the control of vehicles (see section 4.2.1 below).

[215] Art 9(2), EC Regulation No. 661/2009

[216] UNECE Regulation No. 13-H, "Uniform provisions concerning the approval of passenger cars with regard to braking", Revision 1 – Amendment 2, 11/11/2009

[217] UNECE, "Draft report on 6th meeting of the GRRF informal group on Advanced Emergency Braking and Lane Departure Warning Systems", AEBS/LDWS-06-13, 3/9/2010

[218] C. Grover *et al.*, "Automated Emergency Braking Systems: Technical requirements, costs and benefits", TRL (UK), Report PPR 227, April 2008

4.1.8 Future developments of relevance to EVITA

The Commission's ambition was originally to launch the full pan-European eCall service in 2009, with the voluntary participation of national authorities. However, a small number of MS were concerned about the potential infrastructure costs, and the system is not yet operational in any EU country. More recent proposals were for the first systems to appear in 2011, with eCall to be installed in all new cars sold in Europe by 2014[219]. The Commission therefore planned[220] to issue a proposal in 2010 for a new regulation under the WVTA legislation for the mandatory introduction of eCall equipment, initially for passenger cars and light commercial vehicles. In practice, however, the timing will depend on the willingness of national authorities to upgrade their emergency response systems to accommodate eCall.

Recent proposals concerning road safety policy directions for 2011-2020[221] also reiterate the interest in eCall. This document calls for the possibility of widening the deployment of "advanced driving assistance systems" (ADAS) by retrofitting them to existing commercial and/or private vehicles to be further assessed. In addition, the role of vehicle technology in enforcing speed limits is also discussed, although only in the context of speed limiters for light commercial vehicles. The latter appears to be prompted by as much environmental concerns[222] as by road safety considerations. Thus, there would appear to be no current plans for actively promoting the deployment of "intelligent speed adaptation" (ISA) systems, and therefore no intention to extend the existing WVTA legislation to include such systems in the near future.

The future deployment of "collision avoidance systems" (CAS) is already anticipated[223] in EC Regulation 78/2009, which notes that, subject to assessment by the Commission, vehicles that are equipped with CAS may be exempted from a certain subset of the type approval test requirements. The requirements that are alluded to are intended to establish the performance of vehicle structural features[224] that should help to reduce the severity of injuries to pedestrians and other vulnerable road users that might arise from accidental impacts. The implication here is that it is expected that at least some CAS will be able to detect and avoid potential collisions with pedestrians and other vulnerable road users (i.e. cyclists, motorcyclists, horses and their riders, as well as infirm and disabled users of low-speed personal mobility vehicles), thus obviating the need to employ structural design measures to limit the severity of impacts between the vehicle and human bodies. However, these structural measures aim primarily to

[219] IP/09/1245, "Last call to implement car safety system voluntarily", Brussels, 21/08/2009

[220] COM (2009) 434, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: eCall – Time for deployment, 21/8/2009

[221] COM (2010) 389, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Towards a European road safety area – policy orientations on road safety 2011-2020, 20/7/2010

[222] COM (2009) 593, Proposal for a Regulation of the European Parliament and of the Council setting emission performance standards for new light commercial vehicles as part of the Community's integrated approach to reduce CO2 emissions from light-duty vehicles, 28/10/2009

[223] Art. 11, EC Regulation No. 78/2009

[224] Annex I, Sect. 2–3, EC Regulation No. 78/2009

reduce injury to pedestrians and may not actually meet the needs of cyclists[225] and other vulnerable road users.

Further developments are also anticipated for the future in EC Regulation 661/2009, which notes that:

- *"The Commission should assess the feasibility of extending the mandatory installation of tyre pressure monitoring systems, lane departure warning systems and advanced emergency braking systems to other categories of vehicle and, if appropriate, propose an amendment to this Regulation."*[226]
- *"The Commission should continue to assess the technical and economic feasibility and market maturity of other advanced safety features, and present a report, including, if appropriate, proposals for amendment to this Regulation, by 1 December 2012, and every three years thereafter."*[227]

Thus, the status of advanced safety technologies will be reviewed in December 2012, and at regular 3-yearly intervals thereafter, and proposals made for amendments to the legislation in order to promote the deployment of further advanced safety features – that are deemed to be sufficiently mature – in future vehicles.

The intention behind such legislation is that mandatory installation will increase the pace of market penetration, which is likely to lead to a reduction in costs, thereby ensuring that society benefits (sooner rather than later) from the improvements in road safety, enhanced transport efficiency and reduced environmental impacts that new technologies are expected to deliver. A possible concern, however, is that reliance on such technology may result in drivers being willing to take greater risks which may have the effect of negating some of the benefits for road safety.

4.1.9 Beyond type approval

The EC WVTA legislation specifies a common set of minimum requirements that vehicles must meet before they can be placed on the market. However, many vehicle manufacturers aim to exceed these minimum requirements, and instead employ their own in-house specifications. Their objectives in doing this include ensuring reliability and customer satisfaction, as well as providing a degree of future-proofing against potential changes in the operating environment over the lifetime of the vehicle.

In addition to this, a number of independent organizations in Europe carry out assessments of vehicles that also go beyond WVTA requirements, particularly in relation to vehicle safety and security, and make these results available to the public. These activities are motivated by government and consumer organisations, as well as by the insurance industry, who wish to promote enhanced safety for vehicle occupants and pedestrians during accidents, as well as improved levels of security against theft of vehicles and theft from vehicles.

[225] SWOV Fact sheet R-2003-33 "Fietser-autofront", 4/07/2004
[226] Page 3, EC Regulation No. 661/2009
[227] Page 2, EC Regulation No. 661/2009

4.1.9.1 Euro NCAP

The "European New Car Assessment Programme" (Euro NCAP)[228] organises crash-tests and provides consumers with a realistic and independent assessment of the safety performance of some of the most popular cars sold in Europe. However, part of the motivation for Euro NCAP is also to encourage vehicle manufacturers to exceed the minimum legislative requirements relating to vehicle safety.

Euro NCAP was initially established for the UK Department of Transport by the UK's Transport Research Laboratory. However, other governments have since joined the programme (including France, Germany, Sweden, The Netherlands and the Spanish region of Catalonia), and many European consumer groups are members through the International Consumer Research and Testing organisation. Automobile clubs are represented by membership of the FIA Foundation and by the individual membership of the German automobile club ADAC and the Automobile Club d'Italia. The European Commission is an observing member of Euro NCAP's board and provides their political support. This wide consortium of members ensures its independence. Euro NCAP is now an International Association under Belgian law, and is totally independent of the automotive industry and political control. No individual member can bias Euro NCAP in favour of their individual interests.

For comparison purposes the testing has to be carried out to more rigorous standards than is necessary to demonstrate compliance with the legislative requirements of EC WVTA. Consequently, a comprehensive suite of tests was developed to allow vehicles to be rated in terms of three key safety attributes: adult protection, child protection, pedestrian protection. Ongoing development has resulted in a fourth attribute, safety assistance, being included in Euro NCAP evaluations since 2009. The safety assistance category includes features such as seatbelt reminders, speed limiters and ESC systems. It is to be expected that the scope of Euro NCAP testing will be further extended to include merging safety-related driving assistance technologies in the future.

4.1.9.2 Thatcham

The UK's "Motor Insurance Repair Research Centre" (known as "Thatcham"[229], after its location) was established by British insurers in 1969. The purpose of this organisation is to carry out research aimed at containing or reducing the cost of vehicle insurance claims, whilst also improving safety and security. This research also helps vehicle manufacturers to produce designs which both limit damage and improve the ease of repair following an accident. In addition, Thatcham has been a member of Euro NCAP since 2004.

Since 1992 Thatcham has also been working to improving the security of passenger cars aiming to reduce thefts of and from vehicles. The scheme was subsequently extended to include light commercial vehicles (1996), heavy commercial vehicles (1997), and motorcycles (1999). Increasing the level of security fitted as standard to vehicles and improving the quality of installation of security systems have helped minimise insurance premiums and

[228] http://www.euroncap.com
[229] http://www.thatcham.org

reduce insurers' costs. In the UK, all existing and new vehicles are issued with a car insurance group (which ranges from one to 20) by the Association of British Insurers (ABI). The insurance group, along with other risk factors, such as age, experience and home address, are used to determine the resulting insurance premium. Factors that are considered in allocating the insurance group for a vehicle include engine size, performance and cost of the vehicle, as well as safety and security features. Thatcham provides some 70% of the data, relating to safety and security, which the ABI use to decide on the insurance grouping of cars.

Thatcham produces a New Vehicle Security Rating (NVSR) for all new vehicles that are assessed. The NVSR provides a 5 star rating system for passenger cars, with separate rankings for "theft of" the vehicle and "theft from" the vehicle. The "theft of" category assesses the ability of a vehicle to resist attempts to steal the vehicle, testing aspects such as the immobiliser, locks and vehicle identification. The "theft from" category assesses the ability of the vehicle to resist unlawful entry, encompassing features such as alarms, door locks and glazing. The NVSR for heavy goods vehicles uses a 10 star rating system. The NVSR also provides the basis for the annual British Insurance Vehicle Security Awards, which recognize the efforts of those manufacturers who have produced the most secure new cars.

Initially, the assessment requires the vehicle manufacturer to complete an application form describing the security system. This is followed by physical attack tests on the vehicle as well as laboratory tests on the components of the security system. The attack tests include breaking into the vehicle through the boot, bonnet or doors, overcoming steering locks and trying to start the engine without the original vehicle keys. The result is a score that can change the insurance rating of a car by up to two groups, depending on the perceived risk of theft.

In addition, Thatcham also tests alarms, immobilisers and other security systems that are intended for after-market fitment. These security systems can be fitted to vehicles that may not have had an alarm or immobiliser as standard equipment, and may help to reduce insurance costs if the equipment achieves particular Thatcham security ratings.

At present the security aspects addressed by Thatcham assessments do not include the types of security threats that are envisaged in the EVITA dark-side scenarios. However, it is likely that assessment of in-vehicle network security will become part of the Thatcham requirements as automotive technology currently under research reaches sufficient maturity for commercial deployment.

4.2 Advanced Vehicle Systems

4.2.1 Vienna Convention on Road Traffic

The 1968 Vienna Convention on Road Traffic[230] is an international treaty that aims to facilitate international road traffic and to increase road safety through the adoption of uniform road traffic rules. In the signatory countries it replaces previous road traffic conventions, most notably the 1949 Geneva Convention on Road Traffic[231]. However, a number of countries

[230] Convention on Road Traffic, Vienna, 8/11/1968, as amended on 3/9/1993 and 28/3/2006

[231] Convention on Road Traffic, Geneva, 19/9/1949, available on-line at http://en.wikisource.org/wiki/Geneva_Convention_on_Road_Traffic

(most notably Australia, China, India, New Zealand and the USA) are not signatories to the 1968 Vienna Convention, with the result that the 1949 Geneva Convention still applies in these regions.

With regard to advanced vehicle systems, it should be noted that the Vienna Convention requires (see Article 8) that:

- *"Every moving vehicle or combination of vehicles shall have a driver".*
- *"Every driver shall at all times be able to control his vehicle or to guide his animals".*
- *"A driver of a vehicle shall at all times minimize any activity other than driving".*

Similar provisions are also to be found in the 1949 Geneva Convention[232].

The objective of minimizing driver distraction has resulted in an additional requirement to prohibit the use of hand-held mobile phones while driving, which (along with a number of other amendments) was adopted in 2003[233].

Relevant definitions[234] are as follows:

- *"**Combination of vehicles** means coupled vehicles which travel on the road as a unit".*
- *"**Driver** means any person who drives a motor vehicle or other vehicle (including a cycle), or who guides cattle, singly or in herds, or flocks, or draught, pack or saddle animals on a road".*

Thus, in terms of the Vienna Convention, a driver must be a person, not a system, and must always be able to control the vehicle, or combination of coupled vehicles or animals.

4.2.1.1 Driving Assistance Systems

The ABS and BAS systems provide enhanced braking support, but both of these functions require the driver to initiate them by applying the brakes. Thus, they can be considered as "driving assistance systems" (DAS), with the driver remaining in control. The situation is similar for "cruise control" (CC), which is used to maintain a fixed speed, and "adaptive cruise control" (ACC), which tracks the speed of the vehicle in front by means of a radar system. These systems are manually engaged by the driver, who continues to drive the vehicle, and either manually disengaged or automatically disengaged (e.g., if the foot pedals are depressed, or if the speed of the vehicle in front falls below a threshold level). Thus, the driver remains in overall control of the vehicle and is able to override these systems when necessary.

However, the driver is already no longer in control, by definition, in situations where a collision has become unavoidable. Thus, the use of ADAS, which can provide some degree of mitigation in circumstances that are beyond the control of the driver, is probably justifiable as not contravening the requirements of the Vienna Convention.

The concept of "controllability" for automotive applications was originally developed by the EU project "DRIVE Safely"[235], and is now used as a qualitative probability measure in

[232] Art. 8, Geneva Convention

[233] UNECE Inland Transport Committee Working Party of Road Traffic Safety, "Proposals for amendments to the Vienna Convention on Road Traffic", TRANS/WP.1/2003/1/Rev.4, 23 April 2004

[234] Art. 1, Vienna Convention

safety risk analysis methods that are applied to vehicle engineering[236] and on-board software development[237]. Controllability is also considered for safety-related security risks in the security risk analysis approach developed in Task 2300 of EVITA[238]. Approaches for evaluating controllability and undertaking risk assessments in the development of driver assistance systems have been proposed in the Code of Practice developed by the EU project "RESPONSE 3"[239].

In terms of this driver controllability criterion[240], "collision mitigation braking systems" (CMBS) do not contravene the Vienna Convention, but this is not so for CAS, where the objective of the system is to take control from the driver before a collision becomes unavoidable (i.e. while the situation is still judged to be controllable).

In order to avoid contravention of the Vienna Convention by DAS, it has also been proposed[241] that:

> *"The system must only "override" the driver if the latter is unable to intervene (e.g. loss of consciousness) and this is evident from the driver's failure to respond to certain information provided by the system. Automatic instant emergency braking initiated by a braking assistant in a speeding situation could impact vehicle handling and lead to the wrong reactions".*

In order to comply with this position, a CAS would need to warn the driver of the impending hazard and only take action if the driver fails to respond within a reasonable period of time (thereby demonstrating a lack of driver control of the situation, due to inattention or some form of physical incapacity). This would give a driver who is able to control the situation the opportunity to override the action of the CAS.

However, ESC systems, which may apply increased or decreased braking pressure amongst other actions (rather than just reduced braking pressure as in ABS), are intended to operate automatically without direct driver initiation at vehicle speeds in excess of 20 km/hour unless the driver has disabled the system or the vehicle is being driven in reverse[242]. Such systems would comply with the Vienna Convention if, like the CMBS, they are only activated when the vehicle is no longer controllable by the driver, or after the driver has been warned of the threat but has failed to take action that would override the action of the ESC system.

---

[235] "Towards a European Standard: The Development of Safe Road Transport Informatics Systems", Draft 2, DRIVE Safely (DRIVE I Project V1051), March 1992

[236] ISO/CD 26262, "Road vehicles – Functional safety", ISO, draft, 2006 (9 parts)

[237] "MISRA Guidelines for safety analysis of vehicle based programmable systems", MIRA, 2007, ISBN 978 0 9524156 5 7

[238] EVITA D2.3

[239] "Code of Practice for the Design and Evaluation of ADAS", Deliverable 11.2, RESPONSE 3 (a sub-project of the "PREVENT Integrated" Project), available online at: http://www.prevent-ip.org/download/deliverables/RESPONSE3/D11.2/PR-11300-SPD-061031-v30-CoP.pdf

[240] J. Schwarz, "Legal problems and suggested solutions in connection with the development of Driver Assistance Systems", German Presidency eSafety Conference, Berlin, June 2007

[241] W. Botman, "Potential benefits of active driver assistance systems and the legal context", German Presidency eSafety Conference, Berlin, June 2007

[242] Annex 9, UNECE Regulation No. 13-H (Revision 1, Amendment 2)

4.2.1.2 Proposed amendments

Recently, proposals for possible amendments to the Vienna Convention have been made by UNECE[243], with the aim of ensuring that systems that are type approved under UNECE regulations are also accepted as complying with the Vienna Convention. These proposals include a definition of a Driving Assistance System as follows:

> ***"Driving Assistance System** means a built-in system intended to help the driver in performing his driving task and which have an influence on the way the vehicle is driven, especially aimed at the prevention of road accidents."*

In addition, the following paragraph is proposed as an addition to Article 13 (which is concerned with speed and distance between vehicles):

> *"Driving assistance systems shall not be considered contrary to the principles mentioned in paragraph 1 of this Article and mentioned in paragraphs 1 and 5 of Article 8 as well, provided that:*
>
> - *either these systems are overridable at any time or can be switched off,*
> - *or they only optimise at technical level some functions which operating depends only on the driver,*
> - *or they operate in case of emergency when the driver lost or is about to lose the control of the vehicle,*
> - *or the intervention of these systems is identical with a usual property of a motor vehicle (e. g. speed limiting device)."*

The UNECE Inland Transport Committee Working Party of Road Traffic Safety recommends that these criteria should be observed when establishing rules for the design of a given DAS.

A few vehicle manufacturers now offer automatic parking systems, which will autonomously manoeuvre the car into a selected parking space with the aid of on-board sensors to identify the positions of nearby obstacles. In most such systems the driver still controls the speed of the vehicle with the accelerator and brake pedals, but any intervention with the steering process causes the vehicle to return to full control to the driver. Systems of this type would therefore comply with the first of the criteria proposed by UNECE for DAS to be acceptable under the Vienna Convention. Vehicles with automatic parking capability – which depends on the availability of electric power steering – may also offer an active lane keeping support function, in which the steering will be adjusted if the vehicle is determined to be on course to leave the current traffic lane without the relevant indicator being activated (rather than just issuing a warning to the driver, as in LDWS). Automatic suspension under driver intervention and the option to turn off this feature would also enable such systems to satisfy the first of the proposed acceptable DAS criteria.

Systems providing "intelligent speed adaptation" (ISA) have been widely studied (including in practical field trials), and are regarded by safety organisations such as ROSPA (Royal

[243] UNECE Inland Transport Committee Working Party of Road Traffic Safety, "Consistency between the Convention on Road Traffic, 1968, and the vehicle technical regulations", Informal document No. 1, March 2011

Society for the Prevention of Accidents)[244] and ETSC (European Transport Safety Council)[245] as offering significant potential to reduce both the occurrence and the severity of road accidents. The last of the DAS criteria proposed by UNECE for inclusion in the Vienna Convention would also permit the adoption of ISA systems that actively restrict the maximum speed of vehicles according to prevailing local limits (other ISA systems simply provide warnings to the driver). However, there are other types of system under investigation that are probably still outside the scope of these proposed amendments.

4.2.1.3 Autonomous driving

A modified Toyota Prius has been reported[246] to be already operating autonomously on public roads in California, although with a human co-pilot constantly monitoring performance and ready to take manual control if needed (this is reported to have been necessary when an earlier vehicle unexpectedly veered off a road in 2005[247]). In this case, therefore, the driver has voluntarily given up control to an on-board system in circumstances that are clearly not uncontrollable, although retaining a supervisory role.

However, such a scheme offers little practical benefit to the driver, as the supervision activity will require the same level of attention as when actually driving, but is probably more difficult to maintain while not actively involved in the driving task. It is more likely that the use of a supervising driver is simply a demonstration step towards an ultimate objective of fully autonomous driving without reliance on human supervision.

The concept of "platooning", in which a number of vehicles travel as an ensemble for some period of time (also described as "road-trains"), has been investigated in a number of collaborative research projects supported with EU and national funding. The perceived benefits of such schemes include improved traffic flow, higher vehicle density on the road, reduced engine emissions, and improvements in road safety. In the EU project "SARTRE"[248] the platoon is envisaged as comprising a "lead vehicle" that is driven by a trained, professional driver, together with one or more "following vehicles" that are being driven autonomously (but linked to the "lead vehicle" via wireless communication), thus allowing the drivers of the "following vehicles" to perform tasks other than driving their vehicles. Thus, the "following vehicles" would not be under the control of their drivers whilst part of the platoon, despite the fact that the driving situation is not expected to be uncontrollable. Nonetheless, they do have the ability to choose to join or leave the platoon, and therefore have the opportunity to override the external control of the driver of the "lead vehicle". However, the override capability

[244] "Cars in the Future", Policy Paper, Royal Society for the Prevention of Accidents (UK), January 2007

[245] "ETSC MEP Briefing: European Parliament Own Initiative Report on Road Safety", European Transport Safety Council, 4th March 2011

[246] J. Markoff, "Google Cars Drive Themselves, in Traffic", New York Times, 9/10/2010, available online at: http://www.nytimes.com/2010/10/10/science/10google.html?pagewanted=1&_r=2

[247] J. Markoff, "Guided by Computers and Sensors, a Smooth Ride at 60 Miles Per Hour", New York Times, 10/10/2010, available online at: http://www.nytimes.com/2010/10/10/science/10googleside.html?ref=science

[248] T. Robinson, E. Chan and E. Coelingh "Operating platoons on public motorways: an introduction to the SARTRE platooning programme", 17th World Congress on Intelligent Transport Systems, October 2010, Busan, Korea

of the drivers of individual "following vehicles" may need to be limited under some circumstances in order to avoid compromising the safety of the other members of the platoon.

The platoon concept described above does not comply with the view that driver assistance systems should override the driver only if the latter is unable to maintain control. In the platoon scenario the "following vehicle" drivers have opted to give up direct control of their vehicle to an autonomous system, although the autonomous systems are linked by wireless communication to a "lead vehicle" that is under the control of a driver. It may also not fully comply with the amendments proposed by UNECE, which require that it must be possible to override DAS at any time. Furthermore, it is possible that the "lead vehicle" may also encounter situations in which on-board systems take control from the driver. In such circumstances the drivers of the "following vehicles" cannot be expected to immediately resume control of their own vehicles, since they have given up control in order to undertake other activities whilst part of the platoon, so the automatic systems of the "lead vehicle" would effectively be in control of the "following vehicles" in the platoon as well.

Although the Vienna Convention does allow for coupled vehicles which travel on the road as a single unit, provided that they are controlled by a driver, references to coupling elsewhere in the text clearly indicate that this was expected to be a mechanical coupling (e.g. for trailers and articulated vehicles). In addition, even the proposed amendments to the Vienna Convention would not support fully autonomous driving. Consequently, on-going amendment and clarification of the Vienna Convention will be necessary in order to ensure that it takes account of recent and anticipated technological developments.

4.2.2 Liability issues

Historically, the responsibility for road accidents and failure to comply with traffic regulations has most commonly been attributed to human errors. Typical examples may include failure to pay full attention while driving, failure to follow the accepted rules, failure to maintain the vehicle correctly, or failure to take adequate account of local traffic and/or environmental conditions. Less frequently, the cause may be attributed to failures or defects of specific vehicle parts or systems, or perhaps due to some shortcoming of the road management (e.g. inadequate road signs or poor junction design). With the introduction of ADAS, however, this situation is likely to become increasingly complex.

It is noted in the EC's Action Plan for ITS[249] that liability and data protection issues could be significant barriers to deployment unless citizens' rights are shown to be fully protected. The following actions were therefore proposed:

- "*Address the liability issues pertaining to the use of ITS applications and notably in-vehicle safety systems.*
- *Assess the security and personal data protection aspects related to the handling of data in ITS applications and services and propose measures in full compliance with Community legislation.*"

[249] COM (2008) 886, "Communication from the Commission: Action Plan for the deployment of Intelligent Transport Systems in Europe", 16/12/2008

The indicated target date for completion of these actions was 2011. The need for action at community level to establish common rules on liability, as well as data security and privacy, is also mentioned in the 2008 proposal[250] for the ITS Directive. The target date for addressing these liability and data protection issues was subsequently more specifically indicated[251] as the end of 2011 at the latest. In a recent publication[252], it is reported that the EC intends to launch (in 2011) a study to identify the major liability issues that need to be addressed in the context of deployment of ITS.

4.2.2.1 Identifying responsibilities

The basic manual braking system has already evolved over recent years, with the addition of on-board sensors, actuators and more sophisticated control algorithms, through enhancing the performance of braking actions instigated by the driver (i.e. ABS and BAS) and on to automatically supporting the driving process (i.e. ESC). These systems enhance safety and are now mandatory for new vehicles. At present, however, the driver still remains responsible for the driving activity and for sensing and processing information received from outside the vehicle (such as local traffic and weather conditions, prevailing speed limits, etc.). Nonetheless, failure to ensure that the user is fully informed of the features and limitations of the available driving support functions may lead to increased accidents if the driver mistakenly believes that the system can be relied upon to mitigate the potential effects of poor driving practices. Behavioural adaptation of this kind is reported to have been observed in connection with a number of different driver support systems[253].

However, the "presentation" of a product is an important factor in relation to the EU Directives concerning Product Safety[254] (see section 4.3) and Product Liability[255] (see section 4.4). For example, inadequate instructions or misleading advertisements regarding the use of ADAS equipment could be regarded as making the system "defective" through inappropriate influence on customer expectations. It is essential for the user to have a correct understanding of the operational characteristics and limitations of such systems in order to ensure that they can be used in a safe manner. Nonetheless, warnings do not mitigate the impact of safety

[250] COM (2008) 887, "Proposal for a Directive Of The European Parliament And Of The Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes", 16/12/2008

[251] Council of the European Union, "Council conclusions on the Commission Communication 'Action Plan for the Deployment of Intelligent Transport Systems in Europe'", 30/03/2009

[252] European Commission, Directorate-General for Mobility and Transport, "Intelligent transport systems in action. Action plan and legal framework for the deployment of intelligent transport systems (ITS) in Europe", ISBN: 978-92-79-18475-8, 2011, p. 27, available on-line at: http://bookshop.europa.eu/en/intelligent-transport-systems-in-action-pbMI3210588/

[253] K. van Wees and K. Brookhuis, "Product liability for ADAS; legal and human factors perspectives", *European Journal of Transport and Infrastructure Research*, Vol. 5, No. 4, 2005, pp. 357–372

[254] Directive 2001/95/EC of the European Parliament and the Council of 2 December 2001 on general product safety, *O J.*, 15/1/2002, L 11/4–17

[255] Council Directive of 25July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), *O J.*, 7/8/1985, L 201/29 (as amended)

limitations that could have been avoided using an alternative design that was economically viable[256].

Further considerations of the Product Safety and Product Liability Directives (see further in this report) include "*the use to which it could reasonably be expected that the product would be put*"[257] and "*normal or reasonably foreseeable conditions of use*"[258]. Thus, there is an obligation on the product producer to take account of the possible impact of foreseeable misuse and non-ideal operating conditions when developing their products. There is already widespread experience of malicious interference with computing systems via the Internet, including attacks against individual home computers as well as institutional networks. Thus, the requirements of the Product Safety and Product Liability Directives would lead to the expectation that ADAS producers should anticipate the possibility of attacks on the security of in-vehicle assets, which could exploit the new wireless communications channels that are now beginning to be provided in modern vehicles. Consequently, failure to address the security of on-board vehicle networks, which may have potential safety implications as well as other possible impacts, could also be considered as a product defect.

The ADAS producer could therefore be held liable for any deaths or injuries that could be attributed to such defects, as well as compensation for associated physical damage sustained by other products (although not the defective product itself) provided that they are intended for private use (see below: the scope of Product Liability is generally restricted to private use). Other possible types of damage that might result (i.e. non-material damage types, such as financial losses or loss of reputation) are not covered by the Product Safety and Product Liability directives and would need to be pursued under the applicable national laws.

The EU-supported project RESPONSE 3 classified ADAS products in terms of three generic types[259], drawing conclusions about the associated liability issues as follows:

- Information and warning systems – where liability generally remains with the driver, who remains in full control although the ADAS producer or distributor may be liable if incorrect or inaccurate information is provided by the system.
- Intervention systems which the driver either cannot override, or where override is impracticable (because of human reaction time) – where ADAS producers and distributors are likely to be liable as the driver is not in control.
- Intervention systems for which driver override is possible at any time – where the driver retains overall responsibility and may therefore be liable, depending on the circumstances, although system malfunctions may also lead to liability for the ADAS producer or distributor.

[256] R. van der Heijden and K. van Wees, "Introducing Advanced Driver Assistance Systems: Some Legal Issues", *European Journal of Transport and Infrastructure Research*, Vol. 1, No. 3, 2001, pp. 309–326

[257] Art. 6.1(b), 85/374/EEC

[258] Art. 2(b), 2001/95/EC

[259] J. Schwarz, "Code of Practice for development, validation and market introduction of ADAS", 5th European Congress on ITS, Hannover, Germany, 3rd June 2005, available on-line at: http://www.prevent-ip.org/en/public_documents/publications/papers_presentations/code_of_practice_for_development_validation_and_market_introduction_of_adas.htm

The functionality that is envisaged for future vehicle systems will be increasingly dependent on inputs from a variety of external systems (e.g. positioning and navigation signals, and messages from other vehicles or roadside infrastructure), as well as a widening array of on-board sensors, actuators and electronic control capabilities. Such systems may diminish the driver's current role, and perhaps ultimately replace the driver with fully autonomous driving systems. In these scenarios the quality of information received from outside the car, the reliability of wireless communication channels, and the dependability of the on-board systems will be increasingly significant factors for successful and safe operation. Consequently, responsibility for accidents might be expected to shift away from the driver towards vehicle manufacturers and their on-board systems suppliers and more and more also to external information providers.

Under fully autonomous operation there is no driver involvement, but determining whether responsibility lies with the on-board systems or the external information sources may not be easy to establish. However, it may prove difficult to establish the responsibility of actors other than the driver in circumstances where the driver still has a role. This was demonstrated by the recent investigation into unintended acceleration in Toyota vehicles, which was carried out by NHTSA. The origin of these behavioural anomalies was widely debated, with driver error, electromagnetic compatibility, mechanical issues and software defects all mooted as possible causes[260]. The associated NASA report[261] concluded that although the unintended acceleration events were unlikely to have been caused by the electronic systems, this was not considered to be impossible. The NASA investigations were unable to demonstrate that the unintended acceleration events were due to unexpected behaviour of the electronic systems. However, exhaustive evaluations were not feasible due to the very large number of possible combinations of system inputs. Thus, the absence of evidence of such effects cannot be assumed to be evidence of their absence. Consequently, the possibility that electronic systems defects could have caused the unintended acceleration events cannot be ruled out based on the available data.

4.2.2.2 Event data recorders

Showing that a mechanical part has broken, perhaps then resulting in the failure of a safety-critical function such as the braking system, should be relatively straightforward. However, establishing that a vehicle control system responded in an unexpected way to a particular combination of transient inputs is likely to be extremely difficult. For this reason, it has been suggested that there should perhaps be an obligation to install an event data recorder (similar to the so-called "black box", which has been used in aircraft for many years) when ADAS are more widely deployed[262]. The first standard for such a device, known as a "motor vehicle

[260] F. Ahrens, "Why it's so hard for Toyota to find out what's wrong with its vehicles", The Washington Post, 4/3/2010, available online at:
http://voices.washingtonpost.com/economy-watch/2010/03/i_wont_lie_to_you.html

[261] NASA Engineering and Safety Centre, "National Highway Traffic Safety Administration: Toyota Unintended Acceleration Investigation", NESC Assessment Report TI-10-00618, January 2011, available online at: http://www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf

[262] R. van der Heijden and K. van Wees, "Introducing Advanced Driver Assistance Systems: Some Legal Issues", *European Journal of Transport and Infrastructure Research*, Vol. 1, No. 3, 2001, pp. 309–326

event data recorder" (MVEDR), was developed by the IEEE in 2004 (IEEE 1616[263]), and has been amended in 2010[264] to address potential security issues associated with MVEDRs, including:

- **Data tampering** – modification, removal, erasure of, or otherwise rendering inoperative, any device or element, including MVEDRs;
- **VIN theft** – duplication and transfer of unique vehicle identification numbers, enabling stolen cars to be passed off as non-stolen;
- **Odometer fraud** – rolling back of vehicle odometers, reducing the reported total distance travelled by the vehicle;
- **Privacy** – prevention of the misuse of collected data relating to vehicle owners.

The availability of MVEDR data could raise a number of possible privacy and liability issues. For example, insurance companies may have an interest in using such data to influence vehicle insurance premiums. In the event of an accident occurring, they might perhaps wish to try to use MVEDR data in order to attempt shifting liability towards:

- the driver, if the data suggest that the driver has been behaving recklessly;
- the ADAS producer, if the data suggest that the accident could be attributed to a defect in the performance of the electronic systems;
- organisations providing information to the vehicle, if the data suggest that erroneous information caused or contributed to the accident.

The United States NHTSA and Federal Motor Carrier Safety Administration (FMCSA) both take the position that the MVEDR and its data belong to the vehicle owner[265], with the implication that no private party could force the vehicle owner to relinquish that data without consent. However, it is conceivable that insurance companies could perhaps require the vehicle owner to provide consent as a condition of the insurance policy, or alternatively offer an incentive such as reduced insurance premiums in return for such consent. The latter approach has already been adopted in the USA by Progressive Insurance[266]. The monitoring device installed in the car does not track where people drive, but only their driving patterns. A similar scheme (recording speed and acceleration) has recently been launched in the UK targeted at young and inexperienced drivers, for whom car insurance costs are becoming prohibitive[267].

Vehicle manufacturers in the USA have been voluntarily installing MVEDRs as part of car and light truck airbag modules since 1996. These devices are triggered by conditions such as rapid changes in vehicle speed in order to collect a variety of data during crash and near-crash events. The data collected typically includes speed at time of impact, steering angle, whether

[263] IEEE 1616:2004, "Standard for Motor Vehicle Event Data Recorder (MVEDR)"

[264] IEEE 1616a:2010, "Standard for Motor Vehicle Event Data Recorders (MVEDRs) – Amendment 1: Motor Vehicle Event Data Recorder Connector Lockout Apparatus (MVEDRCLA)"

[265] T.M. Kowalick, "Fatal Exit: The Automotive Black Box Debate", IEEE Press, 2005, ISBN 0-471-69807-5, p. 277

[266] J. Lendino, "Progressive uses "black box" to monitor drivers", 31/07/2008, available online at: http://www.pcmag.com/article2/0,2817,2326909,00.asp

[267] N. Lyndon, "Black box technology to monitor young drivers", The Telegraph, 18/07/2011, available online at: http://www.telegraph.co.uk/motoring/columnists/neil-lyndon/8458515/Black-box-technology-to-monitor-young-drivers.html

brakes were applied, and seatbelt usage during the crash. The United States NHTSA requires MVEDRs, where voluntarily fitted, to meet specific data collection standards from September 2010[268] for light vehicles. Furthermore, the findings of the NHTSA-NASA investigation of unintended acceleration in Toyota vehicles[269] include (amongst others) recommendations to:

- consider initiating rulemaking to:
  - require brake override systems (to ensure that the brake has priority over the throttle);
  - standardize operation of keyless ignition systems (so that drivers know how to stop the engine quickly);
  - require the installation of MVEDRs in all passenger vehicles;
- begin broad research on the reliability and security of electronic control systems for vehicles by examining existing industry and international standards for best practices and relevance to automotive applications.

In this proposed reliability and security research, NHTSA plan to give full consideration to NASA's recommendation that NHTSA should consider controls for managing safety critical functions in vehicles, based on those currently applied to the rail, aerospace, military, and medical industries.

4.2.3 Best Practice for Complex Systems Development

The difficulties involved in developing and demonstrating the reliability of ADAS derive from their inherent complexity. The following definitions, which derive from the defence systems domain[270], serve to demonstrate this issue.

- *"**Simple.** A hardware item may be classified as 'simple' if its design is suitable for exhaustive simulation and test."*
- *"**Complex.** The degree to which a system or component has a design or implementation that is difficult to understand and verify. For the purposes of this document 'complex' is defined as 'unsuited to the application of exhaustive test'."*
- ***"Exhaustive test.** Thorough exercising of a component through test or analysis using values applied at its terminals. The aim is to exercise all possible combinations. The phrase 100% test is not used because the number of possible tests is infinite, taking account of all physical properties. Judgement is involved which needs to be justified in a safety case."*

[268] U.S. Department Of Transportation, National Highway Traffic Safety Administration, 49 CFR, Part 563: Event Data Recorders – EDRs in Vehicles", available online at: http://www.nhtsa.gov/DOT/NHTSA/Rulemaking/Rules/Associated%20Files/EDRFinalRule_Aug2006.pdf

[269] U.S. Department Of Transportation, National Highway Traffic Safety Administration, "Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems", February 2011, available online at: http://www.nhtsa.gov/staticfiles/nvs/pdf/NHTSA-UA_report.pdf

[270] Def Stan 00-54, "Requirements for Safety Related Electronic Hardware in Defence Equipment", UK Ministry of Defence, 1999

A consequence of complexity is that the traditional test-based methods used in establishing compliance with WVTA requirements, which have been developed for validating the safety performance of relatively simple and largely independent mechanical and electrical systems, are unlikely to be suitable for increasingly sophisticated mechatronic vehicle systems with significant software content and widespread inter-dependencies. Exhaustive testing is not practicable for such complex systems because the number of possible system states (i.e. combinations of inputs) is extremely large. Furthermore, in complex, software based systems it is systematic, rather than random, faults that predominate, with the result that testing to establish probabilistic failure rates is also likely to be of impracticable duration.

4.2.3.1 Safety case

The recommended approach for establishing the safety of complex electronic control systems, based on experience in safety-critical applications found in the aerospace, defence, nuclear, rail and off-shore oil industries, is to create a safety argument to show that the system is *acceptably safe for the intended application and for the intended operating environment*. The important points here are that complete safety is recognized as unachievable, although mitigation measure must be implemented as necessary to ensure that any residual risks are deemed to be acceptable, and that the safety argument only applies to the intended application and operating environment. For networked vehicles, however, the operating environment is known to include hackers and criminals, who are already actively engaged in security attacks against existing computer networks. Thus, a safety case for such applications should also take account of safety-related security threats.

The safety argument and supporting evidence should be documented in a "safety case", which should[271]:

- make an explicit set of claims about the properties of the system;
- identify the supporting evidence (i.e. facts, assumptions, or sub-claims derived from lower-level arguments);
- provide a set of safety arguments that link the claims to the evidence;
- make clear the assumptions and judgements underlying the arguments;
- allow for different viewpoints and levels of detail.

The safety case should be subject to independent assessment and audit by a suitably qualified third party. Constructing the safety case in the form of a relatively simple top-level safety claim supported by a hierarchy of sub-claims makes it easier to understand the main arguments and to partition the safety case development activities. Claims can be made more robust by using independent evidence and more than one argument to support the claim, ideally with different styles of safety argument. A catalogue of generic patterns for a number of canonical

[271] P. Bishop and R. Bloomfield, "A methodology for Safety Case development", *Industrial Perspectives of Safety-Critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium*, Birmingham, UK, February 1998, F. Redmill and T. Anderson (eds), Springer, 1998, ISBN 3-540-76189-6

safety argument types that could be used in this have recently been described and applied to an automotive case study[272].

The EC WVTA legislation is also moving in the direction of a Safety Case approach for vehicle systems based on complex electronic controls. Extensions have already been added to the UNECE regulations concerning braking[273] and steering[274], which detail special requirements to be applied to the safety aspects of complex electronic vehicle control systems. It is expected that similar extensions will eventually be added to all regulations concerning vehicle systems that may involve complex electronic control systems.

4.2.3.2 Safety development processes

The international standard IEC 61508[275] on the functional safety of safety-related electrical, electronic or programmable electronic systems provides a basic functional safety standard applicable to all kinds of industry. It has its origins in the process control industry sector, but is also intended to provide a basis for the development of sector-specific safety standards. In particular, IEC 61508 reflects the following views on safety risks:

- zero risk is unachievable;
- safety must be considered from the outset;
- unacceptable risks must be reduced "as low as reasonably practicable" (ALARP).

Consequently, hazard identification, analysis of safety risks and assessment of the need for measures to mitigate such risks are key elements of the IEC 61508 approach.

Another important aspect of the IEC 61508 approach is the requirement for increasingly rigorous development processes to be applied for more critical safety functions, which is intended to provide greater confidence in the reliability of complex systems that are not amenable to exhaustive testing. The safety requirements are described in terms of "safety function requirements" (i.e. what the function should do) and "safety integrity requirements" (i.e. the likelihood that the safety function will be carried out satisfactorily). The safety integrity requirements of the safety functions are specified in terms of a number of discrete levels, known as "safety integrity levels" (SILs), which are related to the risk level and range from SIL1 to SIL4. The SILs reflect requirements for increasingly rigorous processes to be applied in a range of development activities, ranging from specification and design, through configu-

[272] R. Palin and I. Habli, "Assurance of automotive safety - a safety case approach", *Proc. 29th International Conference on Computer Safety, Reliability and Security*, Vienna, Austria, September 2010, pp. 82–96

[273] UNECE Regulation No. 13, "Uniform provisions concerning the approval of vehicles of categories M, N and O with regard to braking: Annex 18 – Special requirement to be applied to the safety aspects of complex electronic vehicle control systems", Revision 5, 08/10/2004

[274] UNECE Regulation No. 79, "Uniform provisions concerning the approval of vehicles with regard to steering equipment: Annex 6 – Special requirement to be applied to the safety aspects of complex electronic vehicle control systems", Revision 2, 21/10/2005

[275] IEC 61508: 1998–2005, "Functional safety of electrical/electronic/programmable electronic safety-related systems", (8 parts)

ration management, testing, validation and verification, to independent assessment. The safety argument for the achievement of a particular SIL should be as follows[276]:

> *"The requirement was for a SIL X system, and good practice decreed that I adhered to the standard's processes for a SIL X system. In doing so, I have generated the evidence appropriate to a SIL X system, and assessment of the evidence has found that I have adhered to the defined processes."*

An approach interpretation of IEC 61508 developed specifically for the automotive industry is provided by ISO 26262[277], which:

- provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring of the necessary activities during these lifecycle phases;
- covers functional safety aspects of the entire development process (including such activities as requirements specification as well as system design, implementation, integration, verification, validation, and configuration);
- provides an automotive-specific and risk-based approach for determining risk classes ("automotive safety integrity levels", ASIL's) that are analogous the IEC 61508 SIL's;
- uses ASIL's for specifying the necessary safety integrity requirements for safety functions that are required to achieve an acceptable level of residual risk, where class D represents the highest integrity category and class A is the lowest;
- provides suitable requirements for validation and confirmation measures to ensure that a sufficient and acceptable level of safety is achieved.

The main difference between the ASIL's of ISO 26262 and the SIL's of IEC 61508 is that the latter employ quantitative target probability values, while the ASIL's are based on qualitative measures.

Related guidance regarding safety analysis for vehicle based programmable systems has also been developed by the Motor Industry Software Reliability Association (MISRA)[278]. This is based on an iterative process, starting with a Preliminary Safety Analysis (PSA) carried out at the system concept stage. This is subsequently refined through more comprehensive Detailed Safety Analysis (DSA) activities as the system design and development activities progress (see Figure 1). Thus, the MISRA safety engineering process is expected to be an iterative activity that is developed and refined as the system evolves and matures.

[276] F. Redmill, "Undertanding the use, misuse and abuse of Safety Integrity Levels", *Proc. Eighth Safety-critical Systems Symposium*, Southampton, UK, February 2000, available online at: http://www.csr.ncl.ac.uk/FELIX_Web/3A.SILs.pdf

[277] ISO/CD 26262, "Road vehicles – Functional safety", (9 parts), draft, 2006

[278] MISRA, "Guidelines for Safety Analysis of Vehicle Based Programmable Systems", MIRA Ltd, November 2007, ISBN 978-0-9524156-5-7

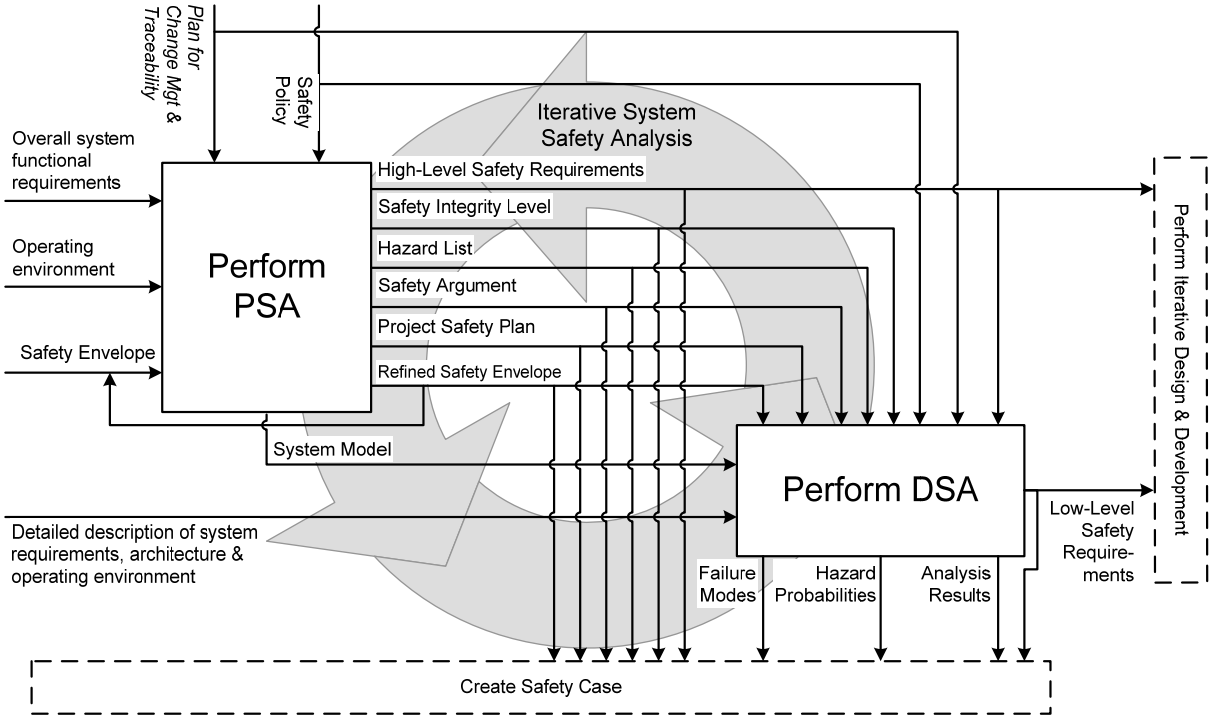

Figure 1 Overview of the MISRA System Safety Analysis Process[279]

4.2.3.3 Security issues

As with safety, zero security risk is in practice unachievable and a similar risk-based approach is needed in order to evaluate potential security threats and to identify requirements to mitigate those threats for which the level of risk is judged to be unacceptable.

The standard IEC 15408[280] is concerned with security evaluation for IT products, but does not explicitly address the possible safety implications of security breaches for safety-critical control systems. A further limitation is that it does not provide a framework for risk analysis. Methods for evaluating the probability of a successful attack (described as "attack potential") are described in IEC 18045[281], but the severity of the impact is not evaluated to allow risk to be assessed. Risk analysis in an IT security context is outlined in ISO/IEC TR 15446[282] and described in more detail elsewhere (e.g. ISO/IEC 13335[283], NIST IT Security Handbook[284]).

In IEC 15408 the concept of "evaluation assurance levels" (EAL) has a similar role for security considerations to the SIL and ASIL categories used in the safety context. The EALs are similarly associated with graded levels of increasing development rigour, ranging from

[279] MISRA, "Guidelines for Safety Analysis of Vehicle Based Programmable Systems", MIRA Ltd, November 2007, ISBN 978-0-9524156-5-7, p. 23

[280] ISO/IEC 15408:2005, "Information technology – Security techniques – Evaluation criteria for IT security", (3 parts), 2nd Edition, 01/10/2005

[281] ISO/IEC 18045:2008, "Information technology – Security techniques – Methodology for IT security evaluation", 2nd Edition, 15/08/2008

[282] ISO/IEC TR 15446:2004, Information technology – Security techniques Guide for the production of Protection Profiles and Security Targets", Technical report, 01/07/2004

[283] ISO/IEC 13335, "Information technology — Security Techniques — Management of information and communications technology security"

[284] NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook". October 1995, available on-line at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

functional testing where the security threat is not deemed to be serious (EAL1), through to formally (i.e. mathematically) verified design and testing for cases where the security risks are judged to be extremely high (EAL7). The similarities between the EAL and SIL/ASIL concepts suggest the potential for developing a unified approach for automotive safety and security[285]. Similar observations have also been made with regard to the security and safety of mobile ad-hoc network applications[286]. Unifying safety and security engineering processes offers potential benefits in terms of reduced costs through sharing of evidence and risk analysis for those applications where security may also have possible safety implications.

The MISRA Development Guidelines for Vehicle Based Software[287] identified the need to protect vehicle software from unauthorised access that could compromise software, or to provide detection of tampering. It was also noted that unauthorised reprogramming of vehicle control systems (so-called "chipping") may cause the vehicle manufacturer to become legally liable in some countries.

The 2010 edition of IEC 61508 (2nd Edition[288]) now includes consideration of security issues with regard to their potential impact on safety. Possible malevolent and unauthorised actions are required to be addressed during the hazard and risk analysis. If a security threat is seen as being reasonably foreseeable, then a security threat analysis should be carried out and if security threats have been identified then a vulnerability analysis (i.e. security risk analysis) should be undertaken in order to specify corresponding security requirements. However, security threats that are not safety-related, such as those affecting privacy or financial security, are beyond the scope of IEC 61508.

For the purposes of EVITA a risk analysis approach[289] was developed from the IEC 61508-based concepts of ISO 26262 and MISRA, which were extended to encompass non-safety aspects of security threats in a unified manner, with security-related risks assessed using the attack potential concept of IEC 15408 and IEC18045 (see section 1.4).

Given that the safety case concept has been widely adopted in many safety-related industrial sectors, it seems logical to consider developing an analogous "security case"[290] to present the security argument for security-related applications, particularly for those where security may also have potential safety implications. Furthermore, it would be also desirable that such a security case should be subject to independent assessment and audit by a suitably qualified third party, as with the safety case.

---

[285] P.H. Jesty and D.D. Ward, "Towards a unified approach to safety and security in automotive systems", *Proc. 15th Safety-critical Systems Symposium*, Bristol, UK, February 2007, pp. 21–35

[286] J.A. Clark, H.R. Chivers, J. Murdoch and J.A. McDermid, "Unifying MANET safety and security", International Technology Alliance in Network-Centric Systems, Report ITA/TR/2007/02 V. 1.0, 06/11/2007, available online at: http://www.usukita.org/papers/3155/ITA-TR-2007-02-v1.0_0.pdf

[287] MISRA, "Development Guidelines for Vehicle Based Software", MIRA Ltd, November 1994, ISBN 0-9524156-0-7, p. 43

[288] IEC 61508:2010, "Functional safety of electrical/electronic/programmable electronic safety-related systems", 2nd Edition, 30/04/2010

[289] EVITA D2.3, Appendix C

[290] G. Despotou and T. Kelly, "Extending the Safety Case concept to address dependability", Proc. 22nd Int. System Safety Conference, Providence, RI, USA, August 2004, pp. 645–654

4.3 General Product Safety Directive

4.3.1 Introduction

The European Union has been regulating safety of goods for quite a while, but the regulation was only product-specific. Thus there was regulation for products such as cars and toys but a general regulation of the safety of products was non-existent. This changed in 1992 when the first version of the General Product Safety Directive (GPSD) was introduced. This version was replaced in 2001 by Directive 2001/95/EC, which currently regulates product safety in general. [291]

4.3.2 Goal

The goal of 2001/95/EC is to prevent unsafe products from entering the market.

4.3.3 Scope

The scope of 2001/95/EC is twofold. The first part is that it only concerns products. These products are defined as follows[292]:

> ***any product*** *— including in the context of providing a service — which is* ***intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them****, and is supplied or made available, whether for consideration or not, in the course of a commercial activity, and* ***whether new, used or reconditioned*** (author emphasis)

2001/95/EC targets all consumer products, even those supplied to the consumer as part of the provisioning of a service. This refers to products being used by the consumer as part of a service. It does not cover products operated by the service provider in the provisioning of a service to consumers. A bus company, for example, is not subject to 2001/95/EC for the busses it operates to transport passengers. These busses are not used by the passengers in a strict sense. They are operated by a bus driver contracted to the public transport company and not by a consumer. That is the difference with a rental car. The rental car is operated by the user and will therefore be subject to the rules of the Directive. A consumer product is evidently first and foremost a product that is intended for consumers. But it also covers products that are intended for professionals but that are likely to be acquired by consumers, so-called migrated products. This likelihood of migration will mainly depend on the marketing channels of a product. If a product is marketed through a channel that is only accessible to professionals then one could consider it unlikely that the product would be acquired by consumers and therefore the product would be out of scope of 2001/95/EC.

[291] Directive 2001/95/EC of the European Parliament and the Council of 2 December 2001 on general product safety, *O.J.* 15/1/2001, L 11

[292] Art. 2.a), 2001/95/EC

Additionally, the definition is restricted to consumer goods marketed in relation to a commercial activity. This excludes consumer-to-consumer trade. If someone sells a product in his capacity of consumer there cannot be a commercial activity. If, however, the person were to make a habit out of buying and selling things to gain some extra income this could be considered a commercial activity. The mentioning of "made available" implies that it is not required that goods are sold to consumers. Other operations such as renting of products are also included.

The facts will thus play an important role in determining whether there is a commercial activity. For example, a shopkeeper selling consumer electronics may be subject to 2001/95/EC for a TV that he sells to a customer. But if he decides to sell his motorcycle he should be considered just as a consumer selling one of his possessions. His commercial activity involves consumer electronics, not motorcycles.

A final aspect is that it does not matter whether the goods are new, used or reconditioned. A reconditioned product is a product that has been restored to a good condition, for example by replacing old parts with new ones[293]. Goods not covered are used goods sold as antiques or goods sold to be reconditioned. This, however, requires that the seller has informed the buyer of the condition of the goods. If this duty of information has not been observed then the distributor will not be able to invoke this exception to the scope.

The second part of the scope is that it only targets products that are not subject to specific provisions relating to product safety in force in EU law. In the introduction we have mentioned that provisions exist in relation to cars and toys. For all aspects of safety that have been regulated by these provisions, 2001/95/EC will not apply. 2001/95/EC is secondary and only those provisions that do not have a counterpart in product-specific provisions will apply. As already mentioned in the introduction, sector-specific provisions do not concern distributors. Consequently the duties of distributors in relation to product safety are those mentioned in the provisions of 2001/95/EC.

4.3.4 General Safety Requirement

Producers are obliged to only put safe products on the market[294]. So far safety has been mentioned regularly but the concept has not yet been defined. 2001/95/EC defines "safe product" as follows:

> *'safe product' shall mean any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular:*
>
> *(i) The characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;*

[293] http://www.merriam-webster.com/dictionary/recondition
[294] Art. 3.1, 2001/95/EC

(ii) The effect on other products, where it is reasonably foreseeable that it will be used with other products;

(iii) The presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product;

(iv) The categories of consumers at risk when using the product, in particular children and the elderly. The feasibility of obtaining higher levels of safety or the availability of other products presenting a lesser degree of risk shall not constitute grounds for considering a product to be 'dangerous';

A safe product is not a product without risks. Safety is a circumstantial characteristic of the product. The definition refers to the reasonably foreseeable use of the product as benchmark. In the reasonably foreseeable conditions of use the product should not present any risks or only the minimum risks compatible with the product's use. If the use of the product imposes risks on the user, these should be compatible with a high standard for the protection of the safety and health of persons. To determine this standard any relevant characteristic can be taken into account. Four of them are mentioned explicitly, but the determination is not limited to using those four characteristics. Let us clarify this assessment using the example of a knife. A knife can be quite dangerous and cause severe physical injury in the form of cuts. Yet knives in general are not considered to be unsafe. It is acceptable that knives are sharp because they are meant to cut things. But a butter-knife for example is not meant to cut things and is often blunt. Therefore a cut from a butter-knife could warrant the butter-knife to be qualified as a dangerous product. In one case the fact that it is sharp, is acceptable for a knife, in the other case it is not. And this is the core of the assessment of safety incorporated in 2001/95/EC: judge the product on its own merits. More attention will be given to this when discussing the duties of the producer.

According to Article 3 of Directive 2001/95/EC a product shall be deemed safe, as far as the aspects covered by the relevant national legislation are concerned, when, in the absence of specific Community provisions governing the safety of the product in question, it conforms to the specific rules of national law of the Member State in whose territory the product is marketed.[295]

Directive 2001/95/EC further considers a product safe if, as far as the risks and risk categories covered by relevant national standards are concerned, when it conforms to voluntary national standards transposing European standards, the references of which have been published by the Commission in the *Official Journal of the European Communities.* [296].

In case a product does not conform to the cited rules, safety is assessed using *one of* the following criteria:

(a) Voluntary national standards transposing relevant European standards other than those of which the references have been published by the Commission.

(b) The standards drawn up in the Member State in which the product is marketed;

(c) Commission recommendations setting guidelines on product safety assessment;

(d) Product safety codes of good practice in force in the sector concerned;

[295] Such rules being drawn up in conformity with the Treaty, and in particular Articles 28 and 30 thereof, and laying down the health and safety requirements which the product must satisfy in order to be marketed.

[296] Art. 3.2, 2001/95/EC

(e) The state of the art and technology;
(f) Reasonable consumer expectations concerning safety

Two things are important in relation to safe products. The fact that a product is considered safe according to the provisions of the Directive does not prevent the taking of measures if the product is in reality found to be unsafe. Secondly, there is no prior approval required to market a product under 2001/95/EC[297]. This does not do away with the fact that if one were to market an unsafe product, one could be held liable for infringing 2001/95/EC. Furthermore, 2001/95/EC explicitly mentions that compliance does not exclude liability under Directive 85/374/EEC on the liability for defective products.

As a closing remark on the concept of safe products it must be mentioned that only the characteristics of the concerned product are of importance. It is not relevant whether it is possible to achieve a higher degree of safety. Neither is it relevant that one can acquire products offering a lesser degree of risk. The safety of a product must be judged on the merits of that particular product regardless of the safety offered by any other product.

4.3.5 Targeted Actors

4.3.5.1 Producer and distributor

2001/95/EC holds different duties depending on whether the producer or the distributor is concerned. The ECJ has ruled that the definitions of producer and distributor should be interpreted very strictly[298]. A producer is the person who qualifies as producer under the definition of the directive and the same goes for the distributor. If a person is qualified as a producer he cannot be a distributor and vice-versa. Consequently, the obligations imposed on a producer cannot be imposed on a distributor and vice versa.

4.3.5.1.1 Definitions

4.3.5.1.1.1 Producer

The first actor concerned is the producer. There are three hypotheses when one is considered a producer under 2001/95/EC[299]:

*(i) The manufacturer of the product, when he is established in the Community, **and** any other person presenting himself as the manufacturer by affixing to the product his name, trade mark or other distinctive mark, **or** the person who reconditions the product;*

[297] A motor vehicle has to undergo a type-approval procedure before it can be brought onto the market. The same goes for pharmaceutical products.
[298] Judgment of the Court (Eighth Chamber) (reference for a preliminary ruling from the Fővárosi Bíróság (Republic of Hungary)) — Lidl Magyarország, 30 April 2009, *O.J.* 04.07.2009, C-132/08
[299] Art. 2.(e), 2001/95/EC

(ii) The manufacturer's representative, when the manufacturer is not established in the Community ***or****, if there is no representative established in the Community, the importer of the product;*

(iii) Other professionals in the supply chain, insofar as their activities may affect the safety properties of a product;

The first person to be considered as producer is the manufacturer of the product, the person or entity making the product. If he is established in the Union he will be primarily responsible for the safety of his products. At a similar level and jointly responsible with the manufacturer is the person affixing any distinctive mark on the product. In this regard we could think of mail-order companies who have clothing manufactured by a third party that they affix their brand-name to. They have not produced the product but they appear to have produced the product because their name is on it. In the case of reconditioned goods, the person who has reconditioned the goods is considered the producer.

If the manufacturer is not established in the Union then his representative will be considered producer if he is established in the Union. If there is no representative of the manufacturer established in the Union, the importer of the good will be considered producer. The importer is the person who imports the product from outside the Union; he brings the product within the borders of the Union. A person importing the product from another Member State to his Member State is not an importer for the purposes of the definition of producer of 2001/95/EC.

Also considered as producers are professionals other than those mentioned already who play a role in the supply chain that may have an effect on the safety characteristics of the product.

4.3.5.1.1.2 Distributor

In contrast a distributor, the second actor involved, is a professional in the supply chain whose activities do not have an impact on the safety aspects of the product[300]. An example of a distributor is a shopkeeper who sells the product as he receives it from the producer. If the shop-keeper would need to perform certain actions on the product prior to delivery the situation may change. A bicycle for example is mostly provided half-assembled to the bicycle-shop. Before handing over the bicycle to the consumer, the shop-keeper or one of his staff finishes assembly of the bicycle and checks whether the assembled bicycle is in good working order. If this assembly or final check-up is not done properly this may have an impact on the safety of the bicycle. A badly fastened pedal may come off during use of the bicycle and may cause the cyclist to crash with physical injury as a consequence. Consequently the bicycle-shop, depending on how the bicycles are received by the shop-keeper (i.e. assembled or requiring final assembly) may have an impact on the safety characteristics of the bicycle and could therefore be considered a producer. The characteristic distinguishing distributor from producer is that a distributor does not have an impact on the safety characteristics of the product. As already mentioned, this distinction should be interpreted strictly.

[300] Art. 2.(f), 2001/95/EC

4.3.5.1.2 Duties

4.3.5.1.2.1 Producer

Firstly, producers have to undertake a risk-assessment before they introduce new products onto the market. How they execute this risk-assessment is left entirely to the discretion of the producers, although some guidelines exist[301]. These guidelines can be found in Appendix II of Commission Decision 2004/905/EC. 2004/905/EC proposes a two-stage assessment. The first stage has two aspects and should identify the severity of the danger presented by the product. In first instance the producer must assess the seriousness of possible injuries caused by the hazard inherent in the product. This does not only concern the impact on the consumer, but also for other people. If a product emits toxic fumes this could affect several people. If multiple persons could be affected the severity should be considered greater that the situation when only one person would be affected. A second aspect is the risk of the injury occurring. This aspect is determined by the probability of the product becoming defective on the one hand and the severity of the negative consequences that a user might endure during exposure corresponding to the intended or reasonably expected use of the product on the other hand.

The second stage is the grading of the risk presented by the product. This requires a combination of three aspects. The first aspect is the type of person using a product. Products intended for children should be subject to different safety requirements compared to products intended for adults. The qualification is done by considering how vulnerable a person is. A second aspect is the knowledge of the risk; this will be further discussed below. A third and final aspect are the precautions the producer has incorporated in the product to make it safe. An example of such a precaution is the safety cap that can be found in bottles containing cleaning agents. These measures may also lead to a reduced level of risk being presented by the product.

Secondly the producer is required to inform the consumers of inherent risks of the product that cannot be noticed at first sight[302]. The information provided should allow consumers to make a personal assessment of the risks involved and take the necessary precautions. This information should be tailored to the characteristics of the goods. If a product requires final assembly by the consumer then the information should take this into account and foresee appropriate information to facilitate safe assembly. The producer could, for example, include references to personal protection equipment to be used during assembly. On spray-paint cans, for example, one can find that they should be used in a well-ventilated area. This information does not release the producer from the other duties he incurs under 2001/95/EC. Providing information does not make a product safe. Providing information is only one of the requirements the producer has to observe.

The producers must also make arrangements so that they can be informed of the possible risks of their products and take appropriate measures to prevent these risks such as recall, withdrawal and the notification of consumers. To receive information he can mention his

[301] Commission Decision 2004/905/EC of 14 December 2004 laying down guidelines for the notification of dangerous consumer products to the competent authorities of the Member States by producers and distributors, in accordance with Article 5(3) of Directive 2001/95/EC of the European Parliament and of the Council (notified under document number C(2004) 4772), *O.J.* 28.12.2004, L 381, pp. 63–77

[302] Art. 5.1, 2001/95/EC

contact details on the packaging of the product. Taking measures can be facilitated by drawing up scenarios in advance in order to execute measures such as recall and withdrawal.

4.3.5.1.2.2 Distributor

Distributors contribute to the best of their ability to the achievement of applicable safety requirements. They do so by not marketing products which they know are unsafe, or by the virtue of their profession should have known were unsafe, based on the data available to them. Additionally they participate actively in guarding the safety of marketed products, especially by transmitting information on product risks as well as keeping and providing the necessary documentation to track the origin of products. They also cooperate in the execution of measures taken by producers and public authorities to prevent these risks. Within the limits of their activities as distributor they make the necessary arrangements to facilitate effective cooperation.

4.3.5.1.2.3 Producer & distributor

Producers and distributors alike must notify the competent authorities of the Member States if they know, or ought to know based on the data available to them and by the virtue of their profession, that they have marketed products that are in violation of the general safety requirement. Previously it has already been mentioned that producers should make arrangements so they can obtain information regarding risks associated with their products. It was also mentioned that distributors must share such information when they obtain it. Additionally they must provide information on the measures taken to mitigate the risk. Guidelines on how this information should be provided can be found in 2004/905/EC. Evidently a large emphasis is put on the identification of the product and its risks and all actors involved in protection of consumer safety. A template of a notification form is also provided in the guidelines.

Furthermore producers and distributors provide the competent public authorities the requested cooperation within the limits of their respective activities on measures undertaken to prevent risks presented by products they have marketed. The competent public authorities decide the procedural rules for such cooperation. To gain insight into these procedures one is therefore required to look at the procedures drawn up by the Member State where the product is marketed or otherwise made available. In short, notification must be given in the Member State where the risk occurs.

4.3.5.2 Member States duties and competences

The final actors involved in 2001/95/EC are the Member States. They are responsible for implementing product safety provisions in their respective national legislations and must foresee appropriate penalties for infringement of product safety rules[303]. Additionally they must also foresee a public authority exercising market supervision and with the competence to take appropriate measures as stated in and required by 2001/95/EC. A detailed analysis of these duties is however out of scope for EVITA.

[303] Art. 6-9, 2001/95/EC

4.3.6 RAPEX

A final aspect of 2001/95/EC to be introduced is RAPEX[304]. RAPEX is the Union's rapid alert system for dangerous non-food consumer products. The information regarding dangerous products is provided by the Member States who also notify the measures that have been taken to deal with the risk. This information is also made available to the public. The guidelines for RAPEX have recently been updated and can be found in Commission Decision 2010/15/EC[305]. The analysis of these requirements is however out of scope for EVITA and will therefore not be continued.

4.4 Product Liability

When determining liabilities in case of an road accident that is possibly not caused by a human factor but by a malfunctioning of technical items, experts will, as we have seen at this stage, first examine whether the relevant parts of the vehicle have been type-approved and if the actual parts involved in the accident have been correctly built according to the approved type. In case of automotive on-board networks, however, products used will often not be under the scope of Directive 2007/46/EC. The next step could then be to analyse if the product is used under the scope of the (general) Product Safety Directive and if it fulfils the safety requirements of this Directive.

Nevertheless a particular vehicle involved in a road accident can be *defective*. This is where the discussion about product liability comes in.

4.4.1 Directive 85/374/EEC on liability for defective products

4.4.1.1 Introduction

Directive 85/374/EEC is a harmonization directive intended to harmonize liability for defective products in the EU. [306] It mainly serves an economic purpose, i.e. it should facilitate the creation of the common market and lift any barriers on trade between Member States caused by differences in product liability law. Therefore the rules set forth by the Directive should be the primary rules in Member States to deal with product liability cases. There is some doubt as to whether this goal has actually been achieved, given the low number of court cases. A counterargument is that many cases are settled out of court and therefore do not contribute to the statistics. Therefore it is difficult to assess the actual impact of Directive 85/374/EEC.

Next to its economic purpose, it also intends to offer the citizens of the EU a harmonized level of protection against damage stemming from defective products. The protection against defective products is to be guaranteed by Directive 2001/95/EC discussed in section 4.3. At

[304] Website RAPEX: http://ec.europa.eu/consumers/safety/rapex/

[305] Commission Decision 2010/15/EC of 16 December 2009 laying down guidelines for the management of the Community Rapid Information System "RAPEX" established under Article 12 and of the notification procedure established under Article 11 of Directive 2001/95/EC (the General Product Safety Directive), *O.J.* 26.01.2010, L22

[306] Many elements mentioned in the "Introduction" can be found in the preamble to 85/374/EEC

the time of introduction of the Directive consumer safety was not given the same importance in EU law is it is given now. Today it is part of the Treaty on the Functioning of the EU and is a basic policy aspect for the EU[307]. Although cooperation between Member States is still required, the EU currently has a broader competence to act and is no longer required to link to realisation of, for example, the internal market as it had to when drafting 85/374/EEC.

Directive 85/374/EEC does not realize a full harmonization. Certain provisions leave a margin of appreciation for the Member States. One is the implementation of the development risk defence which will be discussed in section 4.4.1.6[308]. Member States can choose not to implement this defence, but only few have done so and some even only for specific types of products. Member States can also cap liability at a maximum amount but this option has only been used rarely by Member States[309].

4.4.1.2 Scope

The scope of 85/374/EEC covers the producer's liability for damage caused by defective products. In relation to defective products everybody involved in the production chain of the defective product can be held liable. It is also important to point out that the liability for defective products does not require the purchase of the product. Only damage caused by a defective product is required.

4.4.1.3 Definitions

In this section we will elaborate on the definitions of product and producer that are key elements of Directive 85/374/EEC.

4.4.1.3.1 Product

Product covers all material movables, even those incorporated in another movable or even immovable object[310]. As a result it does not only cover the defective product, but also the components of the defective product and the components of the components of the defective product[311]. Immaterial goods are not covered by Directive 85/374/EEC. This means that software sold on a CD is covered by the Directive, but software sold as a download over the internet is not covered.

[307] Art. 4 (k), 6 (a), TFEU
[308] Art. 15, 85/374/EEC
[309] Art. 16, 85/374/EEC
[310] Art. 2, 85/374/EEC; A. Deleu, "La responsabilité du fait des produits defectueux" in X., Vente. Commerce Pratique, losbl., (I.6-50) 105
[311] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, (110) 16824

4.4.1.3.2 Producer

The *producer* is the manufacturer of a finished product, the producer of a raw material or the manufacturer of a component part and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as its producer[312]. The main point of focus of the legislation is the manufacturer of the finished product. A finished product is a product that can be used or consumed without the need for any further modification. Car manufacturers such as BMW are manufacturers of a finished product. In the second instance, the producers of components and raw materials are also contained within this concept for as far as their products are defective. Such companies are Bosch and Continental. Then there are *apparent producers*: people who are regarded as the producer because they link their trademark, name or any other distinctive sign to the product. The reasoning is that in some cases people cannot make out who has produced a particular product. This could be the case if a certain brand has its products made by a sub-contractor. If one cannot determine who has produced a particular product, the consumers' rights are threatened. To preserve these rights, the persons selling those goods under their name are liable for any defects since the seller creates the appearance of being the producer of the product. This assessment will have to be done case by case, but it is not sufficient that the seller mentions his name for advertising purposes or when made mandatory by a legal obligation, as is for example the case for a pharmacist in Belgium and the U.K.[313].

Any person who imports into the Community a product for his commercial activity with a view of selling it or transferring use to a third party shall be deemed to be a producer within the meaning of this Directive and shall be responsible as a producer as well[314]. This liability is not detrimental to the liability of the producer, but prevents consumers from having to pursue legal action against a non-EU producer[315]. 'Transfer of use' is meant to give a broader reach to the provision. This could include contracts such as lease or rent. The importer is liable if he has imported the product with a view to selling it or to transfer the use of the product to a third party. Import must be done in the commercial activity of the importer and the product must be imported from outside the EU[316]. This does leave the problem of an importer located in a different Member State to that of the injured consumer[317]. Although many provisions have already been implemented in EU law to deal with such matters, this is a far from straightforward operation. Where the producer of the product cannot be identified, each supplier of the product shall be treated as its producer unless he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product[318]. The same goes for an imported product if the importer is not known, even if the address of the producer outside the EU is indicated. It is important to note that this liability does not impede with the application of other liability schemes on the supplier, such

[312] Art. 3.1., 85/374/EEC.
[313] G. Howells, *The law of product liability*, Butterworths , London, 2007, nr. 4.92
[314] Art. 3.2., 85/374/EEC
[315] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 125; D., Wuyts, "Productaansprakelijkheid", 36
[316] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 125; D., Wuyts, "Productaansprakelijkheid", 37; A. Deleu, "La responsabilité", 075
[317] G. Howells, "Europe's solution to the product liability phenomenon", *Anglo-Am. L. Rev.* 1991, 208
[318] Art. 3.3., 85/374/EEC; D. Wuyts, "Productaansprakelijkheid", 37; A. Deleu, "La responsabilité", 085

as the warranty for consumer goods[319]. This warranty concerns the sale of consumer goods and regulates the relationship between the vendor and the customer-consumer. The relation between vendor and customer-professional is not covered by this warranty and is to be settled under tort law or contract law.

4.4.1.4 Constitutive Elements

There are three constitutive elements that need to be present for invoking the liability of the producer under Directive 85/374/EEC. It requires damage, a defective product and a causal relation between damage and defect[320]. These elements have to be proven by the injured person[321]. Note that fault is not a constitutive element of liability under Directive 85/374/EEC. It is a system of strict liability where one is held liable because of a certain capacity and not because of a fault one has committed. This is comparable to liability of an employer for damage caused by his employees. The three elements will be discussed in the following sections.

4.4.1.4.1 Damage

Two types of damage are subject to repair under the Directive. The first type is any personal damage suffered through physical injury or death. The second type is material damage suffered because of damage to or destruction of a product[322]. This material damage is subject to two cumulative conditions. Firstly, it does not cover damage to the defective good. Secondly, it only covers damage to goods that are mainly destined for use in the private sphere. This does not mean it only applies to consumer goods but to any good that is mainly used in the private sphere, even if it would be a professional product. The problem of migrated goods has been discussed in the section on product safety and more specifically in section 4.3.3.

Immaterial damage such as moral damage or economic loss of any kind is not covered by the Directive[323]. Those would have to be recovered using other liability regimes available in applicable national law since these regimes are not affected by the Directive[324].

4.4.1.4.2 Defect

As defined by Directive 85/374/EEC, a product is defective if it does not provide the safety one can reasonably expect taking into account all the circumstances, including[325]:

- the presentation of the product;
- the use to which it could reasonably be expected that the product would be put;
- the time when the product was put into circulation

[319] Art. 13, 85/374/EEC; T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5,127
[320] Art. 4, 85/374/EEC
[321] Art. 4, 85/374/EEC
[322] Art. 9, 85/374/EEC
[323] Art. 9 in fine, 85/374/EEC
[324] Art. 13, 85/374/EEC
[325] Art. 6.1., 85/374/EEC

The assessment is one that has to be made case-by-case. The elements summed up are not an exhaustive list. They are just some of the elements to be taken into account. A product does not become defective merely because a better product was subsequently put into circulation[326]. A product is defective because it provides inadequate safety. The safety required is that which a normally careful person in the same situation can expect. This also includes that *system damage* is not covered by product liability[327]. System damage is the inevitable damage inherent in a product but which is nevertheless considered justifiable to the market. System damage is for example the fact that one can die in a car accident or break a leg when falling off a bicycle. In this regard a parallel could be drawn to Directive 2001/95/EC and the General Safety Requirement for product safety legislation[328]. A product can be considered safe according to the General Safety Requirement if the associated risks are deemed acceptable. In both cases it concerns products that are inherently unsafe but despite that fact are allowed on the market because the risk is deemed acceptable.

Safety is assessed based on a consumer expectation test and not an objective standard[329]. To assess safety there are three elements that should be taken into account and that can be supplemented by any other relevant elements. The first element is the presentation of the product. This refers to how the product is commercialised or how it is offered or introduced to the public[330] (considering the packaging, user manual, advertisement, instructions, etc.). By informing the public the producer can meet the safety expectations of the public, but the information might also be inadequate[331]. Examples are the number of safety warnings that can be found in user manuals these days or are affixed on the product. Only unreasonable abuse is thus excluded from the scope of the legislation. When one buys a cup of coffee in a coffee shop it is not uncommon to find the words "Caution, contents may be hot" printed on the lid of the coffee cup. In Common Law tort law a similar situation exists: the failure to warn[332]. Failure to warn can lead to liability of the producer if in failing to warn the injured person he was negligent. Note that the system in the USA mainly revolves around negligence contrary to the strict liability of 85/374/EEC. It is still unclear how the courts will deal with this element relating to information. In the USA there are two sets of discourse. The first says that the possession of information imposes obligations to share this information. A second discourse says that one should weigh the cost of providing information against the cost of product injuries. If the producer, for example, can suffice with an additional mentioning on the packaging of a product he is required to do so. In the EU there is already extensive legislation on information to be provided to consumers.

---

[326] Art. 6.2., 85/374/EEC

[327] G. Howells, "Europe's solution to the product liability phenomenon", *Anglo-Am. L. Rev.* 1991, 212

[328] Section 4.1.4.

[329] A. Stoppa, "The concept of defectiveness in the Consumer Protection Act 1987: a critical analysis", *Legal Stud.* 1992, 211

[330] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 129; D., Wuyts, "Productaansprakelijkheid", 14; A. Deleu, "La responsabilité", 165

[331] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 130; D., Wuyts, "Productaansprakelijkheid", 15A. Deleu, "La responsabilité", 170

[332] M. Shapo, "Comparing products liability: Concepts in European and American Law", *Cornell Int'l L.J.* 1993, 306

The second situation is the reasonable abuse of the product. The Directive mentions that safety must be judged taking into account the use the product could reasonably be put to. This also means that the product must be able to endure a reasonable amount of abuse or the wrong or careless use that can be anticipated[333]. Consequently the producer should not be liable if the most elementary safety measures have been neglected when using the product. Handing a chain-saw to a four year old child is such an unreasonable abuse. Liability for damage caused in those circumstances should not fall on the producer of the chain-saw.

A third element is the moment the product has been put into circulation. This is the moment in time that serves as a reference point for the safety requirements. The moment the damage is incurred is irrelevant in this regard. Stricter requirements that have been put into effect after the product was put into circulation should have no effect on the assessment unless explicitly stated. The criticism on a consumer expectation test is that it requires a consumer to accurately assess the safety he may be entitled to expect from a product. But the problem is that the consumer often does not have the necessary data available to make such an assessment[334]. Also consumers cannot expect that products are 100% safe and at times a dangerous product may leave the production line due to a manufacturing defect[335]. If one were to accept this thought, this could be reason to discard product liability as useless since consumers should expect to be confronted with dangerous products and as a result are not entitled to any safety expectations. Such an approach to product liability seems exaggerated. Moreover, such a defence existed in German product liability rules, the "odd one out"-defence, but this was removed by the implementation of directive 85/374/EEC[336]. A manufacturing defect is not something the injured person should expect[337]. They should always be held against the manufacturer. Therefore it is important that the three situations mentioned by the directive are only indicative and that the actual assessment should be made based on the merits of the case and not based on an abstract frame of reference.

4.4.1.4.3 Causation

Causation refers to the causal relation between the defect and the damage[338]. The defect must have caused the damage for the rules on product liability to be invoked. That is how causation is defined by Directive 85/374/EEC.

4.4.1.5 Remedy

The remedy is not mentioned in Directive 85/374/EEC. The remedy that is cited most frequently and seems most appropriate is damage payments.

---

[333] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 131-132; D., Wuyts, "Productaansprakelijkheid", 16; A. Deleu, "La responsabilité", 175

[334] G. Howells, "Europe's solution to the product liability phenomenon", *Anglo-Am. L. Rev.* 1991, 213

[335] G. Howells, "Europe's solution to the product liability phenomenon", *Anglo-Am. L. Rev.* 1991, 214

[336] A. Cavaliere, "The economic impact of product liability and product safety regulations in the European Union", *Quaderni del dipartimento di economica publica e territoriale* 2001, nr. 4, p.8

[337] A. Stoppa, "The concept of defectiveness in the Consumer Protection Act 1987: a critical analysis", *Legal Stud.* 1992, 211

[338] Art. 4, 85/374/EEC

4.4.1.6 Release from liability

If the injured person succeeds in providing the evidence the producer can release himself of liability if he proves one of the following grounds[339]:

1. that he did not put the product into circulation,
2. that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards,
3. that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business activity,
4. that the defect is due to compliance of the product with mandatory regulations issued by the public authorities,
5. that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered,
6. in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.

If he can prove any of the cited grounds, he is exempted from liability. The first possibility is proving that he did not put the product into circulation. According to the European Court of Justice in the O'Byrne case, a product is put into circulation if it has left the production process of the producer and has entered a sales process where it is offered in a shape ready for use or consumption[340]. The O'Byrne criterion allows an assessment based on a factual situation. This means the product could be considered put into circulation prior to the moment it is sold. This exception has to be interpreted quite restrictively following the Henning Veedfald decision of the European Court of Justice[341]. That concerned a perfusion liquid manufactured by a hospital for use in a kidney transplant. Since the hospital used it for providing a medical service, it is considered to be put in into circulation[342]. The provision is to prevent liability for products that have not left the production process yet, or products that have been put on the market without consent form the producer[343]. It is also aimed at products that are intended for private use or similar situations. This provision also excludes that the producer is held liable for stolen or counterfeit products[344]. Products undergoing testing to establish their soundness are not put into circulation and are therefore not subject to this legislation. If it concerns prod-

[339] Art. 7, 85/374/EEC

[340] E.C.J. 9 February 2006, *O'Byrne* C-127/04, *O.J.* C 8.04.2006, 27; D., Wuyts, "Productaansprakelijkheid", 41; A. Deleu, "La responsabilité", 265

[341] ECJ C-203/99, Henning Veedfald v. Arhus Amtskommune

[342] T. Vansweevelt, "Productaansprakelijkheid"in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, Mechelen, Kluwer, losbl., II.3, 72

[343] G. Gathem, "la responsabilité du fait des produits", in X., *Guide juridique de l'entreprise*, Brussel, Kluwer, losbl., XII-118.3, 28 ; D. Wuyts, "Productaansprakelijkheid: een Richtlijn voor (n)iets?", *T.B.B.R.* 2008, 40

[344] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 135; A., Deleu, "La responsabilité", 195

ucts used in the provision of a service or freely available on the market the exemption will not apply. These products are considered to be put into circulation.

He could also prove that the defect was probably not present at the time it was put into circulation. This can be done by proving that the defect did not exist at the time the product was put into circulation (negative proof) or that the defect originated sometime after the product was put into circulation (positive proof)[345]. In case of negative proof, the court has a considerable margin of appreciation[346]. The producer is only liable for the products he puts into circulation, not for the use that people make of the products. If this use causes the products to become unsafe, it is an improper use of the product that causes the defect and the damage and we have to refer to general liability law to claim for damages. It is also important that the law requires only a probability given the circumstances; there is no requirement of absolute proof as is the case for the development risk discussed below[347]. This gives a large margin of appreciation to the judge although this should not be necessarily viewed as a benefit to the producer[348]. They will still have to make a solid case and there is a risk that the courts might take the easy way and use their margin of appreciation against the producer.

Alternatively, he could prove that the product is produced or distributed neither for his economic activity, nor his professional occupation. Both facts have to be proven simultaneously for the producer to benefit from the exemption[349]. This is has to be interpreted very restrictively following the Henning Veedfald decision. The perfusion liquid was manufactured in the normal course of business of the hospital and therefore the rules on product liability apply. That one could doubt it is manufactured for an economic activity is no reason to release the hospital from liability. The hospital used the liquid for its professional activity. Here again, a very strict interpretation of the provision is to be observed and the conditions have to be applied cumulatively. What this provision is mostly aiming at is voluntary performances, albeit that these should not relate to the professional occupation of the volunteer[350]. This means that a baker can be exempted from liability for a wooden table he makes as a pastime unless he sells it, which implies an economic activity, but not for a cake he baked for a friend's party, since baking cakes is part of his professional occupation[351].

He will also be exempt from liability if he can prove that the defect is due to compliance of the product with mandatory regulations issued by the public authorities. Three aspects must be proven[352]. Firstly, he must prove the product is subject to government regulations. The

---

[345] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 136; D., Wuyts, "Productaansprakelijkheid", 42; A. Deleu, "La responsabilité du fait des produits defectueux" in X., Vente. Commerce Pratique, losbl., (I.6-50) 280

[346] D. Wuyts, "Productaansprakelijkheid", 42

[347] G. Gathem, "la responsabilité du fait des produits", in X., *Guide juridique de l'entreprise*, Brussel, Kluwer, losbl., XII-118.3, 31 ; T. Vansweevelt, "Productaansprakelijkheid"in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, Mechelen, Kluwer, losbl., II.3, 72b

[348] D. Wuyts, "Productaansprakelijkheid: een Richtlijn voor (n)iets?", *T.B.B.R.* 2008, 42

[349] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 137; A. Deleu, "La responsabilité", 285

[350] ECJ C-203/99, Henning Veedfald v. Arhus Amtskommune; G., Gathem, "la responsabilité du fait des produits", in X., *Guide juridique de l'entreprise*, Brussel, Kluwer, losbl., XII-118.3, 31

[351] D. Wuyts, "Productaansprakelijkheid", 43

[352] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 138; D., Wuyts, "Productaansprakelijkheid", 44; A. Deleu, "La responsabilité", 290; G. Howells, "Europe's solution to the product liability phenomenon", *Anglo-Am. L. Rev.* 1991, 219

term government is to be interpreted broadly. It covers not only the normal institutions that are considered as the government, but also governmental standardization and normalization institutions. The latter's private counterparts are not covered by the legislation unless their norms are made mandatory by law. This brings us to the second aspect to be proven, that the defect results from mandatory regulation. This means that the manufacturer does not have any margin of appreciation in applying the regulation. If the manufacturer has a choice whether or not to adhere to the rules, then it is not considered a mandatory regulation, hence the extra requirement of mandated by law for industry standards stemming from private bodies. Thirdly, the causal relation between the defect and the mandatory government regulation must be proven. This means that the defect must follow from the requirements set forth by the regulation.

The fifth ground of release is a debatable one[353]. It is the *development risk defence*[354]. The state of scientific and technical knowledge at the time when the producer put the product into circulation was not such as to enable the existence of the defect to be discovered[355]. 'The state' refers to the most advanced state of scientific and technical knowledge that is publicly available at the time the product was put into circulation[356]. The competences of the producer are irrelevant in that regard, which gives the criterion an abstract character typical for a strict liability scheme such as product liability[357]. Whether it is reasonable or not to assume the producer should have the knowledge is irrelevant. It is however not completely abstract since it only takes into account only publicly available knowledge, not all the existing knowledge including knowledge that was secret at that time. This provision focuses on the discovery of the defect. It is irrelevant whether or not the defect could be repaired or prevented; the provision only looks at the detection of the defect[358]. This raises an issue with regard to the concept of 'knowledge'[359]. One can enquire when knowledge becomes relevant. Sometimes a discovery is made but the result may not be universally accepted[360]. It may not be sufficient to identify a risk; one should also consider what the appropriate response to that risk could be[361]. The view of the European Court of Justice expressed in Commission v. United Kingdom is that if it was impossible to discover the defect following the state of scientific and technical

[353] D. Struyven, "Responsabilité du fait des produits: l'Europe dans la tourmente?", *Rev. Dr. intern. comp.* 2001, 263-266; D., Wuyts, "Productaansprakelijkheid: een Richtlijn voor (n)iets?", *T.B.B.R.* 2008, 45

[354] Art. 7 e) 85/374/EEC

[355] D. Fairgrieve, G. Howells, "Rethinking product liability: a missing element in the European Commission's third review of the European Product liability Directive", *The Modern Law Review* 2007, 970

[356] Cass. 6 avril 2006, *Pas.* 2006, 802 ; G. Gathem, "la responsabilité du fait des produits", in X., *Guide juridique de l'entreprise*, Brussel, Kluwer, losbl., XII-118.3, 33; D., Wuyts, "Productaansprakelijkheid: een Richtlijn voor (n)iets?", *T.B.B.R.* 2008, 45

[357] G. Gathem, "la responsabilité du fait des produits", in X., *Guide juridique de l'entreprise*, Brussel, Kluwer, losbl., XII-118.3, 32-33 ; T., Vansweevelt, "Productaansprakelijkheid"in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, Mechelen, Kluwer, losbl., II.3, 73 ; M. Shapo, "Comparing products liability: Concepts in European and American Law", *Cornell Int'l L.J.* 1993, 303

[358] D. Wuyts, "Productaansprakelijkheid: een Richtlijn voor (n)iets?", *T.B.B.R.* 2008, 46

[359] C. Newdick, "Risk, Uncertainty and "Knowledge" in the development risk defence", *Anglo-American Law Review* 1991, 310

[360] C. Newdick, "Risk, Uncertainty and "Knowledge" in the development risk defence", *Anglo-American Law Review* 1991,314-315

[361] C. Newdick, "Risk, Uncertainty and "Knowledge" in the development risk defence", *Anglo-American Law Review* 1991, 316

knowledge, the producer is exempt[362]. Consideration 29 of the judgment expresses the position:

> *It follows that, in order to have a defence under Article 7(e) of the Directive, the producer of a defective product must prove that the objective state of scientific and technical knowledge, including the most advanced level of such knowledge, at the time when the product in question was put into circulation was not such as to enable the existence of the defect to be discovered. Further, in order for the relevant scientific and technical knowledge to be successfully pleaded as against the producer, that knowledge must have been accessible at the time when the product in question was put into circulation.*

The inclusion of scientific knowledge is very important[363]. The knowledge goes beyond that which stems from the business community which would be more or less akin to a negligence criterion. Also, knowledge available in the scientific community must be taken into account. The possibility of access to relevant information thus implies "knowledge".

It is important to note that not every country in the Community adopted this exception in national law, as is the case for Luxemburg[364]. Some countries have limited the scope of this exception, as Germany did by excluding pharmaceuticals[365]. The most common example that is cited for development risk defence is the Softenon-drama[366]. This concerned pain medication given to pregnant women. This medication led to babies being born with all sorts of birth defects caused by the medication. These side-effects had not been discovered during the development phase and there was no scientific evidence available that would suggest such side-effects. Another example concerns blood transfusion in France and HIV-infected blood products in Germany and Denmark[367]. Because only few examples seem to exist some believe the development risk is of little use and should not have been included in the directive[368]. A counterargument was that not including the defence might be detrimental to research and development or manufacturers might release products without proper risk assessment given that they would be liable anyway. None of these arguments pro or contra development risk defence in Europe has yet been proven in practice. In the USA one can find the "state-of-the-art" defence. While some make the parallel with the development risk defence, this parallel is incorrect[369]. The state-of-the-art is a measure to ascertain whether a product is defective or not. The development risk defence is a measure to ascertain whether the defect should have

[362] Judgment C-300/95 of the Court (Fifth Chamber) of 29 May 1997, Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland, *European Court reports* 1997 Page I-02649; J. Stapleton, "Product Liability in the United Kingdom: The Myths of Reform", *Texas International Law Review* 1999, 34

[363] F. Cafaggi, "Product Safety, Private Standard Setting and Information Networks", *EUI WP LAW 2008/17*, 7

[364] D. Struyven, "Responsabilité du fait des produits: l'Europe dans la tourmente?", *Rev. Dr. intern. comp.* 2001, 265; D. Wuyts, "Productaansprakelijkheid: een Richtlijn voor (n)iets?", *T.B.B.R.* 2008, 45; A., Cavaliere, "The economic impact of product liability and product safety regulations in the European Union", *Quaderni del dipartimento di economica publica e territoriale* 2001, nr. 4, p. 7

[365] G. Howells, "Europe's solution to the product liability phenomenon", *Anglo-Am. L. Rev.* 1991, 213

[366] T. Vansweevelt, "Productenaansprakelijkheid", *VENA* 2004, afl. 5, 139

[367] A. Cavaliere, "The economic impact of product liability and product safety regulations in the European Union", *Quaderni del dipartimento di economica publica e territoriale* 2001, nr. 4, p. 8

[368] C. Stolker, "Vijf argumenten tegen het ontwikkelingsrisicoverweer", *NJB* 1998, nr.19, 643-644

[369] C. Stolker, "Vijf argumenten tegen het ontwikkelingsrisicoverweer", *NJB* 1998, nr.19, 645

been uncovered by the manufacturer. Development risk defence starts from the notion that a product is defective contrary to state-of-the-art.

Manufacturers of a component have a specific release ground. They can be released if they can prove the defect in the component is due to the design of the product it was fitted in, or to the instructions given by the manufacturer of the product[370]. As stated in the scope, the manufacturer of the end product is always liable as producer, manufacturers of components or raw materials only for defects to their component or raw material. This provision adds another limitation to the liability of manufacturers of components; it does not include the manufacturers of raw materials. It is also very precise concerning the possibilities for release, only when the defect is due to the design of the product to which the component was fitted or the instructions of the manufacturer. This is all to be proved by the manufacturer of the component who sees his liability invoked[371]. What this provision actually does is make the origin of the defect relevant. Normally, liability is encountered because the product is defective and irrespective of the origin of the defect. In this provision, the origin of the defect becomes relevant. We have mentioned before that in some cases the defect is clear. Take for example a tyre blow-out. This is not normal and the tyre manufacturer could be held liable. If he can prove that the blow-out was due to a bad set-up of the suspension putting abnormal strain on the tire and as such causing the blow-out, he could be released from liability. In the hypothesis made the suspension set-up is the cause of the blow-out. It should be remembered that a defective product is a product that is unsafe. It is irrelevant whether or not there is a structural flaw in the product. This release ground is very important for companies such as Bosch and Continental who supply vehicle components.

The cited grounds are the only possibility for the producer to release himself from liability. Contractual release clauses have been explicitly excluded by Directive 85/374/EEC[372]. This concerns both clauses excluding liability and clauses limiting liability. Product liability falling within the scope of 85/374/EEC is dealt with according to the rules of the Directive and those rules only.

4.4.1.7 Terms

Two terms apply in relation to 85/374/EEC. Firstly, any claims following from 85/374/EEC expire 3 years after the injured person became aware or should have become aware of the defect, the damage and the identity of the producer[373]. This means that the injured person has 3 years to file a claim from when the right to claim came into existence.

Dissolution of the right to claim damages under 85/374/EEC takes place 10 years after the product has been put on the market[374]. This means that after 10 years the producer can no longer be held liable under the rules of Directive 85/374/EEC. However this does not mean that the producer is fully exempt from liability. Firstly, claims that have been filed prior to the

[370] art. 7 f) 85/374/EEC

[371] G. Gathem, "la responsabilité du fait des produits", in X., *Guide juridique de l'entreprise*, Brussel, Kluwer, losbl., XII-118.3,33

[372] Art. 12, 85/.74/EEC

[373] Art. 10, 85/374/EEC

[374] Art. 12, 85/374/EEC

date of dissolution remain in existence[375]. Secondly, the producer could still be held liable based on other regimes existing in the Member States. This will be elaborated on in sections 4.4.2and 4.5of this deliverable.

These terms are not fixed. National law may impose rules relating to suspension or interruption[376]. Suspension means that the time is stopped and, after the ground requiring the suspension has ceased to exist, time starts running again from the moment the time has been stopped. This means that if the 3-year term is suspended after 2.2 years, the term will run the remainder of the 3 years after the ground for suspension has ceased to exist. Only 0.8 years will remain until the term fully expires. In case of interruption the term restarts anew. This means that in relation to the given example a new 3-year term will start after the moment the grounds for interruption have ceased to exist.

4.4.2 National Law

Even though the Directive is meant to harmonize European legislation with regard to product liability it is not a full harmonization of product liability law given the rather restrictive scope. Damage to products used for professional purposes is not covered, and neither are non-physical personal damages nor immaterial damages. The problems this raises will be further elaborated on in the next section 4.5.

4.5 Intermediate conclusion with regard to the liability issues

Although the rules on product liability apply throughout the EU, Member States still have other legislation dealing with product liability. This is justified by the fact that the rules on product liability do not cover all the damage that could be caused by defective products. Damage caused by professional products is not covered and neither is damage caused by goods used for professional purposes. Additionally it should not be forgotten that the directive on product liability only dates back to 1985 and it only entered into force in 1988. Prior to those rules damage caused by products was dealt with under the then existing rules on liability. These rules have not been abolished by the entry into force of the product liability directive. In Belgium, litigation involving product liability was long conducted under the old rules, to the detriment of the legislation stemming from the Directive on product liability, even though this legislation had priority over the tort rules on product liability. This priority follows from the rule *lex specialis lege generali derogat*. A specific law has priority over a general law. But there remain some dissonant voices in this regard, mainly the UK[377].

Although legislation based on the Product Liability Directive is similar throughout Europe, or so it should be, the tort liability schemes differ quite significantly. There are evidently differences between the common law and the civil law tradition, but even between the civil law traditions there are differences that are non-negligible. In general three families are distin-

[375] Art. 12, 85/374/EEC
[376] Art. 10.2, 11, 85/374/EEC
[377] M. Griffiths, P. De Val, R.J. Dormer, "Developments in English Product Liability Law: a Comparison with the American System", *Tulane Law Review* 1987-1988, 364

guished in Europe: English, French and German. The English family is based on common law. The French family is the civil law tradition. The German family contains elements from both common and civil law. Yet these families should only be considered as an indicative division and not as an absolute division. Even within the families considerable discrepancies can be found. An example from the French family may clarify this. French and Belgian law are both based on the Code Napoleon and share provisions on general liability law as for example article 1384 of the Civil Code which even has the same article number in both civil codes. But French law holds parents liable for all damage caused by their children, while Belgian law only holds parents liable for illegitimate acts of their children. One provision with the same wording yet interpreted differently resulting in different outcomes. Such is the problem of the General Liability Law in Europe.

5 Conclusions

The objectives of the EVITA project are to design, to verify, and to prototype a modular, (cost-) efficient security solution for automotive on-board networks in order to protect data within such networks against compromise and, in doing so, to enable secure communication among cars and between cars and infrastructure.

The aim of this Deliverable is to provide guidance in relation to legal issues related to the use of automotive on-board networks and, insofar as necessary, to formulate legal guidelines for the other partners in the EVITA project. The envisaged use cases are more in particular:

- **V-2-X:** use cases involving external wireless communication between vehicles and other vehicles or roadside infrastructure;
- **eToll:** toll transactions;
- **eCall:** emergency assistance calls;
- **nomadic devices:** use cases involving in-vehicle wireless communications links or temporary wired connection such as USB devices;
- **aftermarket:** installation of aftermarket modules or replacement of defective modules;
- **diagnosis:** including both diagnostic and software maintenance activities.

In the first place EVITA needs to take into account the European legal framework that is currently under development in the area of ITS. At the time of writing, this framework consists of the ITS Framework Directive 2010/40/EU and the specific legal provisions on electronic road tolling in Directive 2004/52/EC and Commission Decision 2009/750/EC. The ITS Framework Directive holds specific provisions on the processing of personal data in its Article 10. This Article doesn't actually create new legal obligations but essentially refers to the existing legal framework in the area of privacy and personal data protection. Together with the Opinion of the EDPS[378] it provides however interesting guidelines on how to apply privacy and data protection rules to the ITS context. Article 11 of the ITS Framework Directive holds a provision with regard to liability referring essentially to the existing European and national legal framework with regard to liability for defective products.

This deliverable examines further in more detail how the existing legal European and national legal rules with regard to **privacy and personal data protection** apply to the use of automotive on-board networks. Some major conclusions of this analysis are:

- In almost all cases where automotive on-board networks are being used, personal data within the meaning of Directive 95/46/EC ("the European Data Protection Directive") will be processed. Possible exceptions would only be use cases where non-identifiable vehicles transmit anonymous signals to other vehicles or to infrastructures.
- One of the most challenging legal questions in the area of automotive on-board networks is how to determine the controller(s) and the processor(s) of the personal data as these terms are defined in Directive 95/46/EC. It is our view that, in the current legal

[378] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:047:0006:0015:EN:PDF

framework, the controller(s) and the processor(s) can only be determined on a case-by-case basis, taking into account the Opinion of the Article 29 Working Party.

- EVITA contributes substantially to the implementation of the most essential legal principles in the area of privacy and personal data protection, for example, by developing technologies to protect personal data against unauthorized access. According to Art. 17 of Directive 95/46/EC the controller must implement *appropriate* technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure to be protected.
- EVITA ensures the legally required "level of security appropriate to the risks represented by the processing and the nature of the data by proposing a risk analysis approach to identify what level of security protection may be required for particular on-board "assets". The range of on-board assets to be considered includes electronic control units (ECUs), data busses, and sensors and actuators. The EVITA Security Architecture Specification[379] proposes three possible levels of hardware security measures (HSMs) for assets that are deemed to need protection.
- The introduction of on-board automotive networks can lead to difficult legal problems related to the correct application of Directive 2002/58/EC ("the E-Communications Privacy Directive"). One example is the application of Art. 5.3 of this Directive – as amended in 2009 – introducing as a new requirement the *consent* of the subscriber or the user for the storing of information or the gaining access to information that is already stored in their terminal equipment. Automotive on-board units undoubtedly belong to the end-user's terminal equipment.
- Specific legal issues arise because the use of on-board automotive networks very often leads to the processing of location data. For example Art. 9.1 of Directive 2002/58/EC clearly stipulates that location data which relates to a user or a subscriber of a network or service can only be processed when (i) such data is made anonymous or (ii) the user or subscriber has given his consent to such processing for the purposes and for the duration of the provision of a value added service. In the latter case, the user or subscriber must be informed prior to consent of the type of location data which will be processed and of whether the data will be transmitted to a third party with a view to providing value added services.
- In cases where consent of the user or subscriber has been obtained for the processing of location data, the network operator or service provider must provide for the possibility for the user or subscriber, by simple means and free of charge, to refuse the processing of his/her location data for a given connection to a network or for a given transmission of a communication (article 9.2). Furthermore, users or subscribers who have given their prior consent to the processing of location data can withdraw such consent at any time.

[379] B. Weyl et al, "Secure On-board Architecture Specification", EVITA Deliverable 3.2, Versions 1.1, 19th July 2010, Section 4.2

In the ITS Action Plan, the European Commission states that **liability** issues have hampered the market introduction of intelligent integrated safety systems, with legal questions regarding product/manufacturer liability and driver responsibility. In the case of automotive on-board networks not only car manufacturers and drivers are involved but a series of other actors can be held liable if damage occurs.

It should be emphasized that liability regimes are deeply rooted in the national legal traditions of every single jurisdiction. Some European legal instruments – some of which we have dealt with in this Deliverable – contain provisions about liabilities but these provisions are subsequently integrated in the national liability regimes of every Member State and adapted to the terminology and the logic of the national jurisdiction.

There are nevertheless a few essential principles that are applied everywhere. One of these principles is that liability – defined as the duty to compensate the damage caused – can be determined by contract or by law. In the first case, parties agree among them who will be liable for which damage and under which conditions. This principle underpins the so-called "disclaimers". In the terms and conditions agreed on at the moment of a car sale, a car manufacturer, for example, can state that he will not be liable for damages caused by the wrong manipulation of a device by the car driver. Or a software vendor can mention in an end user license agreement that the he will not be liable for damages caused by the malfunctioning of his product. Or, vice versa, a customer can negotiate a service level agreement with a service provider or a network operator and agree that damages will be compensated if agreed service levels are not realised.

On the other hand, many laws prevent parties to freely establish their mutual liabilities in a contract. One example is so-called liability for defective products. As defined by Directive 85/374/EEC, a product is defective if it does not provide the safety one can reasonably expect taking into account all the circumstances, including the presentation of the product, the use to which it could reasonably be expected that the product would be put or the time when the product was put into circulation. The assessment is one that has to be made case-by-case.

Probably the most frequent situation is, however, the one in which damage leads to liability questions between people who never concluded a contract about this topic. This is what, in certain jurisdictions, is called "tort liability" or "liability for negligence". Generally speaking this situation is regulated by law. For example the (national) law can stipulate that, if damage is caused by the negligence of a person, the negligent person shall compensate the damage.

The rule just mentioned will probably be the basic rule for tort liability in almost every jurisdiction but its interpretation and its application in concrete circumstances will differ. Over years and centuries legal courts in the national jurisdictions have developed their own jurisprudence about how to apply this basic rule. What is meant by "damage"? Which kind of damage will be taken into account? How to provide evidence of the damage? What is meant by "negligence"? Who should provide the proof that someone has been negligent? Which kind of causal relationship should there be between the negligence and the damage occurred? Etc. Answers to these questions are provided by the jurisprudence of the national courts but often also by other sector-specific or general legal rules.

The functionality that is envisaged for future vehicle systems will be increasingly dependent on inputs from a variety of external systems (e.g. positioning and navigation signals, and messages from other vehicles or roadside infrastructure), as well as a widening array of on-board sensors, actuators and electronic control capabilities. Such systems may diminish the driver's current role, and perhaps ultimately replace the driver with fully autonomous driving

systems. In these scenarios the quality of information received from outside the car, the reliability of wireless communication channels, and the dependability of the on-board systems will be increasingly significant factors for successful and safe operation. Consequently, responsibility for accidents might be expected to shift away from the driver towards vehicle manufacturers and their on-board systems suppliers and more and more also to external information providers.

Establishing that a vehicle control system responded in an unexpected way to a particular combination of transient inputs is likely to be extremely difficult. For this reason, it has been suggested that there should perhaps be an obligation to install an event data recorder (similar to the so-called “black box”, which has been used in aircraft for many years)

A final comment stems from the ITS legal framework. Directive 2010/40/EU requires interoperability of ITS. The plug-in architecture of EVITA would appear to be a very good step in achieving this. EVITA does not have to be integrated, it can be just attached to the modules or networks that it is intended to protect, provided that sufficient bandwidth is available to cope with the additional payload required for security purposes as described in section 2.1 of Deliverable 3.2. Additionally, the intention of EVITA is to develop an open standard for use within other EU projects and also within the industry. The development of open standards is advocated by Directive 2010/40/EU as well.