Grant Agreement Number: 731993

Project acronym: AUTOPILOT

Project full title: AUTOmated driving Progressed by Internet Of Things

D. 4.9

Preliminary legal perspectives on the use of IoT for AD

Due delivery date: 30/06/2018

Actual delivery date: 28/06/2018

Organisation name of lead participant for this deliverable: ERTICO – ITS Europe

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the GSA)	
RE	Restricted to a group specified by the consortium (including the GSA)	
CO	Confidential , only for members of the consortium (including the GSA)	

Project funded by the European Union's Horizon 2020 Research and Innovation Programme (2014 – 2020)

AUTOPILOT

Document Control Sheet

Deliverable number:	D4.9
Deliverable responsible:	ERTICO – ITS Europe
Work package:	WP4
Editor:	Rita Bhandari

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
François Fischer	ERTICO	f.fischer@mail.ertico.com
Haibo Chen	UNL	H.Chen@its.leeds.ac.uk
Jordi Pont	IDIADA	jordi.pont@idiada.com
Rita Bhandari	ERTICO	r.bhandari@mail.ertico.com
Rubén Heras	IDIADA	ruben.heras@idiada.com

Document revision history			
Version	**Date**	**Modifications introduced**	
		Modification reason	**Modified by**
V0.1	26/02/2018	Outline	Rita Bhandari, ERTICO - ITS
V0.2	01/03/2018	1st draft	Rita Bhandari, ERTICO - ITS
V0.3	01/06/2018	Added Section 3.3.3 Privacy-enhancing and privacy-preserving techniques	Haibo Chen, UNL
V0.4	05/06/2018	Added content to Section 2.3 2.3 Recommendations - industry and regulation	Jordi Pont / Rubén Heras, IDIADA
V0.5	14/06/2018	Integration of comments + Internal review	Rita Bhandari / François Fischer, ERTICO - ITS
V0.6	25/06/2018	Peer review (UITP & STM) WPL check (TNO)	Jochen Langheim / Gaelle Kermorgant, STM Guido Di Pasquale, UITP Bart Netten, TNO
V1.0	28/06/2018	Final version for delivery	Rita Bhandari, ERTICO - ITS

Abstract

As a likely disruptive technology, Internet-of-Things (IoT) comes with a number of potential legal challenges. These challenges are heightened when IoT technologies are used in the context of autonomous driving (AD).

This document presents preliminary legal perspectives and the methodology for evaluating legal issues – such as security and privacy aspects, liability issues, concerns and expectations – relating to AUTOPILOT's use of IoT technologies for advancing AD in a connected environment. The methodology presented here revolves around processes aligned with activities to be carried out as part of Task 4.6. Quantitative and qualitative consultation methods are used in the form of surveys and workshops to define, analyse and report on the legal aspects of using IoT solutions for AD. As a first step, expertise from AUTOPILOT project partners representing various stakeholder clusters is gathered and is complemented by user surveys on legal issues from pilot sites. The description by the internal experts of the legal impacts of using IoT solutions for AD and the results of the user surveys are then analysed in consultation with legal and regulation experts through focus groups and workshops.

This document will be updated in M34 in deliverable D4.10: *Legal perspectives on the use of IoT for AD*. D4.10 will present the outcome of the activities carried out in T4.6 and provide recommendations to the study group from the industry and the regulation committees at the European Commission and the United Nations Economic Commission for Europe that work on regulations relating to autonomous vehicles.

Legal Disclaimer

Abbreviations and Acronyms

Acronym	Definition
AD	Autonomous Driving
GDPR	General Data Protection Regulation
IoT	Internet-of-Things
IPR	Intellectual Property Rights
MNO	Mobile Network Operator
OEM	Original Equipment Manufacturer
WP	Work Package

Table of Contents

Table of Figures

Executive Summary

The aim of the AUTOPILOT project is to bring together knowledge and technology from the automotive and the Internet-of-Things (IoT) value chains in order to develop IoT-architectures and platforms that will advance autonomous driving (AD) in a connected environment. AUTOPILOT will develop new automated driving services by connecting automated driving equipped vehicles over IoT. The services being developed will enable fully autonomous driving.

As a likely disruptive technology, Internet-of-Things (IoT) comes with a number of potential legal challenges. These challenges are heightened when IoT technologies are used in the context of autonomous driving.

This document presents the **methodology for evaluating legal issues** – data security and privacy, liability, physical safety, regulation, concerns and expectations – relating to AUTOPILOT's use of IoT technologies for advancing AD in a connected environment.

Quantitative and qualitative consultation methods are used in the form of surveys and workshops to define, analyse and report the legal aspects of using IoT solutions for AD. The methodology revolves around a three-step process aligned with activities to be carried out as part of Task 4.6. The first step includes collecting information – expertise, concerns and expectations regarding legal matters – by conducting surveys of AUTOPILOT project partners and potential users. The feedback from internal experts on the legal impacts of using IoT solutions for AD will be then analysed in consultation with legal and regulation experts through focus groups and workshops. Finally, the findings will be used to make recommendations on regulation.

The **Legal impacts of using IoT for Autonomous Driving** touch upon a number of issues ranging from regulation, data privacy and security, liability, insurance, intellectual property rights (IPR), etc. The fact that the use of cloud-based IoT for AD brings together a number of actors who collaborate to provide an enhanced driving experience where the traditional role of the human driver is diminished, is a big contributor to legal complexities. There is also the need for regulation to match the progress in the IoT and AD domains and address issues of liability, data privacy and data security.

The large number of partners involved in bringing the connected and automated driving experience to the user could cause difficulties in attributing liability when things go wrong.

The contrary pulls of cloud-based services offering privacy on one hand, and IoT, which is about wide reach and sharing, on the other hand can have legal repercussions to do with issues of customer awareness and EU regulation regarding data processing.

Last but not least, cybersecurity concerns of hacking and the potential for intrusive behaviour, including from law-enforcement authorities is also a legal concern affecting IoT based autonomous driving.

The potential legal intricacies of this new paradigm need to be understood and analysed so that solutions, be they standards or legislation and regulations, can be put in place as the IoT-AD services and products reach users.

1 Introduction

1.1 Purpose and scope of the document

The AUTOPILOT project brings together knowledge and technology from the automotive and the Internet-of-Things (IoT) value chains in order to develop IoT-architectures and platforms that will advance autonomous driving (AD) in a connected environment. As a potential disruptive technology, IoT brings with it the possibility of a number of legal challenges. These challenges are heightened when IoT technologies are used in the context of autonomous driving.

Deliverable D4.9 – *Preliminary legal perspectives for the use of IoT for AD* – has a twofold purpose: First, it presents the methodology for evaluating legal issues – data security and privacy, liability, physical safety, regulation, concerns and expectations – relating to AUTOPILOT's use of IoT technologies for advancing AD. The methodology aligns with three main activities to be carried out as part of Task 4.6: 1) information gathering by involving knowledge holders (AUTOPILOT experts and test users); 2) consulting with external legal and regulation experts; and 3) providing recommendations to regulatory agencies.

The second objective of this document is to provide a preliminary report explaining the impact of using IoT solutions from a legal perspective. This draft report will be used as a basis for the second activity of T4.6, i.e. the external legal expert consultation.

The scope of T4.6, and hence D4.9 and D4.10, is the legal impact of using IoT and the data collected for progressing autonomous driving. The legal issues considered within this task relate to the potential impact on privacy, data protection, physical safety and liability. The scope of this task does not involve analysing day-to-day legal obligations or due diligence of AUTOPILOT's activities individually. Legal issues relating to pilot site activities, for instance the conditions for use of an automated vehicle during the test phases or the conditions for involving users in the evaluation task, are out of scope of the task T4.6.

This document will be updated in M34 as deliverable D4.10: *Legal perspectives on the use of IoT for AD*. D4.10 will present the outcome of the activities carried out in T4.6, including external legal consultations, and provide recommendations to the study group from the industry and the regulation committees at the European Commission and the United Nations Economic Commission for Europe (UNECE) that work on regulations relating to autonomous vehicles.

1.2 Intended audience

Since the legal issues presented in D4.9 bear on AUTOPILOT's core elements – IoT and AD – it is relevant to all project beneficiaries in all WPs.

D4.9 is a public deliverable and also of potential interest to an external audience concerned with the legal implications of IoT and/or AD. It will also be relevant to users to demystify the industry of autonomous driving.

It must be pointed out, however, that as an initial draft of the planned legal perspectives report, this document is considered a working document.

1.3 Structure of the document

Chapter 1 introduces the purpose, intended audience and structure of the document.

Chapter 2 details the methodology used for legal analysis in AUTOPILOT. The activities described are: 1) information gathering by involving knowledge holders (AUTOPILOT experts and test users); 2) consulting with legal and regulation experts; and 3) providing recommendations to regulatory agencies.

Chapter 3 presents a preliminary report on the legal impacts of using IoT solutions for automated driving based on our study of current research and trends.

The primary conclusions are outlined in Chapter 4.

Annex 1 is the internal survey used to collect feedback from AUTOPILOT partner beneficiaries on legal impacts as relevant to various stakeholder groups.

Annex 2 lists the questions provided to task T4.5 to assess the legal perspective as it relates to user acceptance.

2 Methodology for analysing legal impacts in AUTOPILOT

AUTOPILOT deliverable D4.1 – *Methodology for evaluation* – described the evaluation methodology and requirements developed in Task 4.1, which are to be "implemented, refined and executed" in other tasks within WP4: T4.2 – Technical Evaluation, Task 4.3 – Business Impact Assessment, Task 4.4 – Quality of Life Impact Assessment and Task 4.5 – User Acceptance Assessment. With reference to T4.6, D4.1 states that, "Task 4.6 will not implement an evaluation methodology, but instead investigate any legal issues that arise from piloting and the other evaluation tasks".

Task 4.6 intends to assess the legal impacts arising from the use of IoT technologies for enabling or improving autonomous driving in a connected environment. Issues of specific interest are security, privacy and liability. The three-step methodology presented here and illustrated in Figure 1 is based on and aligns with three objectives delineated in T4.6 of AUTOPILOT's *Description of Action* document.

Step 1: Information gathering by involving knowledge holders (AUTOPILOT experts and test users)

Description of Action: Gather the expertise of the project partners to provide a preliminary report (D4.9 draft) explaining the impact of using IoT solutions from a legal perspective. A questionnaire will be provided to task T4.5 for collecting user feedback on the legal issue during the Pilot Site tests.

Step 2: Consultation with external legal and regulation experts

Description of Action: Consultation with legal and regulation experts, analysing the preliminary report elaborated in the previous activity and the questionnaire collected from the users at the Pilot Site.

Step 3: Recommendations to regulatory agencies

Description of Action: Provide recommendations (D4.10) to the study group from the industry and the regulation committees at the European Commission and the UNECE, working on regulations relating to autonomous vehicles.

The processes and methods of legal impact analysis used in T4.6 are detailed in the sections that follow in this chapter. In accordance with D4.1, input from other evaluation tasks will be taken into consideration at every step.

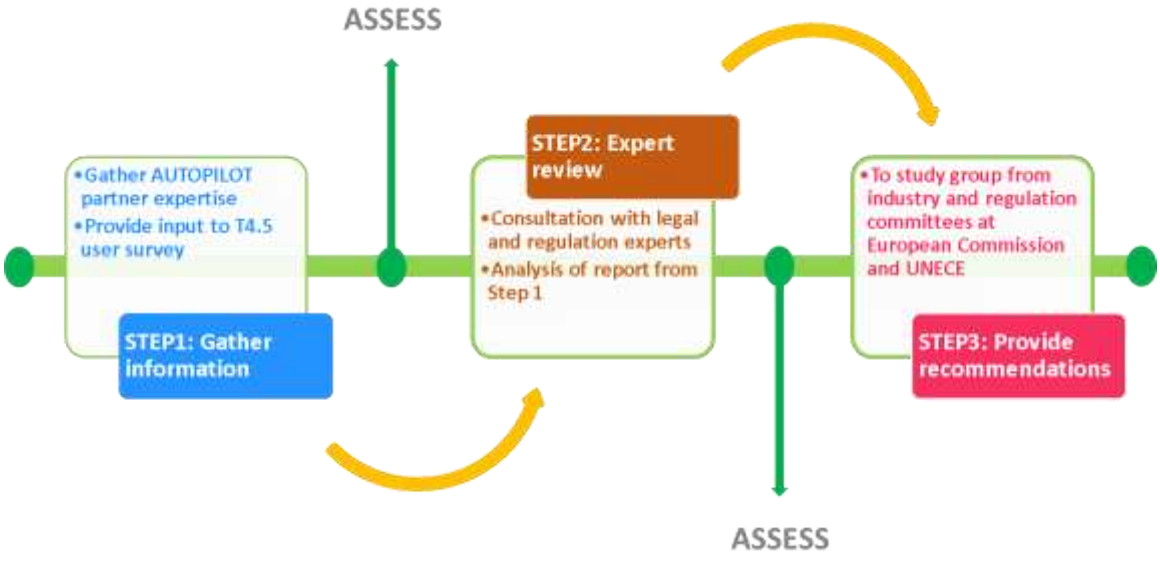

Figure 1: Methodology for evaluating legal issues in AUTOPILOT

2.1 Information gathering

The purpose of this step is to assemble information pertaining to the legal aspects of using IoT for AD. This information will be put together in a report and used as the basis for consultation with external legal experts. At the time of writing this deliverable, we have conducted a review of the current research and regulation relevant to connected and automated driving. A summary of some of the most important elements to emerge from our study are presented in Chapter 3. We will submit a selection of these issues to an in-depth analysis using two different information sources with specific objectives. The first stream of information will be generated from experts in the AUTOPILOT project, while the second source will result from feedback collected on user acceptance as part of T4.5. The information gathered in this way will lead to legal insights covering the scientific and technical aspects as well as having a strong and practical user focus.

The following subsections layout the objectives and plans of both processes of collecting information.

2.1.1 AUTOPILOT experts consultation

Objective: The aim of the internal consultation is to collect the expertise of AUTOPILOT partners about legal issues related to IoT and autonomous driving. The large AUTOPILOT consortium has a diverse makeup with OEMs, research institutions, public authorities as well as ITS organisations. The perspectives they bring would cover a wide spectrum of legal impacts that concern AUTOPILOT's work and mission. The experience and knowledge of the various partners will provide extremely valuable input for framing our analysis of legal issues and ultimately making recommendations to relevant regulation bodies.

Method: Two methods will be used to elicit internal expertise. First, an online survey (in Annex 1) will collect information from the entire consortium about legal concerns that must be addressed in the context of using IoT with AD. Second, a focus group or consultation workshop will be conducted, very likely as a side event alongside a consortium meeting, with relevant AUTOPILOT consortium members to analyse the issues raised.

2.1.2 Feedback from T4.5 user survey

Objective: Collecting feedback from user acceptance surveys conducted as part of T4.5, which is the task evaluating user acceptance, aligns with the objective specified in D4.1 for task T4.6 to "investigate any legal issues that arise from piloting and the other evaluation tasks". The feedback will throw light on users' legal concerns related to privacy (data anonymization), security (data protection), liability and possibly physical safety.

Method: Based on our research review (see Chapter 3), T4.6 has identified some legal issues that could impact user acceptance. A questionnaire (see Annex 2) has been provided to T4.5 to include in the user acceptance surveys they conduct on pilot sites. Once the survey is completed, the results from T4.5 will be analysed and integrated in order to feed into the external consultation workshops on legal impacts of IoT based AD.

2.1.3 Approach

The two information collection methods will be closely connected. Both surveys include questions that have emerged from an initial examination contemporary research and analyses of legal issues of connected and automated driving. In providing input to T4.5, advice and direction was sought from experts within AUTOPILOT, and feedback generated from the user surveys will be submitted for analysis by the internal experts.

The results of the internal consultation and the user acceptance survey will be the basis of the next step of analysis, which is the external legal expert consultation.

2.2 External legal expert consultation

Objective: The results of the internal survey as well as the questionnaire collected during user acceptance evaluations in T4.5 will present a picture from various and diverse standpoints. The main purpose of the consultation with external legal stakeholders will be to analyse the preliminary report elaborated in the previous activity and frame it in the context of regulatory and technical propositions.

Method: The internal expert and user survey results as well as workshop outcomes will be used for the external consultation. Workshops involving legal stakeholders are planned to start in October 2018, and will include issues of liability, data privacy and protections, and current regulation. A number of similar workshops will be held in 2019 around pilot site events. These reviews will inform the recommendations we make to regulatory bodies as the final step towards the end of the project.

2.3 Recommendations – industry and regulation

2.3.1 Current regulatory environment

Connected and automated vehicles pose new challenges regarding privacy and data protection. Since 1995 until recently, the EU approach to privacy was mainly regulated by the Data Protection Directive (Directive 95/46/EC of the European Parliament)[1]. It has now been replaced by the General Data Protection Regulation 2016/679 (GDPR)[2], approved by the EU Parliament on 14th April 2016 and enforced since 25th May 2018. This is the main European regulation regarding data protection. EU privacy laws apply to all sectors and industries, including connected and automated vehicles.

The GDPR applies to information related to identified or identifiable natural persons; not to anonymous information, i.e., the information not related to an identified or identifiable natural person, or that has been made anonymous in such a manner that the individual is no longer identifiable. In particular, the GDPR requires user consent for the purposes of data processing. Prior to giving consent, the subject user shall be informed thereof. Consent must be clearly distinguishable, freely given, as easy to withdraw as it is to give, and auditable or verifiable. Consent must be an explicit (not a passive) activity. Consent shall not be included in a long privacy policy and consent for one use, i.e., it cannot be bundled with other types of consents. Under certain circumstances, the GDPR recognizes a right to data portability, therefore, allowing the consumer to request the transfer of his/her information from one provider to a different one. This right has consequences regarding harmonization of standards. Organizations dealing with personal data need to ensure that their process for collecting and storing this information is compatible with the processes in place by other companies.

Some of the other regulations in place at European level are:

- Directive ECE/TRANS/WP.29/2017/46. Guidelines on cybersecurity and data protection, prepared by the expert from Informal Working Group (IWG) on Intelligent Transport Systems / Automated Driving (ITS/AD)
- Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe)
- Directive 2009/136/EC of the European Parliament and of the Council of 25th November 2009 amending Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector

- Directive 95/46/EC of the European parliament and the Council of 24th October 1995, concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data

Regarding safety and liability, the following regulations are to be found:

- ISO 26262, Road vehicles - Functional safety, concerning functional safety of electrical and/or electronic systems in production automobiles is an international standard defined in 2011 by the International Organization for Standardization (ISO)
- Decision 2001/95/EC of the European Parliament and of the Council of 3rd December 2001, concerning general product safety (the General Product Safety Directive)
- Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9th July 2008, concerning the application of certain national technical rules to products lawfully marketed in another Member State

2.3.2 Approach

At this stage of the project, we have evaluated current EC and UNECE regulations relevant to automated driving and IoT, as presented in the preceding section. This situation, integrated with our findings from internal and user surveys along with the external expert consolations on legal issues, will be presented to industry stakeholders to collect their feedback and concerns around M26. Finally, AUTOPILOT will present recommendations to industry and regulatory bodies to ensure the best possible outcome for cloud-based IoT autonomous driving in terms of wide impact and exploitation.

In the following section, we will look at some of the greatest legal issues facing connected and automated driving in the current climate.

3 Legal impacts of using IoT solutions for AD

In their paper entitled 'Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles', Krasniqi & Hajrizi (2016)[3] point out that IoT is transforming the automobile industry in a revolutionary manner, even compared to other forms of connectivity. They point out that the transformation involves transitioning "from an age of products to an age of services and experiences, from hardware to software, from functionality to information as the key object of value creation, and from industry silos to complex connected ecosystems". It is to be expected that such a disruption in business models will bring with it a host of legal consequences.

A 2017 paper by the international legal firm Allen & Overy LLP[4] states that "six of the biggest legal issues facing the connected and self-driving car market" are: *regulation*, *liability*, *big data and data analytics*, *cybersecurity*, *collaborations and partnerships*, and *cars as socially networked devices*. The paper describes the risks that coincide with these issues and suggests ways to mitigate them. For instance, EU regulation must keep pace with the rapid development of ITS technology, with particular attention to cross-border use of connected cars, interoperability of platforms, net neutrality, etc. The connected and automated mobility paradigm is creating new partnerships between the automotive sector, technology companies and mobile service providers, among others. Such cross-industry collaborations will need to address matters such as third-party liability allocation, responsibility of complying with laws and standards and ownership of jointly created intellectual property. Automobiles as connected vehicles also have legal implications relating to driver distraction, liability, data usage (and its implications for cost apportionment) and cyberattacks.

Four of the legal issues mentioned in the Allen & Overy report – regulation, liability, big data and data analytics, and cybersecurity – cut across all stakeholder clusters, be they regulatory authorities, original equipment manufacturers (OEMs), mobile network operators (MNOs), public and private fleet operators, or end users (drivers). Last year the legal firm Foley & Lardner LLP[5] conducted a survey of automakers, suppliers, start-ups, investors and technology companies in the US about the business and legal issues significant for the development of connected and autonomous vehicles. The survey found that the technologies behind connected cars and autonomous vehicles were at different stages of development and implementation, and thus had different obstacles to growth. While safety and user acceptance were the big challenge for autonomous vehicles, the concerns regarding connected vehicles related foremost to cybersecurity and privacy issues.

By using cloud-based IoT to advance AD, AUTOPILOT has a distinct perspective on EU regulation, cybersecurity, big data analytics and privacy, and liability – matters which are the focus of task T4.6. This document, deliverable D4.9, provides a preliminary synthesis of how these issues are impacted by the use of IoT for autonomous driving.

3.1 Regulation

The 1968 Vienna Convention on Road Traffic, which was premised on a human driver being fully responsible for a vehicle in traffic, now allows the use of driver assistance systems. Since March 2016, driving tasks can be transferred to the vehicle, provided that the UN general safety requirements are not breached and the systems can be overridden or switched off by the driver. Some European governments, such as Germany, France and the UK have provided legal frameworks for the testing and/or use of autonomous vehicles on public roads.

Allen & Overy (2017) point out that, since at least 2008, the European Commission has been working to establish harmonised standards for ITS implementation. However, ITS technology has been developing at a considerably faster pace than EU legislation. The technology has progressed beyond 'Release 1' specifications. Some of the issues that need addressing are cross-border use of connected and autonomous vehicles, clear standards for interoperability, net neutrality, etc.

Once clear guidelines and policies emerge, the onus will be on car manufactures to address these. It is also important that regulations across different regions and countries be uniform.

3.2 Liability

In traditional driving, accidents are normally caused by driver negligence or by defective and malfunctioning vehicles. Accidents may also result from the behaviour of other road users, including pedestrians, and problems with road infrastructure. Once it is clear where the fault lies, liability can be attributed accordingly. Council Directive 85/374/EEC of 25 July 1985[6] clearly outlines liability for defective products in Member States. Connected and autonomous driving is undoubtedly complicating the attribution of liability in case of an accident because it involves a number of additional elements in the equation and at times blurs the distinction between the driver and the vehicle.

3.2.1 Driver/owner vs the autonomous system

One aspect to consider is the relationship between the driver/owner and the autonomous vehicle. How should responsibility to override the autonomous system be delineated? In fully autonomous driving, will the system be completely representative of the driver? Can the driver be liable if an accident results from a decision, for instance a navigation choice, made by the system that the driver would not have made?

In the case of a shared fleet of autonomous vehicles, the operator is an additional actor that should be considered in the responsibility issue.

3.2.2 Product liability: manufacturing vs design defect

The global law firm DLA Piper points out[7] that the question of whether something is a manufacturing defect or a design defect will also raise the stakes in determining fault and liability. Deviations from the manufacturer's specifications and requirements result in manufacturing defects. Even when a product is correctly manufactured, the adoption of one design instead of another may result in a malfunction or cause injury or harm. The connected and autonomous driving scenario includes the car manufacturer, the software provider, and the connectivity provider, all of which may be distinct entities. Liability will depend on whether the flaw lies in manufacturing or in the design.

3.2.3 Software and connectivity

Another important legal issue relates to liability associated with software defects. Liability may have to be apportioned between the software producer for inherent defects, the vehicle manufacturer for 'failure to warn' about possible design defects, and the vehicle owner for failing to install software updates. Liability may arise when an algorithm used for making navigation decision has a design defect. Perhaps the network provider could be liable if a defect in connectivity led to the accident.

3.2.4 Insurance

Where liability has to be shared between various parties it follows that insurance matters will become more complex. The intricacies of whether the fault is assigned to the vehicle manufacturer, the owner, the software provider, or the maker of a specific piece of equipment will impact insurance recovery. In their 2016 paper, which focuses on the marketing and technical trends towards AD, Krasniqi & Hajrizi claim that AD will probably increase the liability of car manufacturers and reduce that of the drivers.

3.3 Big data and privacy

The ever increasing numbers of networks connecting people, devices and sensors is allowing a

seemingly infinite amount of data to be collected, stored, processed and analysed. With cars becoming connected as part of the internet of things, the potential of data collection and big data analytics grows even more. This of course has major repercussions for privacy issues especially with respect to the abuse of personal data.

3.3.1 Personalised services versus privacy infringement

Collecting, storing and other processing operations of personal data are essential in order to provide a personalised mobility. A connected car can access data from a range of sources but when the grounds for processing data is consent and the data is not used strictly for the purpose for which the owner gave consent, it could give rise to serious legal issues. Similarly, if the data is not used solely for the stated purposes, legal problems could arise.

3.3.2 Legal questions and risks

Allen & Overy (2017) point out some of the legal questions and risks linked to data collection and usage:

- **Customer awareness:** Transparency and purpose limitation specifications in data protection laws require customers to be informed about exactly how their data will be used and to sometimes get their consent for that purpose.
- **Data minimisation:** The concept of data minimisation states that there should be minimal data processing and that data should only be stored until necessary. The "Privacy by Design" principle of the GDPR, which states that data protection safeguards must be put in place from the very beginning, also seeks to find a balance between the contrary forces of data minimisation and big data.
- **Storing and processing data under EU law:** Since the transfer of personal data outside of the EEA is restricted, the partners involved must have a compliance framework to be able to share data across national borders within the bounds of the law. The framework must eventually extend beyond data exchange between EU Member States for global compliance.
- **Good data governance:** An individual's vehicle speed, performance and location could be used for public benefit in the complete overall scheme of a connected vehicle system. It would be useful to define standards that make it impossible to identify individuals to enable the use of such data.

The GDPR imposes severe penalties on firms that fail to comply and put consumer data privacy at risk. In order to conform with privacy legislation, especially the GDPR for instance, all participants in the IoT and automotive sectors will have to take adequate measures to avoid risks of privacy infringement. Using cloud-based IoT connectivity for AD can magnify the benefits of connected and autonomous driving and provide a truly personalised and secure autonomous driving experience. Due diligence will be especially needed for access control for the IoT cloud, data anonymization and encryption, and matters of data ownership, etc. must be clearly defined.

3.3.3 Privacy-enhancing and privacy-preserving techniques

Several EU projects funded under ICT-18-2016[8], ICT-14-2016-2017[9] and ICT-15-2016-2017[10] have addressed the privacy-enhancing and privacy-preserving issues in the context of the acquisition, analysis, curation, storage and usage of big data. As many datasets generated from AUTOPILOT are IoT-enabled and can be easily integrated with other big data sources, these privacy enhancing and preserving techniques should be considered (and preferably used) in the AUTOPILOT project.

The e-SIDES project[11] carried out a comprehensive literature review of eleven privacy-enhancing and privacy-preserving technologies which are briefly summarised as follows.

1) **Anonymisation**: Encrypting or removing personally identifiable information from datasets by

using full de-identification models such as k-anonymity, l-diversity, t-closeness and differential privacy.

2) **Sanitisation**: Encrypting or removing sensitive information from datasets by using sanitisation techniques such as masking data, substitution, shuffling and number variance.
3) **Encryption**: Big data applications require fine grade sharing policies using cryptographic primitives include ABE, IBE, PRE and functional encryption.
4) **Multi-party computation (MPC)**: Distributing data and processing tasks over multiple parties to allow securely computing the result of any function without revealing the input data.
5) **Attribute Based Access Control (ABAC)**: Supporting fine grained access control policies in big data based on attributes that are evaluated at run-time.
6) **Automated policy enforcement mechanisms**: Focusing on the enforcement of rules for the use and handling of resources to ensure that data policies do not get lost or neglected in the course of data being transferred between different systems.
7) **Accountability**: Providing the provision of automated and scalable control and auditing processes that can evaluate the level of compliance with policies.
8) **Data provenance**: Attest the origin and authenticity of information.
9) **Transparency**: Explicating information collection and processing to allow data subjects informed choices.
10) **Access and portability**: facilitating the use and handling of data in different contexts, and enabling data subjects to change service providers without losing their data.
11) **Users control**: Specifying and enforcing rules for data use and handling by using consent mechanisms, privacy preferences, sticky policies and personal data stores.

More recently, two EU big data-focused projects (i.e. NOESIS and LeMO) are identifying and addressing the potential privacy and security concerns. NOESIS focuses on the assessment of possible areas of misuse and potential danger that arise with the implementation of big data generation and technologies in the field of transport. LeMO aims to bring crucial issues linked to privacy, data security and legal aspects to the forefront, paving the way for future legal framework for the collection and exploitation of big data in transport. So far, no deliverables have been published. However, the AUTOPILOT Task 4.6 team will work closely with these projects to ensure that their relevant outputs are taken into account when handling the IoT-enabled personal data.

3.4 Cybersecurity

The legal stakes around data security are extremely high for connected and autonomous driving. Cybersecurity breaches would have major legal and business consequences for car manufacturers, other equipment makers, service providers, mobile network operators and all other stakeholders.

3.4.1 Cyberattacks and liability

Cyberattacks on a vehicle, particularly an autonomously driving one, in an IoT system could have dire consequences for the safety and privacy of the user. Any of the electronic devices in a connected car or the car itself could be vulnerable to cyberattacks through various entry points. In this case, the private data collected by the system to enhance the safety and comfort of the autonomous driving experience could be used for exactly the opposite effect. The responsibility of each participant in the IoT connected autonomous car ecosystem must be clearly considered. They will ultimately have to have adequate tools in place to prevent security threats that are proportionate to their legal liability.

3.4.2 Outsourcing and cross-border controls

Cloud computing as used by IoT connectivity has an affinity for outsourcing services and infrastructure, and allows cloud providers to offer better security than internally implemented solutions. Allen & Overy (2017) point out, however, that outsourcing and cloud computing also have

a number of drawbacks that could have serious legal repercussions. First, outsourcing reduces a company's control on its IT security thereby hampering its ability to respond to data security threats. Second, as something EU regulators have to deal with increasingly, cloud computing and outsourcing increase the risk of foreign governments accessing data across national borders.

Data from cars and their occupants could be very highly sought after for surveillance purposes but it could also come in very handy in determining fault and liability, especially in autonomous driving situations.

3.4.3 Internal responsibility

In the current climate, personal data is highly valued and could have an enormous price tag. Allen & Overy (2017) point out that 60% of the data-security breaches in 2015 came from within the company. Additionally, sloppy follow through of data-protection policies and procedures could lead to data security being compromised.

Some of these concerns may be less relevant in the IoT-based autonomous driving context, as IoT sensors will allow wider and more detailed perception of the environment making it more efficient to assess responsibilities in case of incidents. In any event, car manufacturers will have to have robust and secure software in their vehicles from the start. Network providers must have measures in place to counter hacking attempts. Data security compromises in an IoT system of AD could have consequences ranging from privacy infringement to loss of life.

4 Conclusion

As with any new technology or product, IoT solutions providers and autonomous vehicle manufacturers must each take stock of their legal risks. The combination of IoT and autonomous AD brings with it specific challenges that could have far reaching legal consequences. Some of the key reasons for this are:

- There are a number of actors involved in providing the IoT-based driving experience. Fault and liability in the event of an accident must be apportioned between car manufacturers, OEMs, MNOs, software providers, fleet operators and the drivers/owners themselves.
- Cloud-based IoT can provide a highly personalised autonomous driving experience but this entails collecting personal data and big data analytics. The collection, storage, analysis and other processing operations of personal data are subject to stringent EU regulation, chief among them being the new GDPR.
- Personal navigation and car data is valuable to potential criminals and law enforcement authorities, both. There are many incentives to hack or aggressively solicit such data even in cross-border situations, irrespective of jurisdiction. IoT powered by the cloud can provide secure solutions but by removing access from 'internal' control, the responsibility to detect and fix security breaches is also once removed, especially from the car manufacturers and software designers. This may lead to vulnerabilities to data security breaches and also cloud the liability issues.

These issues are a subset of all the legal concerns regarding connected and autonomous driving. Other issues have to do with regulation, especially in the context of increasing international collaborations, and the large number of partners involved outside the automotive industry raising questions of conformance, liability and intellectual property rights. It is clear that there is plenty of scope to fall foul of the law when using IoT for autonomous driving. The legal stakes are particularly high when data security compromises could be a matter of life and death. There is also a clear need for regulation to keep pace with the advances in IoT and AD technology.

Annex 1 – Internal survey of AUTOPILOT beneficiaries

AUTOPILOT **AUTOPILOT - T4.6 Internal questionnaire on legal perspectives**

PART 1 - REGULATION

This survey is part of the effort in task T4.6 to collect knowledge from AUTOPILOT partner beneficiaries on legal perspectives related to the use of the Internet of Things (IoT) for Autonomous Driving (AD).
Results of this survey will be analysed (including in external stakeholder workshops) and will also inform the recommendations we will make towards the end of the project to regulatory and other authorities.

All the questions in this survey pertain to the context of using IoT for AD and focus on regulation, liability, privacy and cybersecurity in this area. The automation level implied in this survey is towards the higher end - at least L3 and above.

Key documents: deliverables D4.9 and D4.10.

Note: There are 30 questions in total, and answers are obligatory for all. If you do not have a response to a question, please write in 'Don't know', 'Not sure', etc.
THANK YOU FOR YOUR TIME and COOPERATION !!!

*** 1. Your sector (choose from only one)**

	Automotive	IoT	Service providers	Research	Public authorities	Users
Sector						

Other (please specify)

*** 2. How well are you acquainted with national and international regulatory matters in this area?**

Not at all familiar						Very familiar

*** 3. How well do you believe that EU regulation is keeping pace with technological developments?**

	Completely outdated						Very forward looking	Don't know
IoT								
AD								
IoT-AD								

*** 4. What area of IoT-AD do you believe needs clear(er) regulation?**

1

* 5. Are you aware of any differences in regulation/legislation between countries (inside or outside EU) that may cause conflict within regulation design?

* 6. In what aspects are standards most needed for or most challenging to the following agents?

Automaker

Connectivity provider

Software developer

Other

* 7. Who should be responsible for conformity with national and international regulation? Choose one sole responsibility or multiple joint responsibility.

- [ ] Automaker
- [ ] Connectivity provider
- [ ] Software developer
- [ ] Other (please specify)

* 8. Is net neutrality (connectivity/internet service providers treating all content equally and impartially) important for IoT-based AD?

- ◯ Yes
- ◯ No
- ◯ Unsure

Comment

*** 9. Who should be liable in the event of an accident due to the following issues?**

	Automaker	Connectivity provider (MNO)	Mobility service provider	Car user/driver
Breakdown of data integrity / misinformation				
Out-dated software applications				
Breach in data privacy				
General equipment failure				

*** 10. How can IoT help in providing information for attributing liability related to AD?**

*** 11. What IoT data would need to be accessed for IoT to facilitate liability attribution or apportionment?**

*** 12. With reference to the two previous questions, is there any additional data needed that would not be required for 'normal' operation (ie gathered ' just in case')?**

*** 13. For how long should the collected data be stored for later analysis?**

- ◯ 6 months - 1 year
- ◯ 1 - 5 years
- ◯ 5 - 10 years
- ◯ More than 10 years
- ◯ Indefinitely

Comment

*** 14. What aspects of IoT use are likely to increase or decrease insurance premiums for autonomous car owners?**

Increase premiums	
Decrease premiums	
No change	

3

AUTOPILOT **AUTOPILOT - T4.6 Internal questionnaire on legal perspectives**

PART 3 - PRIVACY

*** 15. How could personalised IoT AD applications affect privacy?**

Complete loss of privacy						Privacy is completely protected
○	○	○	○	○	○	○

Comment

*** 16. What data would you be willing to give up to get more personalised IOT-AD service?**

*** 17. What data would you be not be willing to give up even to get more personalised IoT-AD service?**

*** 18. To what extent is data minimisation (processing only data necessary for the specific functions) effective for IoT-AD?**

4

*** 19. What IoT-AD data should be accessible to other parties such as?**

Police / National security	
Automakers	
Connectivity providers	
Insurance companies	
Mobility service providers	
Other autonomous vehicles	
Other	

*** 20. Is GDPR a barrier or an enabler for developing new data-based IoT-AD applications?**

Barrier						Enabler
○	○	○	○	○	○	○

Comment

*** 21. Would the IoT managed system inspire more trust if personal information is segregated – for instance, if anonymous data could be freely shared with many organizations and/or IoT devices but law enforcement authorities (Police/National security) would hold the de-anonymization key?**

Strongly disagree						Strongly agree
○	○	○	○	○	○	○

Comment

*** 22. IoT must answer the contrary needs of both data protection and data sharing. Can cloud design for IoT autonomous driving do justice to both equally in an effective way?**

- ○ Yes
- ○ No
- ○ Unsure
- ○ Comment

5

AUTOPILOT AUTOPILOT - T4.6 Internal questionnaire on legal perspectives

PART 4 - CYBERSECURITY

* 23. What are some of the risks that cloud computing brings to IoT-AD?

* 24. What is the greatest risk of those mentioned above?

* 25. How could these risks be minimised?

* 26. Which of the various participants in the IoT for AD system is most vulnerable as an entry point for a cyberattack?

* 27. What aspects of IoT-AD require more specific cybersecurity than other IoT elements?

* 28. In terms of security, how do you view the use of mobile apps for user authentication and access to IoT devices and services? Do you believe they are secure enough?

Not at all secure						Completely secure
○	○	○	○	○	○	○

* 29. With reference to the previous question, what is for you an unacceptable risk?

6

* 30. What would you perceive as the main legal risks related to mobile app usage for user authentication and access to IoT devices and services?

31. Any other comments on legal issues regarding using IoT to advance autonomous driving.

Annex 2 – User survey

AUTOPILOT legal issues questions from Task 4.6 for user acceptance survey (T4.5)

Q1. IoT-enabled autonomous driving (AD) adds many benefits (e.g. informed route choice, congestion avoidance, and quick emergency break to avoid collision) as well as complications to the assignation of liability in case of malfunction. If you decide to buy or hire such a vehicle for the first time, would you:

a. Disable the IoT device straightway

b. Like to know more about the safety standards of the IoT technologies before drive off

c. Use the IoT device with no concern as your insurance policy covers liability

Q2. Compared to your mobile phone which provides your location data, do you think that an IoT-enabled vehicle possesses more concerned about security and vulnerability of access to your location data?

a. Yes

b. No

c. I don't know

Q3. (business) When developing IoT technology for AD, which of the following legal issues would your company be most concerned about?

a. Consumer data privacy

b. Cybersecurity attacks

c. Personal injury/property liability

d. Intellectual property protection

e. Warranties

f. Compliance with state and federal regulations

Q4. Who should be legally responsible in the event of a pedestrian being injured during a valet parking manoeuvre?

a. The owner of the vehicle

b. The owner of the parking premises

c. The car maker

d. The software/application provider

Q5. Vehicle-to-vehicle communication can enable safer interaction at intersections, but there is also a complex chain of responsibility (software providers on each vehicle, sensor providers, road authorities, map-makers and communication providers. Who should have legal responsibility if things go wrong in the case of:

a. An advice system — one that gives the driver warning messages?

b. A control system — one that adjust the approach speed of two or more potentially conflicting vehicles so that they do no collide at an intersection?

Q6. With connection to cloud data, for example to provide weather or traffic information to CAVs, who should have legal responsibility to ensure the accuracy of the information?

a. The information provider if they charge for the information to be used

b. The car maker or their service supplier

c. The cloud service provider

d. No-one

Q7. Would you be willing to provide some personal data (e.g. your address, workplace, commuting patterns) to get more personalised service?

a. No

b. Yes, what data would you be happy to give up?

Q8. If IoT can help in providing information for attributing liability, would you switch on IoT while driving?

a. Yes

b. No, why?

Q9. Would you perceive usage of mobile Apps for user authentication and access to cars as secure enough?

a. Yes

b. No

c. I don't know

Q10. Are you aware about how to react to a cyber-attack if you were in the autonomous car?

a. Yes

b. No

c. I don't know

Q11. Do you know how protection system from your device works?

a. Yes

b. No

c. I don't know

Q12. AUTOPILOT has a team dedicated to IT and cyber security in order to have always the last version of its App updated and installed. Do you feel safer with a double check control for login to the AUTOPILOT App?

a. Yes

b. No

c. I don't know

Q13. Do you prefer a card to be inserted to access the system instead of giving data by the AUTOPILOT app?

a. Yes

b. No

c. I don't know

Q14. Would you be more willing to share information if your data were anonymized?

a. Yes

b. No

c. I don't know

Q15. Would you trust the system more if personal information is segregated – for instance, if anonymous data could be freely shared with many organization but law enforcement authorities (Police/National security) would hold the de-anonymization key?

a. Yes

b. No

c. Unsure

References

[1] 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 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[3] Krasniqi, X. and J. Hajrizi 2016, *Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles* https://www.sciencedirect.com/science/article/pii/S2405896316325162

[4] Allen & Overy LLP 2017, *Autonomous and connected vehicles: navigating the legal issues* http://www.allenovery.com/SiteCollectionDocuments/Autonomous-and-connected-vehicles.pdf

[5] Foley & Lardner LLP 2017, *Connected Cars & Autonomous Vehicles Survey* https://www.foley.com/files/uploads/2017-Connected-Cars-Survey-Report.pdf

[6] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31985L0374

[7] DLA Piper 2018, *The Internet of Things and connected cars: new opportunities and risks* https://www.dlapiper.com/en/europe/insights/publications/2018/01/iot-and-connected-cars-opportunities-and-risks/

[8] ICT-18-2016-Big data PPP: Privacy-preserving big data technologies.

[9] ICT-14-216-2017-Big data PPP: Cross-sectorial and cross-lingual data integration and experimentation.

[10] ICT-15-2016-2017-Big data PPP: Large Scale Pilot actions in sectors best benefitting from data-driven innovation.

[11] Bachlechner, D (lead author) 2018, *D3.1 Overview of Existing Technologies*, e-SIDES: Ethical and Societal Implications of Data Sciences, www.e-sides.eu.